HITRUST
Common Security Framework

2015 – Version 7.0

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Summary of Changes

Version	Description of Change	Author	Date Published
1.0	Final Version of Initial Release	HITRUST	September 11, 2009
2.0	NIST SP 800-53 r2 PCI-DSS v1.2 HITECH ISO/IEC 27002 Rework	HITRUST	January 12, 2010
2.1	(State of Mass.) 201 CMR 17.00 CMR 17.00	HITRUST	March 1, 2010
2.2	Cloud Security Alliance Controls Matrix v1.0, Joint Commission (formerly JCAHO) Information Management State of Nevada (NRS 603A)	HITRUST	September 10, 2010
3.0	CMS IS ARS v1-Appendix A (HIGH)	HITRUST	December 1, 2010
3.1	PCI-DSS v2.0	HITRUST	August 4, 2011
4.0	NIST SP 800-53 r3 HIE WG Recommendations NIST-ISO-HIPAA Harmonization	HITRUST	December 28, 2011
5.0	NIST SP 800-53 R4 (Feb 2012 IPD) Texas Health & Safety Code § 181 ("TX HB 300") HITECH (MU Stage 2) CAQH Committee on Operating Rules for Information Exchange (CORE) NIST-CMS Harmonization Implementation Requirement Harmonization for CSF 2013 Certification-required Controls	HITRUST	January 28, 2013
6.0	NIST SP 800-53 R4 (Apr 2013 Final) CMS IS ARS v1.5 (2012) Title 1 TX Admin. Code 390.2 (TX Standards), including privacy requirements to support TX certification of the HIPAA Privacy Rule NIST-CMS Harmonization (Publication Updates)	HITRUST	February 12, 2014
6.1	PCI-DSS v3.0 HIPAA Omnibus Rule NIST Cybersecurity Framework v1 ISO/IEC 27001:2013 ISO/IEC 27002:2013	HITRUST	April 25, 2014

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Version	Description of Change	Author	Date Published
7.0	CMS IS ARS v2 (2013) HIPAA Omnibus Rule (Rework – Updated Category 13 – Privacy Practices) NIST SP 800-53 R4 Appendix J MARS-E v1.0 IRS Pub 1075 (2014)	HITRUST	January 31, 2015

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

CSF Table of Contents

Introduction 11
Organization of the CSF 13
Key Components 13
Control Categories 14
Implementation Requirement Levels 16
Segment Specific Requirements 16
Risk Factors 16
Alternate Controls 18
Evolution of the CSF 18
CSF Assurance and MyCSF 19
Implementing the CSF 21
Management Commitment 21
Scope 21
Organization 21
Systems 21
Implementation 22
Critical Success Factors 22
Primary Reference Material 23
Control Category: 0.0 - Information Security Management Program 26
Objective Name: 0.01 Information Security Management Program 26
Control Reference: 0.a Information Security Management Program 26
Control Category: 01.0 - Access Control 32
Objective Name: 01.01 Business Requirement for Access Control 32
Control Reference: 01.a Access Control Policy 32
Objective Name: 01.02 Authorized Access to Information Systems 34
Control Reference: 01.b User Registration 34
Control Reference: 01.c Privilege Management 39
Control Reference: 01.d User Password Management 44
Control Reference: 01.e Review of User Access Rights 48
Objective Name: 01.03 User Responsibilities 50
Control Reference: 01.f Password Use 50

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 01.g Unattended User Equipment 53
Control Reference: 01.h Clear Desk and Clear Screen Policy 55
Objective Name: 01.04 Network Access Control 57
Control Reference: 01.i Policy on the Use of Network Services 57
Control Reference: 01.j User Authentication for External Connections 60
Control Reference: 01.k Equipment Identification in Networks 64
Control Reference: 01.l Remote Diagnostic and Configuration Port Protection 66
Control Reference: 01.m Segregation in Networks 69
Control Reference: 01.n Network Connection Control 73
Control Reference: 01.o Network Routing Control 77
Objective Name: 01.05 Operating System Access Control 79
Control Reference: 01.p Secure Log-on Procedures 79
Control Reference: 01.q User Identification and Authentication 82
Control Reference: 01.r Password Management System 88
Control Reference: 01.s Use of System Utilities 90
Control Reference: 01.t Session Time-out 93
Control Reference: 01.u Limitation of Connection Time 95
Objective Name: 01.06 Application and Information Access Control 97
Control Reference: 01.v Information Access Restriction 97
Control Reference: 01.w Sensitive System Isolation 101
Objective Name: 01.07 Mobile Computing and Teleworking 104
Control Reference: 01.x Mobile Computing and Communications 104
Control Reference: 01.y Teleworking 108
Control Category: 02.0 - Human Resources Security 112
Objective Name: 02.01 Prior to Employment 112
Control Reference: 02.a Roles and Responsibilities 113
Control Reference: 02.b Screening 115
Objective Name: 02.02 During On-Boarding 118
Control Reference: 02.c Terms and Conditions of Employment 119
Objective Name: 02.03 During Employment 122
Control Reference: 02.d Management Responsibilities 122
Control Reference: 02.e Information Security Awareness, Education and Training 126
Control Reference: 02.f Disciplinary Process 131
Objective Name: 02.04 Termination or Change of Employment 133

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 02.g Termination or Change Responsibilities 133
Control Reference: 02.h Return of Assets 136
Control Reference: 02.i Removal of Access Rights 138
Control Category: 03.0 - Risk Management 142
Objective Name: 03.01 Risk Management Program 142
Control Reference: 03.a Risk Management Program Development 142
Control Reference: 03.b Performing Risk Assessments 146
Control Reference: 03.c Risk Mitigation 150
Control Reference: 03.d Risk Evaluation 154
Control Category: 04.0 - Security Policy 157
Objective Name: 04.01 Information Security Policy 157
Control Reference: 04.a Information Security Policy Document 157
Control Reference: 04.b Review of the Information Security Policy 162
Control Category: 05.0 - Organization of Information Security 168
Objective Name: 05.01 Internal Organization 168
Control Reference: 05.a Management Commitment to Information Security 168
Control Reference: 05.b Information Security Coordination 171
Control Reference: 05.c Allocation of Information Security Responsibilities 176
Control Reference: 05.d Authorization Process for Information Assets and Facilities 179
Control Reference: 05.e Confidentiality Agreements 182
Control Reference: 05.f Contact with Authorities 185
Control Reference: 05.g Contact with Special Interest Groups 187
Control Reference: 05.h Independent Review of Information Security 189
Objective Name: 05.02 External Parties 191
Control Reference: 05.i Identification of Risks Related to External Parties 191
Control Reference: 05.j Addressing Security When Dealing with Customers 195
Control Reference: 05.k Addressing Security in Third Party Agreements 198
Control Category: 06.0 – Compliance 206
Objective Name: 06.01 Compliance with Legal Requirements 206
Control Reference: 06.a Identification of Applicable Legislation 206
Control Reference: 06.b Intellectual Property Rights 208
Control Reference: 06.c Protection of Organizational Records 210
Control Reference: 06.d Data Protection and Privacy of Covered Information 215
Control Reference: 06.e Prevention of Misuse of Information Assets 219

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 06.f Regulation of Cryptographic Controls 222
Objective Name: 06.02 Compliance with Security Policies and Standards, and Technical Compliance 224
Control Reference: 06.g Compliance with Security Policies and Standards 224
Control Reference: 06.h Technical Compliance Checking 228
Objective Name: 06.03 Information System Audit Considerations 230
Control Reference: 06.i Information Systems Audit Controls 231
Control Reference: 06.j Protection of Information Systems Audit Tools 233
Control Category: 07.0 - Asset Management 236
Objective Name: 07.01 Responsibility for Assets 236
Control Reference: 07.a Inventory of Assets 236
Control Reference: 07.b Ownership of Assets 241
Control Reference: 07.c Acceptable Use of Assets 244
Objective Name: 07.02 Information Classification 246
Control Reference: 07.d Classification Guidelines 246
Control Reference: 07.e Information Labeling and Handling 249
Control Category: 08.0 - Physical and Environmental Security 253
Objective Name: 08.01 Secure Areas 253
Control Reference: 08.a Physical Security Perimeter 253
Control Reference: 08.b Physical Entry Controls 256
Control Reference: 08.c Securing Offices, Rooms, and Facilities 262
Control Reference: 08.d Protecting Against External and Environmental Threats 264
Control Reference: 08.e Working in Secure Areas 267
Control Reference: 08.f Public Access, Delivery, and Loading Areas 269
Objective Name: 08.02 Equipment Security 271
Control Reference: 08.g Equipment Siting and Protection 271
Control Reference: 08.h Supporting Utilities 274
Control Reference: 08.i Cabling Security 277
Control Reference: 08.j Equipment Maintenance 280
Control Reference: 08.k Security of Equipment Off-Premises 285
Control Reference: 08.l Secure Disposal or Re-Use of Equipment 287
Control Reference: 08.m Removal of Property 290
Control Category: 09.0 - Communications and Operations Management 292
Objective Name: 09.01 Documented Operating Procedures 292

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 09.a Documented Operations Procedures 292
Control Reference: 09.b Change Management 295
Control Reference: 09.c Segregation of Duties 296
Control Reference: 09.d Separation of Development, Test, and Operational Environments 299
Objective Name: 09.02 Control Third Party Service Delivery 302
Control Reference: 09.e Service Delivery 302
Control Reference: 09.f Monitoring and Review of Third Party Services 305
Control Reference: 09.g Managing Changes to Third Party Services 307
Objective Name: 09.03 System Planning and Acceptance 309
Control Reference: 09.h Capacity Management 309
Control Reference: 09.i System Acceptance 312
Objective Name: 09.04 Protection Against Malicious and Mobile Code 315
Control Reference: 09.j Controls Against Malicious Code 315
Control Reference: 09.k Controls Against Mobile Code 320
Objective Name: 09.05 Information Back-Up 322
Control Reference: 09.l Back-up 322
Objective Name: 09.06 Network Security Management 326
Control Reference: 09.m Network Controls 326
Control Reference: 09.n Security of Network Services 335
Objective Name: 09.07 Media Handling 338
Control Reference: 09.o Management of Removable Media 338
Control Reference: 09.p Disposal of Media 342
Control Reference: 09.q Information Handling Procedures 346
Control Reference: 09.r Security of System Documentation 350
Objective Name: 09.08 Exchange of Information 351
Control Reference: 09.s Information Exchange Policies and Procedures 352
Control Reference: 09.t Exchange Agreements 358
Control Reference: 09.u Physical Media in Transit 360
Control Reference: 09.v Electronic Messaging 363
Control Reference: 09.w Interconnected Business Information Systems 366
Objective Name: 09.09 Electronic Commerce Services 368
Control Reference: 09.x Electronic Commerce Services 368
Control Reference: 09.y On-Line Transactions 371
Control Reference: 09.z Publicly Available Information 374

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Objective Name: 09.10 Monitoring 377
Control Reference: 09.aa Audit Logging 377
Control Reference: 09.ab Monitoring System Use 384
Control Reference: 09.ac Protection of Log Information 393
Control Reference: 09.ad Administrator and Operator Logs 396
Control Reference: 09.ae Fault Logging 398
Control Reference: 09.af Clock Synchronization 400
Control Category: 10.0 - Information Systems Acquisition, Development, and Maintenance 403
Objective Name: 10.01 Security Requirements of Information Systems 403
Control Reference: 10.a Security Requirements Analysis and Specification 403
Objective Name: 10.02 Correct Processing in Applications 409
Control Reference: 10.b Input Data Validation 409
Control Reference: 10.c Control of Internal Processing 413
Control Reference: 10.d Message Integrity 417
Control Reference: 10.e Output Data Validation 419
Objective Name: 10.03 Cryptographic Controls 420
Control Reference: 10.f Policy on the Use of Cryptographic Controls 421
Control Reference: 10.g Key Management 423
Objective Name: 10.04 Security of System Files 426
Control Reference: 10.h Control of Operational Software 426
Control Reference: 10.i Protection of System Test Data 430
Control Reference: 10.j Access Control to Program Source Code 432
Objective Name: 10.05 Security in Development and Support Processes 434
Control Reference: 10.k Change Control Procedures 434
Control Reference: 10.l Outsourced Software Development 442
Objective Name: 10.06 Technical Vulnerability Management 444
Control Reference: 10.m Control of Technical Vulnerabilities 445
Control Category: 11.0 - Information Security Incident Management 453
Objective Name: 11.01 Reporting Information Security Incidents and Weaknesses 453
Control Reference: 11.a Reporting Information Security Events 453
Control Reference: 11.b Reporting Security Weaknesses 461
Objective Name: 11.02 Management of Information Security Incidents and Improvements 463
Control Reference: 11.c Responsibilities and Procedures 463
Control Reference: 11.d Learning from Information Security Incidents 471

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 11.e Collection of Evidence 474
Control Category: 12.0 - Business Continuity Management 478
Objective Name: 12.01 Information Security Aspects of Business Continuity Management 478
Control Reference: 12.a Including Information Security in the Business Continuity Management Process 478
Control Reference: 12.b Business Continuity and Risk Assessment 480
Control Reference: 12.c Developing and Implementing Continuity Plans Including Information Security 483
Control Reference: 12.d Business Continuity Planning Framework 491
Control Reference: 12.e Testing, Maintaining and Re-Assessing Business Continuity Plans 494
Control Category: 13.0 – Privacy Practices 498
Objective Name: 13.01 – Openness and Transparency 498
Control Reference: 13.a Notice of Privacy Practices 498
Control Reference: 13.b Rights to Protection and Confidentiality 500
Control Reference: 13.c Authorization Required 503
Control Reference: 13.d Opportunity Required 505
Control Reference: 13.e Authorization or Opportunity Not Required 508
Objective Name: 13.02 – Individual Choice and Participation 511
Control Reference: 13.f Access to Individual Information 511
Control Reference: 13.g Accounting of Disclosures 514
Control Reference: 13.h Correction of Records 516
Control Reference: 13.i Required Uses and Disclosures 518
Control Reference: 13.j Permitted Uses and Disclosures 520
Objective Name: 13.03 - Correction 525
Control Reference: 13.k Prohibited or Restricted Uses and Disclosures 525
Control Reference: 13.l Minimum Necessary Use 526
Control Reference: 13.m Confidential Communications 528
Control Reference: 13.n Organizational Requirements 531

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Introduction

The Health Information Trust Alliance (HITRUST) exists to ensure that information security becomes a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges.

All organizations within the healthcare industry currently face multiple challenges regarding information security. These challenges include:

- Public and regulatory concern over the increasing number of breaches in the industry
- Redundant and inconsistent requirements and standards for healthcare organizations
- Inconsistent adoption of minimum controls
- Inability to implement security in medical devices and healthcare applications
- Rapidly changing business, technology and regulatory environments
- Ineffective and inefficient internal compliance management processes
- Inconsistent business partner requirements and compliance expectations
- Increasing scrutiny from regulators, auditors, underwriters, customers and business partners
- Growing risk and liability associated with information security

HITRUST collaborated with healthcare, business, technology, and information security leaders and established the Common Security Framework (CSF) to be used by any and all organizations that create, access, store, or exchange protected health information (PHI). HITRUST is driving adoption and widespread confidence in the CSF and sound risk mitigation practices through the HITRUST Central community that provides awareness, education, advocacy, support, knowledge-sharing, and additional leadership and outreach activities.

The HITRUST CSF addresses these industry challenges by leveraging and enhancing existing standards and regulations to provide organizations of varying sizes and risk profiles with prescriptive implementation requirements. In doing so, the HITRUST CSF accomplishes the following:

- Establishes a single benchmark for organizations to facilitate internal and external measurements that incorporates the requirements of applicable standards and regulations including ISO, PCI, COBIT, HIPAA, HITECH, and NIST
- Increases trust and transparency among business partners and consumers by incorporating best practices, building confidence, and streamlining interactions across the industry

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

- Obtains industry consensus on the most effective way to address information security while containing the cost of compliance and the number, complexity, and degree of variation in security audits or reviews

By engaging HITRUST, implementing the CSF, and getting assessed, organizations will have a common security baseline and mechanism for communicating validated security controls to a variety of constituents without redundant, overlapping, frequent, and costly audits.

The following HITRUST document categories located under the Downloads section on the HITRUST Alliance Website:

- MyCSF
- CSF Assurance
- CSF Assessors
- HITRUST 2014
- CSF, RMF and Related Documents
- C3 and Cyber Threat

Specific documents that should be referenced for additional program background and use of the CSF include:

- HITRUST CSF Assurance Program Requirements
- HITRUST CSF Assessment Methodology
- HITRUST CSF Standards and Regulations Cross-Reference
- HITRUST CSF Assessor Requirements
- HITRUST Risk Analysis Guide for HITRUST Organizations

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Organization of the CSF

HIPAA is not prescriptive, which makes it open to interpretation and difficult to apply. Organizations must necessarily reference additional standards for guidance on how to implement the requirements specified by HIPAA. It is also not the only set of security requirements healthcare organizations need to address (e.g., PCI, state, business partner requirements).

The HITRUST Common Security Framework (CSF) is not a new standard. The CSF is a framework that normalizes the security requirements of healthcare organizations including federal legislation (e.g., ARRA and HIPAA), federal agency rules and guidance (e.g., NIST, FTC and CMS), state legislation (e.g., Nevada, Massachusetts and Texas), and industry frameworks (e.g., PCI and COBIT), so the burden of compliance with the CSF is no more than what already applies to healthcare organizations. The CSF was built to simplify these issues by providing direction for security tailored to the needs of the organization. The CSF is the only framework built to provide scalable security requirements based on the different risks and exposures of organizations in the industry.

The HITRUST CSF also supports the requirements for an industry-specific cybersecurity program outlined in the new Framework for Improving Critical Infrastructure Cybersecurity, developed as part of a public-private sector partnership between NIST and representatives from multiple critical infrastructure industries. The NIST framework provides broad guidance to critical infrastructure industries on the development and implementation of industry, sector, or organizational-level risk management programs that are holistic, based upon a common set of principles, and can be communicated with stakeholders regardless of organization, sector or industry. The HITRUST CSF, along with the CSF Assurance Program and associated methodologies and tools, provides a model implementation of the Cybersecurity Framework for the healthcare industry.

Key Components

The HITRUST CSF includes but is not limited to the following major components:

- **Information Security Implementation Requirements:** Certifiable and best-practice based specifications that include sound security governance practices (e.g., organization and policies) and security control practices (e.g., people, process, and technology) that scale according to the type, size, and complexity of each organization.
- **Standards and Regulations Mapping:** A reconciliation of the framework to common and unique aspects of generally adopted standards.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

The CSF includes the control objectives and control specifications based on the ISO/IEC 27001:2005 and ISO/IEC 27002:2005 standards. These guidelines from ISO were enhanced, leveraging the NIST 800-series framework documents, ISO/IEC 27799:2008 Health Informatics (guidance for information security management for healthcare organizations using ISO/IEC 27002), HIPAA Omnibus, PCI, COBIT, State requirements, and the experience and best practices of the HITRUST community.

The CSF normalizes all of this material into the requirements of the CSF, referencing the applicable standards and regulations as authoritative sources.

Control Categories

The CSF contains 14 security Control Categories comprised of 45 Control Objectives and 149 Control Specifications[1]. The CSF Control Categories, accompanied with the number of objectives and specifications, are:

0. Information Security Management Program (1, 1)
1. Access Control (7, 25)
2. Human Resources Security (4, 9)
3. Risk Management (1, 4)
4. Security Policy (1, 2)
5. Organization of Information Security (2, 11)
6. Compliance (3, 10)
7. Asset Management (2, 5)
8. Physical and Environmental Security (2, 13)
9. Communications and Operations Management (10, 32)
10. Information Systems Acquisition, Development and Maintenance (6, 13)
11. Information Security Incident Management (2, 5)
12. Business Continuity Management (1, 5)
13. Privacy Practices (3, 14)

It should be noted that the order of the control categories does not necessarily imply their importance, and all security controls should be considered important. However, the full implementation of an Information Security Management Program (Control Category 0) will allow an organization to better identify and understand their needs, objectives, and requirements for information security. This will in turn allow the organization to identify,

[1] HITRUST has updated its proposed new Control Category, 13.0 Privacy Practices, in the 2015 CSF v7.0 release to support a broader range of covered entity privacy programs in addition to its original support for Texas certification of the HIPAA Privacy Rule and other legislative and regulatory requirements outlined in Title 1 Texas Administrative Code § 390.2.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

define, and manage the processes and resources that are necessary for the implementation of the rest of the CSF.

Each control category contains the following:

- **Control Reference**: Control number and title.
- **Control Objective**: Statement of the desired result or purpose of what is to be achieved.
- **Control Specification:** The policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature, to meet the control objective.

Each control contains the following:

- **Risk Factor:** Listing of organizational, system, and regulatory factors that drive requirements for a higher level of control.
- **Implementation Requirement:** Detailed information to support the implementation of the control and meeting the control objective. Up to three (3) levels of requirements are defined based on the relevant organizational or system applicability factors. Level 1 provides the minimum baseline control requirements as determined by the industry. Each additional level encompasses the lower levels and includes additional requirements commensurate with increasing levels of risk.
- **Control Assessment Guidance:** Guidance in performing an assessment is included in the online version of the CSF, available as Illustrative Procedures in MyCSF, to provide clarity to both assessor organizations and those adopting the CSF when validating the security controls implemented by the organization against the requirements of the CSF (e.g., by compliance or internal audit). This guidance includes examination of documentation, interviewing of personnel, and testing of technical implementation. These procedures exist solely as guidance and are neither comprehensive nor required for assessments submitted to HITRUST for review.
- **Standard Mapping:** The cross-reference between each Implementation Requirement Level and the requirements and controls of other common standards and regulations.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Implementation Requirement Levels

The HITRUST CSF follows a risk-based approach by practically applying security resources commensurate with level of risk or as required by applicable regulations or standards. HITRUST addresses risk by defining multiple levels of implementation requirements, which increase in restrictiveness. Three levels of requirements are defined based on organizational, system, or regulatory risk factors. Level 1 is considered the baseline level of control requirements as determined by the industry; each subsequent level encompasses the lower levels and includes additional requirements commensurate with increased risk.

Segment Specific Requirements

Certain industry segments have specific requirements that do not apply to other segments or would not be considered reasonable and appropriate from a general controls perspective. For example, the HITRUST CSF contains a CMS Contractors category which outlines additional controls and requirements that contractors of CMS will need to implement in addition to those controls listed in the Implementation Requirement Levels. An example of this would be requiring specific authorization or approval from the CMS CIO. New for 2015 are segment specific requirements for Health Insurance Exchanges (HIXs) and Federal Agencies and Contractors.

Risk Factors

The HITRUST CSF defines a number of organizational, system, and regulatory risk factors that increase the inherent risk to an organization or system, necessitating a higher level of control.

- **Organizational Factors:** The Organizational Factors are defined based on the size of the organization and complexity of the environment as follows:
    - Volume of business
        - Health Plan / Insurance – Number of Covered Lives
        - Medical Facilities / Hospital – Number of Licensed Beds
        - Pharmacy Companies – Number of Prescriptions Per Year
        - Physician Practice – Number of Visits Per Year
        - Third Party Processor – Number of Records Processed Per Year
        - Biotech Companies – Annual Spend on Research and Development
        - IT Service Provider / Vendor – Number of Employees
        - Health Information Exchange – Number of Transactions Per Year
    - Geographic scope
        - State
        - Multi-state
        - Off-shore (outside U.S.)

- **Regulatory Factors:** The regulatory factors are defined based on the compliance requirements applicable to an organization and systems in its environment:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

- Subject to PCI Compliance
- Subject to FISMA Compliance
- Subject to FTC Red Flags Rules
- Subject to the State of Massachusetts Data Protection Act
- Subject to the State of Nevada Security of Personal Information Requirements
- Subject to the State of Texas Medical Records Privacy Act
- Subject to Joint Commission Accreditation
- Subject to CMS Minimum Security Requirements (High-level Baseline)
- Subject to MARS-E Requirements
- Subject to FTI Requirements

- **System Factors:** The system factors are defined considering various system attributes that would increase the likelihood or impact of a vulnerability being exploited. These factors are to be assessed for each system or system grouping to determine the associated level of control.

  - Stores, processes, or transmits PHI
  - Accessible from the Internet
  - Accessible by a third party
  - Exchanges data with a third party/business partner
  - Publicly accessible
  - Mobile devices are used
  - Connects with or exchanges data with a Health Information Exchange (HIE)
  - Number of interfaces to other systems
  - Number of users
  - Number of transactions per day

For a system to increase from a Level 1 Implementation Requirement to a Level 2 or 3 Implementation Requirement, the system must be processing ePHI **AND** include at least one of the other system factors associated with the control. For example, if a system is accessible from the Internet, exchanges data with a business partner, and has the Level 2 threshold number of users, but DOES NOT process ePHI, that system is only required to meet the Level 1 Implementation Requirements. However, if another system DOES process ePHI AND is accessible from the Internet, then that system must meet an Implementation Requirement level higher than Level 1.

If a control contains more than one category of factors, the organization must adhere to the highest level of Implementation Requirements that the factors drive it to. For example, if a health plan is at the Level 2 threshold for a control based on their number of covered lives but must also be FISMA compliant (implementing and adhering to the controls of NIST), the

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

organization must implement the Level 3 requirements of the CSF since FISMA is a Level 3 Regulatory Factor for that control.

Alternate Controls

With the diverse nature of today's information systems, organizations may have systems in their environments that do not have the capability to meet the CSF requirements. Consequently, organizations may need to employ alternate security controls to mitigate risk or compensate for a system control failure. HITRUST defined the alternate control process to provide the means for organizations to meet CSF requirements by deploying alternate controls as a substitute for control weaknesses. An alternate control is defined as a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a security control for the Level 1, 2 or 3 Implementation Requirements described in the CSF, and provides equivalent or comparable protection for an information system.

An alternate control for a system, application or device may be employed by an organization only under the following conditions:

1. The organization selects the alternate control(s) from the CSF, or if an appropriate alternate control is not available, the organization proposes a suitable alternate control,
2. The organization provides a complete and convincing rationale to HITRUST addressing how the alternate control provides an equivalent security capability or level of protection for the information system, why the related minimum security control could not be employed, and information about the associated application or device,
3. The HITRUST Alternate Controls Committee reviews and approves the alternate control, and
4. The organization assesses and formally accepts the risk associated with employing the alternate control for the information system.

Evolution of the CSF

Fundamental to HITRUST's mission is the availability of a framework that provides the needed structure, clarity, functionality and cross-references to authoritative sources. HITRUST will ensure the CSF stays relevant and current to the needs of healthcare organizations based on the demands of the industry.

The CSF is designed to easily adapt based on changes to the healthcare environment to address and incorporate new standards and regulations. HITRUST has done extensive work in the past several releases to harmonize NIST and CMS requirements, track inconsistencies due to CMS's current reliance on an older release of NIST SP 800-53, and better align and eliminate redundant requirements within the framework. HITRUST will continue streamlining the framework based on continued analysis of the framework's implementation requirements and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

recommendations from the HITRUST Community, and plans to add the following sources in 2015 in an interim release (version 7.1):

- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) v3.0.1
- FedRAMP Security Controls Baseline Revision 4
- Homeland Security Cyber Resilience Review
- OCR Audit Protocol (harmonization) (held over from 2014 pending release of a new version to support audit of risk analysis and management)

CSF Assurance and MyCSF

HITRUST has developed a set of resources that allows an organization or CSF Assessor to efficiently assess the high risk areas of an environment, and/or apply the CSF's Risk Factors and Implementation Requirements to create a custom set of requirements tailored to an environment.

Organizations can now utilize this approach with a subscription to MyCSF.

This fully integrated, optimized, and powerful tool marries the content and methodologies of the HITRUST CSF and CSF Assurance program with the technology and capabilities of a governance, risk and compliance (GRC) tool. The new user-friendly MyCSF tool provides healthcare organizations of all types and sizes with a secure, web-based solution for accessing the CSF, performing assessments, managing remediation activities, and reporting and tracking compliance. Managed and supported by HITRUST, MyCSF provides organizations with up-to-date content, accurate and consistent scoring, reports validated by HITRUST and benchmarking data unavailable anywhere else in the industry, thus going far beyond what a traditional GRC tool can provide.

Through MyCSF organizations both large and small will maintain complete access to the CSF and authoritative sources, and now have the expanded benefit of a complete picture of not only their current state of compliance, but also the support and direction needed to track and manage their remediation efforts and report on their progress. Organizations will also be able to easily collaborate and work with HITRUST CSF Assessor organizations to share documentation already in the tool, incorporate necessary corrective action plans, and monitor progress.

In addition to the CSF, MyCSF incorporates several other "building blocks."

GRC Capabilities and Functionality: MyCSF provides organizations with a sophisticated and user-friendly tool in which to scope, assess and manage their environment. This new tool increases the efficiency with which organizations can implement and assess against the CSF by utilizing advanced workflows, custom criteria and notifications, and enhanced navigation and search tools. The tool also provides a user-friendly interface with the availability of dashboards

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

and reports and acts as a central repository for managing documents, corrective action plans, test plans, and system scoping.

CSF Assurance Methodology: The CSF Assurance program provides simplified and consistent compliance assessment and reporting against the HITRUST CSF and the authoritative sources it incorporates. This risk-based approach, which is governed and managed by HITRUST, is designed for the unique regulatory and business needs of the healthcare industry and provides organizations with an effective, standardized and streamlined assessment process to manage compliance. HITRUST CSF Assessments utilize a maturity level scoring model and risk ratings similar to PRISMA which provide more accurate, consistent and repeatable scoring, and help organizations to prioritize their remediation efforts. This is a more effective process than that used by other assessment approaches and toolkits which only support limited requirements and use classic checkbox approaches.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Implementing the CSF

The CSF is applicable to all healthcare organizations, of varying size and complexity, as the framework encompasses the fundamental security controls required by all relevant standards and regulations for which healthcare organizations are accountable.

The CSF incorporates the concept of an "Information Security Management System (ISMS)" from the ISO 27001 standard, and it describes the need for this detailed framework of controls when meeting the security objectives defined within the CSF. Industry experience and professional best practice principles indicate that ongoing information security and compliance is best met by the implementation of a formal management program.

Management Commitment

It is essential that an organization have the visible support and commitment of management before attempting to implement the CSF. Management's active involvement and support are essential for success and, at minimum, should include written and verbal statements of commitment to the importance of information security and recognition of its benefits. Management's clear understanding of purpose and their dedication to adopting the CSF will help manage expectations and minimize problems around implementation efforts.

Scope

The CSF applies to covered information (i.e., information that organizations deem necessary to secure, such as PHI) in all its aspects, regardless of the form the information takes (e.g., words and numbers, sound recordings, drawings, video and medical images), the means used to store it (e.g., printing or writing on paper or electronic storage), and the means used to transmit it (e.g., by hand, via fax, over computer networks or by post).

Organization

HITRUST allows organizations to break up their organization into auditable business units. An auditable business unit is defined as units or departments within the organization that can operate distinctly from one another. However, depending on the size and complexity of the organization, they may also represent geographical regions or associations with other (external) groups. Both distinctions are acceptable for the purposes of a CSF Validated or CSF Certified assessment.

Systems

The controls of the HITRUST CSF are designed to apply to all information systems irrelevant of classification or function. This includes all critical business systems and applications that store, process, or transmit covered information regardless of whether they are standalone systems or connected to the network. Supporting systems and applications are also within the scope of the CSF, including application software components, databases, operating systems, interfaces, tools, and servers. For the purposes of the CSF, there is a clear distinction between medical devices and systems; however, medical devices are within the scope of the assessment.
When implementing the CSF, it is appropriate to aggregate assets into one observation if the management, function, and environment allow the assets to be logically grouped.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Implementation

Implementation of the HITRUST CSF and assessment process will vary by organization in both time commitment and level of effort, as a product of the following factors:

- **Complexity of the environment**: Considering the size, amount of data processed, type of data processed, and sophistication of information systems technology;
- **Security maturity**: Considering the adequacy of people devoted to the security organization, processes defined and controls currently implemented; and
- **Resources**: Considering the number of resources available and budgetary constraints.

Critical Success Factors

In addition to management commitment and consistent application across systems and defined business units, experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

- A good understanding of the information security requirements, risk assessment, and risk management structure of the organization
- Effective marketing of information security to all managers, employees, and other parties to achieve awareness
- Distribution of guidance on information security policy and standards to all managers, employees and other parties
- Provisions to fund information security management activities
- Implementation of a measurement system that is used to evaluate performance in information security management and provide suggestions for improvement.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Primary Reference Material

For the HITRUST CSF, a broad base of U.S. federal regulations and international information protection standards and frameworks were used to ensure the CSF addresses all areas of InfoSec governance and control as it relates to the healthcare industry.
The CSF integrates and normalizes these different authoritative sources, incorporating key objectives under one umbrella framework that also provides prescriptive implementation requirements for meeting the objectives.

For the 2015 CSF v7, twenty-five (25) of the major information security related standards, regulations and frameworks are included as the major supporting references to ensure appropriate coverage, consistency, and alignment:

- 16 CFR Part 681 - Identity Theft Red Flags
- 201 CMR 17.00 – State of Massachusetts Data Protection Act
  Standards for the Protection of Personal Information of Residents of the Commonwealth
- Cloud Security Alliance (CSA) Cloud Controls Matrix Version 1.1
- CMS Information Security ARS 2013 v2
  CMS Minimum Security Requirements for High Impact Data
- COBIT 4.1 and 5
  Deliver and Support Section 5 – Ensure Systems Security
- *Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements*
- Federal Register 21 CFR Part 11
  Electronic Records; Electronic Signatures
- HIPAA – Federal Register 45 CFR Part 164, Subpart C
  HIPAA Administrative Simplification: Security Standards for the Protection of Electronic Protected Health Information (Security Rule)
- HIPAA – Federal Register 45 CFR Part 164, Subpart D
  HIPAA Administrative Simplification: Notification in the Case of Breach of Unsecured Protected Health Information (Breach Notification Rule)
- HIPAA – Federal Register 45 CFR Part 164, Subpart E
  HIPAA Administrative Simplification: Privacy of Individually Identifiable Health Information (Privacy Rule)
- IRS Publication 1075 v2014
  Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for protecting Federal Tax Returns and Return Information
- ISO/IEC 27001:2005
  Information technology - Security techniques - Information security management systems – Requirements
- ISO/IEC 27001:2013
  Information technology - Security techniques - Information security management systems – Requirements
- ISO/IEC 27002:2005

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Information technology — Security techniques — Code of practice for information security management

- ISO/IEC 27002:2013
  Information technology — Security techniques — Code of practice for information security controls
- ISO/IEC 27799:2008
  Health informatics — Information security management in health using ISO/IEC 27002
  Joint Commission (formerly the Joint Commission on the Accreditation of Healthcare Organizations, JCAHO)
- MARS-E v1.0
  Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement
- NIST Framework for Improving Critical Infrastructure Cybersecurity v1.0
  Framework Core - Subcategories
- NIST Special Publication 800-53 Revision 4 (Final), including Appendix J – Privacy Control Catalog
  Security Controls for Federal Information Systems and Organizations
- NIST Special Publication 800-66
  An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- NRS: Chapter 603A – State of Nevada
  Security of Personal Information
- Payment Card Industry (PCI) Data Security Standard Version 3.0
  Information Management (IM) Standards, Elements of Performance, and Scoring
- Texas Health and Safety Code § 181 – State of Texas (aka "TX HB 300")
  Texas Medical Records Privacy Act
- Title 1 Texas Administrative Code § 390.2 – State of Texas
  Standards Relating to the Electronic Exchange of Health Information

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Questions and Comments on the CSF

HITRUST encourages organizations to provide their comments to ensure the CSF continues to evolve as the most relevant framework for information security in the healthcare industry. Organizations who wish to provide HITRUST with feedback on the CSF can do so by sending their comments via email to csfcomments@hitrustalliance.net. The form contains instructions and a template to document your comments. Any questions about use or distribution of the CSF should be sent to notices@hitrustalliance.net.

About HITRUST

The Health Information Trust Alliance or HITRUST was born out of the belief that information security is critical to the broad adoption, utilization and confidence in health information systems, medical technologies and electronic exchanges of health information, and in turn realizing the promise for quality improvement and cost containment in America's healthcare system.

COPYRIGHT (c) 2010-2015 HITRUST

This document has been provided AS IS, without warranty. HITRUST and its agents and affiliates are not responsible for content of third parties.

HITRUST and CSF are trademarks of HITRUST Alliance LLC. HITRUST CENTRAL is a trademark of HITRUST Service Corporation. All other marks contained herein are the property of their respective owners.

Control Category: 0.0 - Information Security Management Program

Objective Name: 0.01 Information Security Management Program

Control Objective:	To implement and manage an Information Security Management Program.

Control Reference: 0.a Information Security Management Program

Control Specification:	An Information Security Management Program (ISMP) shall be defined in terms of the characteristics of the business, and established and managed including monitoring, maintenance and improvement. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Audit and Accountability Documentation and Records IT Organization and Management Roles and Responsibilities Monitoring Planning Policies and Procedures Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	An Information Security Management Program (ISMP) shall be documented that addresses the overall Security Program of the organization. Management support for the ISMP shall be demonstrated through signed acceptance or approval by management. The ISMP shall consider all the HITRUST Control Objectives and document any excluded control domains and the reasons for their exclusion. The ISMP shall be updated at least annually or when there are significant changes in the environment.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Control Standard Mapping:	• COBIT 4.1 DS5.2 • COBIT 5 APO13.02 • CSA IS-01 • HIPAA § 164.308(a)(1)(i) • HIPAA § 164.308(a)(1)(ii)(A) • HIPAA § 164.308(a)(1)(ii)(B) • HIPAA § 164.308(a)(8) • HIPAA § 164.316(b)(1) • HIPAA § 164.316(b)(2)(iii) • ISO/IEC 27001-2005 4.1 • ISO/IEC 27001:2013 4.4 • NIST Cybersecurity Framework ID.GV-4 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Geographic Scope: Multi-state, BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: The organization shall formally establish, implement, operate, monitor, review, maintain and improve the ISMP. The ISMP shall be formally documented, and such records shall be protected, controlled and retained according to federal, state and organizational requirements. The ISMP shall incorporate a Plan, Do, Check, Act (PDCA) cycle for continuous improvement in the ISMP, particularly as information is obtained that could improve the ISMP, or indicates any shortcomings of the ISMP.
Level 2 Control Standard	• CMSRs 2013v2 PM-1 (HIGH) • COBIT 4.1 DS5.5

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Mapping:	• COBIT 5 DSS05.07 • ISO/IEC 27001-2005 4.2.1 • ISO/IEC 27001-2005 4.2.2 • ISO/IEC 27001-2005 4.2.3 • ISO/IEC 27001-2005 4.2.4 • ISO/IEC 27001-2005 4.3.1 • ISO/IEC 27001-2005 4.3.2 • ISO/IEC 27001-2005 4.3.3 • ISO/IEC 27001:2013 4.3 • ISO/IEC 27001:2013 5.1(a) • ISO/IEC 27001:2013 5.2 • ISO/IEC 27001:2013 5.3 • ISO/IEC 27001:2013 6.1.1(d) • ISO/IEC 27001:2013 6.1.1(e)(1) • ISO/IEC 27001:2013 6.1.1(f) • ISO/IEC 27001:2013 6.1.2 • ISO/IEC 27001:2013 6.1.3 • ISO/IEC 27001:2013 6.2(e) • ISO/IEC 27001:2013 7.1 • ISO/IEC 27001:2013 7.4 • ISO/IEC 27001:2013 7.5.1(a) • ISO/IEC 27001:2013 7.5.2 • ISO/IEC 27001:2013 7.5.3 • ISO/IEC 27001:2013 8.1 • ISO/IEC 27001:2013 8.2 • ISO/IEC 27001:2013 8.3 • ISO/IEC 27001:2013 9.1 • ISO/IEC 27001:2013 9.2 • ISO/IEC 27001:2013 9.3(b) • ISO/IEC 27001:2013 9.3(f) • ISO/IEC 27001:2013 10.1(c) • ISO/IEC 27001:2013 10.2 • ISO 27799-2008 6.4 • ISO 27799-2008 6.5 • ISO 27799-2008 6.6 • ISO 27799-2008 6.7 • MARS-E v1 PM-1 • NIST Cybersecurity Framework PR.IP-7 • NIST SP 800-53 R4 PM-1 • (State of Mass.) 201 CMR 17.03(1)

Level 3 Implementation Requirements

Level 3 Organizational	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year,

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Geographic Scope: Off-Shore (Outside U.S.), Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements, Subject to State of Massachusetts Data Protection Act
Level 3 Implementation:	Level 2 plus: Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMP. The organization shall determine and provide the resources needed to establish, implement, operate, monitor, review, maintain and improve an ISMP. The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMP are competent to perform the required tasks. The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMP objectives. The organization shall conduct internal ISMP audits at planned intervals to determine the continuing suitability, adequacy and effectiveness of the program. Management shall review the organization's ISMP at planned intervals (at least once a year) to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the ISMP, including the information security policy and information security objectives. The results of the reviews shall be clearly documented and records maintained. The organization shall continually improve the effectiveness of the ISMP through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 PM-2 (HIGH) • CMSRs 2013v2 PM-3 (HIGH) • CMSRs 2013v2 PM-4 (HIGH) • CMSRs 2013v2 PM-6 (HIGH) • CMSRs 2013v2 PM-9 (HIGH) • CMSRs 2013v2 PM-13 (HIGH)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• IRS Pub 1075 v2014 9.3.18.1 • ISO/IEC 27001-2005 5.1 • ISO/IEC 27001-2005 5.2.1 • ISO/IEC 27001-2005 5.2.2 • ISO/IEC 27001-2005 6 • ISO/IEC 27001-2005 7.1 • ISO/IEC 27001-2005 7.2 • ISO/IEC 27001-2005 7.3 • ISO/IEC 27001-2005 8.1 • ISO/IEC 27001-2005 8.2 • ISO/IEC 27001-2005 8.3 • ISO/IEC 27001:2013 4.1 • ISO/IEC 27001:2013 4.2(b) • ISO/IEC 27001:2013 5.1(c) • ISO/IEC 27001:2013 5.1(d) • ISO/IEC 27001:2013 5.1(e) • ISO/IEC 27001:2013 5.1(f) • ISO/IEC 27001:2013 5.1(g) • ISO/IEC 27001:2013 6.1.1 • ISO/IEC 27001:2013 6.2 • ISO/IEC 27001:2013 7.2 • ISO/IEC 27001:2013 7.3(b) • ISO/IEC 27001:2013 7.3(c) • ISO/IEC 27001:2013 9.3 • ISO/IEC 27001:2013 10.1(b) • ISO/IEC 27001:2013 10.1(d) • ISO/IEC 27001:2013 10.1(e) • ISO/IEC 27001:2013 10.1(g) • MARS-E v1 PM-2 • MARS-E v1 PM-3 • MARS-E v1 PM-4 • MARS-E v1 PM-6 • MARS-E v1 PM-9 • MARS-E v1 PM-13 • NIST SP 800-53 R4 PM-2 • NIST SP 800-53 R4 PM-3 • NIST SP 800-53 R4 PM-4 • NIST SP 800-53 R4 PM-6 • NIST SP 800-53 R4 PM-9 • NIST SP 800-53 R4 PM-13 • (State of Mass.) 201 CMR 17.03(2)(b) • (State of Mass.) 201 CMR 17.03(2)(h) • (State of Mass.) 201 CMR 17.03(2)(i)

Health Insurance Exchange Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Health Insurance Exchanges:	The organization provides sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Category: 01.0 - Access Control

Objective Name: 01.01 Business Requirement for Access Control

Control Objective:	To control access to information, information assets, and business processes based on business and security requirements.

Control Reference: 01.a Access Control Policy

Control Specification:	An access control policy shall be established, documented, and reviewed based on business and security requirements for access. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Audit and Accountability Authentication Authorization Policies and Procedures User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to Joint Commission Accreditation, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	Access control rules shall account for and reflect the organization's policies for information dissemination and authorization, and these rules shall be supported by formal procedures and clearly defined responsibilities. Access control rules and rights for each user or group of users shall be clearly stated. Access controls are both logical and physical and these shall be considered together. Users and service providers shall be given a clear statement of the business requirements to be met by access controls. Specifically the access control program shall take account of the following: i. security requirements of individual business applications;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	ii. information dissemination and authorization (e.g., need-to-know, need to share, and least privilege principles; security levels; and classification of information.) iii. relevant legislation and any contractual obligations regarding protection of access to data or services; iv. standard user access profiles for common job roles in the organization; v. requirements for formal authorization of access requests; vi. requirements for emergency access; vii. requirements for periodic review of access controls; and viii. removal of access rights. The organization shall develop and disseminate/communicate a formal access control program (e.g., through policies and procedures) and review and update the program annually.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-1 (HIGH) • CSA IS-07 • HIPAA § 164.308(a)(3)(i) • HIPAA § 164.308(a)(3)(ii)(a) • HIPAA § 164.308(a)(4)(i) • HIPAA § 164.308(a)(4)(ii)(B) • HIPAA § 164.312(a)(1) • IRS Pub 1075 v2014 9.3.1.1 • JCAHO IM.02.01.03, EP 1 • MARS-E v1 AC-1 • NIST Cybersecurity Framework ID.GV-3 • NIST SP 800-53 R4 AC-1 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Implementation:	Level 1 plus: All information related to the business applications and the risks the information is facing shall be identified. The access control and information classification policies of different systems and networks shall be consistent. Access rights shall be managed in a distributed and networked environment ensuring all types of connections available are recognized. Access control roles (e.g., access request, access authorization, access administration) shall be segregated.
Level 2 Control Standard Mapping:	• ISO/IEC 27002-2005 11.1.1 • ISO/IEC 27002-2013 A.9.1.1 • ISO 27799-2008 7.8.1.2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Objective Name: 01.02 Authorized Access to Information Systems

Control Objective:	To ensure authorized user accounts are registered, tracked and periodically validated to prevent unauthorized access to information systems.

Control Reference: 01.b User Registration

Control Specification:	There shall be a formal documented and implemented user registration and de-registration procedure for granting and revoking access. *Required for HITRUST Certification 2015
Factor Type:	System
Topics:	Authorization Monitoring Policies and Procedures

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act, Subject to Joint Commission Accreditation; Subject to FTI Requirements
Level 1 Implementation:	User registration and de-registration shall formally address establishing, activating, modifying, reviewing, disabling, and removing accounts. Account types shall be identified (individual, shared/group, system, application, guest/anonymous, emergency and temporary) and conditions for group and role membership shall be established. Access to the information systems shall be granted based on a valid need-to-know/need-to-share that is determined by assigned official duties and intended system usage. Access granted shall satisfy all personnel security criteria. Proper identification shall be required for requests to establish information system accounts and approval of all such requests. Guest/anonymous, shared/group, emergency and temporary accounts shall be specifically authorized and use monitored. Unnecessary accounts shall be removed, disabled or otherwise secured. Account managers shall be notified when users are terminated or transferred, their information system usage or need-to-know/need-to-share changes, or when accounts (including shared/group, emergency, and temporary accounts) are no longer required. Shared/group account credentials shall be modified when users are removed from the group. The access control procedure for user registration and de-registration shall: i. communicate password procedures and policies to all users who have system access ii. check that the user has authorization from the system owner for the use of the information system or service; iii. separate approval for access rights from management; iv. check that the level of access granted is appropriate to the business purpose and is consistent with organizational security policy (e.g., it is consistent with sensitivity and risks associated with the information and/or information system, it does not compromise segregation of duties); v. give users a written statement of their access rights; vi. require users to sign statements indicating that they understand the conditions of access;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	vii. ensure service providers do not provide access until authorization procedures have been completed; viii. ensure default accounts are removed and/or renamed; ix. maintain a formal record of all persons registered to use the service; x. remove or block critical access rights of users who have changed roles or jobs or left the organization immediately and remove or block non-critical access within 24 hours; and xi. automatically remove or disable accounts that have been inactive for a period of sixty (60) days or more.
Level 1 Control Standard Mapping:	• COBIT 4.1 DS5.3 • CMSRs 2013v2 AC-2 (HIGH) • CMSRs 2013v2 AC-2(3) (HIGH) • CMSRs 2013v2 IA-1 (HIGH) • CMSRs 2013v2 IA-4 (HIGH) • CMSRs 2013v2 IA-5 (HIGH) • CSA IS-08 • HIPAA § 164.312(a)(2)(i) • HIPAA § 164.312(a)(2)(ii) • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(3)(ii)(B) • HIPAA § 164.308(a)(3)(ii)(C) • HIPAA § 164.308(a)(4)(i) • HIPAA § 164.308(a)(4)(ii)(B) • HIPAA § 164.308(a)(4)(ii)(C) • HIPAA § 164.308(a)(5)(ii)(C) • HIPAA § 164.308(a)(5)(ii)(D) • HIPAA § 164.312(d) • IRS Pub 1075 v2014 9.3.1.2 • IRS Pub 1075 v2014 9.3.7.1 • IRS Pub 1075 v2014 9.3.7.4 • IRS Pub 1075 v2014 9.3.7.5 • IRS Pub 1075 v2014 9.3.7.6 • JCAHO IM.02.01.03, EP 5 • MARS-E v1 AC-2 • MARS-E v1 AC-2(3) • MARS-E v1 IA-1 • MARS-E v1 IA-4 • MARS-E v1 IA-5 • NIST Cybersecurity Framework DE.CM-3 • NIST Cybersecurity Framework PR.AC-1 • NIST Cybersecurity Framework PR.AC-4 • NIST SP 800-53 R4 AC-2 • NIST SP 800-53 R4 AC-2(3) • NIST SP 800-53 R4 IA-1 • NIST SP 800-53 R4 IA-4 • NIST SP 800-53 R4 IA-5

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• • PCI DSS v3 8.1.2 • PCI DSS v3 8.1.3 • PCI DSS v3 8.1.4 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.04(2)(a) • (State of Mass.) 201 CMR 17.04(2)(b) • (State of Mass.) 201 CMR 17.04(1)(d) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Accessible from the Internet: Yes
Level 2 Regulatory Factors:	Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: The organization shall require that the registration process to receive hardware administrative tokens and credentials used for two (2)-factor authentication be verified in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor or other individual defined in an applicable security plan). Organizations shall not use group, shared or generic accounts and passwords.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 IA-5(3) (HIGH) • COBIT 4.1 DS5.4 • COBIT 5 DSS05.03 • COBIT 5 DSS05.04 • ISO/IEC 27002-2005 11.2.1 • ISO/IEC 27002-2013 A.9.2.1 • ISO/IEC 27002-2013 A.9.2.2 • ISO 27799-2008 7.8.2.1 • MARS-E v1 IA-5(3) • NIST SP 800-53 R4 IA-5(3) • NRS 603A.215.1 • PCI DSS v3 8.5

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements
Level 3 Implementation:	Level 2 plus: The organization shall employ automated mechanisms to support the management of information system accounts. In addition to assigning a unique ID and password, at least one of the following methods shall be employed to authenticate all users: i. token devices (e.g., SecureID, certificates, or public key); or ii. biometrics. The organization shall automatically disable emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed thirty (30) days.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 AC-2(1) (HIGH) • CMSRs 2013v2 AC-2(2) (HIGH) • CMSRs 2013v2 AC-2(13) (HIGH) • MARS-E v1 AC-2(2) • NIST SP 800-53 R4 AC-2(1) • NIST SP 800-53 R4 AC-2(2) • PCI-DSS v3 8.2

CMS Contractor Requirements

CMS Contractors	The organization disables accounts of users posing a significant risk within sixty (60) minutes of discovery of the risk. Disabled accounts shall be deleted during the annual re-certification process.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	Disabled accounts shall be deleted during the annual re-certification process.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 01.c Privilege Management

Control Specification:	The allocation and use of privileges to information systems and services shall be restricted and controlled. Special attention shall be given to the allocation of privileged access rights, which allow users to override system controls.
Factor Type:	System
Topics:	Authorization User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act, Subject to Joint Commission Accreditation
Level 1 Implementation:	The allocation of privileges for all systems and system components shall be controlled through a formal authorization process. The access privileges associated with each system product (e.g., operating system, database management system and each application) and the users to which they need to be allocated shall be identified. Privileges shall be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (i.e. the minimum requirement for their functional role, e.g., user or administrator, only when needed). At a minimum, the organization explicitly authorizes access to the following list of security functions (deployed in hardware, software, and firmware) and security-relevant information: i. Setting/modifying audit logs and auditing behavior; ii. Setting/modifying boundary protection system rules; iii. Configuring/modifying access authorizations (i.e., permissions, privileges); iv. Setting/modifying authentication parameters; and v. Setting/modifying system configurations and parameters. An authorization process and a record of all privileges allocated shall be maintained.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-6 (HIGH) • CMSRs 2013v2 AC-6(1) (HIGH) • COBIT 4.1 DS5.4

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• COBIT 5 DSS05.04 • CSA IS-08 • HIPAA § 164.308(a)(3)(i) • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(4)(i) • HIPAA § 164.308(a)(4)(ii)(A) • HIPAA § 164.308(a)(4)(ii)(B) • HIPAA § 164.308(a)(4)(ii)(C) • HIPAA § 164.308(a)(5)(ii)(C) • HIPAA § 164.312(a)(1) • HIPAA § 164.312(a)(2)(i) • HIPAA § 164.312(a)(2)(ii) • IRS Pub 1075 v2014 9.3.1.6 • ISO/IEC 27002-2005 11.2.2 • ISO/IEC 27002-2013 A.9.2.3 • JCAHO IM.02.01.03, EP 5 • MARS-E v1 AC-6 • NIST Cybersecurity Framework PR.AC-4 • NIST SP 800-53 R4 AC-6 • NIST SP 800-53 R4 AC-6(1) • PCI DSS v3 7.1 • PCI DSS v3 7.1.1 • PCI DSS v3 7.1.4 • PCI DSS v3 7.2.1 • PCI DSS v3 7.2.2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.04(2)(a) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Accessible from the Internet: Yes, Number of Users: > 500, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: Role-based access control shall be implemented and capable of mapping each user to one or more roles, and each role to one or more system functions.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The development and use of system routines shall be promoted to avoid the need to grant privileges to users. The development and use of programs which avoid the need to run with elevated privileges shall be promoted. Elevated privileges shall be assigned to a different user ID from those used for normal business use. All users shall access privileged services in a single role (users registered with more than one role shall designate a single role during each system access session). The use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) shall be minimized. Access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware shall be restricted. Security relevant information shall be restricted to explicitly authorized individuals. The organization shall facilitate information sharing by enabling authorized users to determine whether access authorizations assigned to business partners match the access restrictions on information for specific circumstances in which user discretion is allowed. Also employs manual processes or automated mechanisms to assist users in making information sharing/collaboration decisions. The access control system for the system components storing, processing or transmitting covered information shall be set with a default "deny-all" setting.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-2 (HIGH) • CMSRs 2013v2 AC-6(2) (HIGH) • CMSRs 2013v2 AC-21 • IRS Pub 1075 v2014 9.3.1.2 • IRS Pub 1075 v2014 9.3.1.6 • IRS Pub 1075 v2014 9.3.1.16 • ISO 27799-2008 7.8.2.2 • MARS-E v1 AC-2 • MARS-E v1 AC-6(2) • NIST Cybersecurity Framework PR.DS-5 • NIST SP 800-53 R4 AC-2 • NIST SP 800-53 R4 AC-6(2) • NIST SP 800-53 R4 AC-21 • PCI DSS v3 7.1.2 • PCI DSS v3 7.1.3 • PCI DSS v3 7.2 • PCI DSS v3 7.2.3

Level 3 Implementation Requirements

Level 3 Organizational	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 3 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 5,500, Number of Transactions Per Day: > 85,000, Number of Interfaces to Other Systems: > 75
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: The organization shall limit authorization to privileged accounts on information systems to a pre-defined subset of users and shall track and monitor privileged role assignments. The organization shall audit the execution of privileged functions on information systems and ensure information systems prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards (e.g., IDS/IPS or malicious code protection mechanisms). All file system access not explicitly required for system, application, and administrator functionality shall be disabled. Contractors shall be provided with minimal system and physical access, and shall agree to and support the organization's security requirements. The contractor selection process shall assess the contractor's ability to adhere to and support the organization's security policy and procedures. The organization ensure only authorized users are permitted to access those files, directories, drives, workstations, servers, network shares, ports, protocols, and services that are expressly required for the performance of the users' job duties.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 AC-6(3) (HIGH) • CMSRs 2013v2 AC-6(5) (HIGH) • CMSRs 2013v2 AC-6(9) (HIGH) • CMSRs 2013v2 AC-6(10) (HIGH) • IRS Pub 1075 v2014 9.3.1.6 • IRS Pub 1075 v2014 9.3.10.6 • IRS Pub 1075 v2014 9.4.2 (E.10) • IRS Pub 1075 v2014 9.4.9 • IRS Pub 1075 v2014 9.4.11 • IRS Pub 1075 v2014 9.4.13 • MARS-E v1 SI-3(3) • MARS-E v1 SI-4(6) • NIST Cybersecurity Framework DE.CM-3 • NIST SP 800-53 R4 AC-6(5) • NIST SP 800-53 R4 AC-6(9) • NIST SP 800-53 R4 AC-6(10) • NRS 603A.215.1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

CMS Contractor Requirements

CMS Contractors:	All system and removable media boot access shall be disabled unless it is explicitly authorized by the organizational CIO for compelling operational needs. If system and removable media boot access is authorized, boot access is password protected. The organization authorizes network access to privileged commands only for defined compelling operational needs (defined in the applicable security plan) and documents the rationale for such access in the security plan for the information system.

FTI Requirements

FTI Custodians:	Business roles and rules shall be imbedded at either the authentication level or application level. In either case, the agency must ensure that only authorized employees or contractors (as allowed by statute) of the agency receiving the information have access to FTI. The agency must restrict the sharing/re-disclosure of FTI to only those authorized in IRC 6103 and as approved by the Office of Safeguards. The organization shall password-protect system initialization (boot) settings. The agency must restrict the use of information system media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, CDs, DVDs) on information systems that receive, process, store, or transmit FTI using physical or automated controls. Multifunction Device (MFD) access enforcement controls must be configured correctly, including access controls for file shares, administrator and non-administrator privileges, and document retention functions. To use FTI in a SAN environment, the agency must ensure: i. access controls are implemented and strictly enforced for all SAN components to limit access to disks containing FTI to authorized users; and ii. fibre channel devices must be configured to authenticate a. other devices with which they communicate in the SAN and b. administrator connections. The least privilege principle must be strictly enforced in a virtualized environment. To use a virtual environment that receives, processes, stores, or transmits FTI, programs that control the hypervisor should be secured and restricted to authorized administrators only.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Health Information Exchange Requirements

Health Information Exchanges:	HIEs shall, for all employees and for all employees of connecting organizations, define and assign roles to each individual with access to the HIE. The roles shall be based on the individual's job function and responsibilities. The roles shall specify the type of access and level of access.

PCI-DSS Requirements

PCI Data:	A service provider shall protect each organization's hosted environment and data by: i. ensuring that each organization only runs processes that only have access to that organization's cardholder data environment , and ii. restricting each organization's access and privileges to only its own cardholder data environment.

Control Reference: 01.d User Password Management

Control Specification:	Passwords shall be controlled through a formal management process. *Required for HITRUST Certification 2015
Factor Type:	System
Topics:	Authentication Authorization Cryptography User Access Password Management

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act,
Level 1 Implementation:	The following controls shall be implemented to maintain the security of passwords: i. passwords shall be prohibited from being displayed when entered; ii. passwords shall be changed whenever there is any indication of

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	possible system or password compromise; and iii. user identity shall be verified before performing password resets. The allocation of passwords shall be controlled through a formal management process: i. the use of third parties or unprotected (clear text) electronic mail messages shall be avoided; ii. users shall acknowledge receipt of passwords; iii. default vendor passwords shall be altered following installation of systems or software; iv. when users are required to maintain their own passwords they shall be provided initially with a secure temporary password, which they are forced to change immediately; v. temporary passwords shall be changed at the first log-on; vi. temporary passwords shall be given to users in a secure manner; vii. passwords shall be changed at least every 90 days or based on the number of accesses; viii. passwords for privileged accounts shall be changed at least every 60 days; ix. passwords shall require at least eight (8) characters which are: a. easy to remember; b. not based on anything somebody else could easily guess or obtain using person related information (e.g., names, telephone numbers, and dates of birth etc.); c. not vulnerable to dictionary attack (do not consist of words included in dictionaries); d. free of consecutive identical characters; and e. a combination of alphabetic, upper and lower case characters, numbers, and special characters (combination of any three [3] of the above four [4] listed is acceptable). x. passwords shall be prohibited from being reused for at least four (4) generations for users or six (6) generations for privileged users; and xi. at least four (4) changed characters are changed when new passwords are created. Alternatively, passwords/phrases must have a strength (entropy) at least equivalent to the parameters specified above.
Level 1 Control Standard Mapping:	• CSA SA-02 • HIPAA § 164.308(a)(5)(ii)(D) • NIST Cybersecurity Framework PR.AC-1 • PCI DSS v3 2.1 • PCI DSS v3 8.2.2 • PCI DSS v3 8.2.6 • PCI DSS v3 8.2.3 • PCI DSS v3 8.2.5 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• Phase 1 CORE 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.1 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.04(1)(b) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Accessible from the Internet: Yes, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The following controls shall be implemented to maintain the security of passwords: i. passwords shall be protected from unauthorized disclosure and modification when stored and transmitted; ii. passwords shall not be included in any automated log-on process (e.g., stored in a macro or function key); iii. all passwords shall be encrypted during transmission and storage on all system components; iv. users shall sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group; and v. temporary passwords shall be unique to an individual and shall not be guessable. Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: i. maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password. ii. ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging); iii. following loss management procedures to electronically de-authorize lost, stolen, missing or otherwise potentially compromised tokens, cards and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	iv. use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organization management; and v. initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.
Level 2 Control Standard Mapping:	• 21 CFR Part 11.30 • CMSRs 2013v2 IA-5 (HIGH) • CMSRs 2013v2 IA-5(1) (HIGH) • IRS Pub 1075 v2014 9.3.7.5 • ISO 27002-2005 11.2.3 • ISO/IEC 27002-2013 A.9.2.4 • ISO 27799-2008 7.8.2.3 • MARS-E v1 IA-5 • MARS-E v1 IA-5(1) • NIST SP 800-53 R4 IA-5 • NIST SP 800-53 R4 IA-5(1) • NRS 603A.215.1 • PCI DSS v3 8.2.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Requirements

CMS Contractors:	The organization enforces the following minimum password requirements (User/Privileged/Process [acting on behalf of a User]):
	i. Minimum Password Age = 1/1/1;
	ii. Maximum Password Age = 60/60/120;
	iii. Minimum Password Length = 8/8/15;
	iv. Password Complexity = 1/1/3 (minimum one (1) character [three (3)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	for a process] from the four (4) character categories (A-Z, a-z, 0-9, special characters); and v. Password History Size = 6/6/12. PIV compliant access cards are valid for no longer than five (5) years; and PKI certificates issued in accordance with the Federal PKI Common Policy are valid for no longer than three (3) years. Organizations shall ensure non-standard account-authenticators are managed in accordance with the CMS Risk Management Handbook (RMH), Volume III, Standard 4.3, "Non-Standard Authenticator Management."

FTI Requirements

FTI Custodians:	The information system must, for password-based authentication: i. Enforce password minimum lifetime restriction of one day; ii. Enforce non-privileged account passwords to be changed at least every 90 days; and iii. iii. Enforce privileged account passwords to be changed at least every 60 days.

Control Reference: 01.e Review of User Access Rights

Control Specification:	All access rights shall be regularly reviewed by management via a formal documented process.
Factor Type:	System
Topics:	Audit and Accountability Monitoring User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	The following procedures shall be carried out to ensure the regular review of access rights by management: i. user's access rights shall be reviewed after any changes, such as promotion, demotion, or termination of employment, or other

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	arrangement with a workforce member ends; and ii. user's access rights shall be reviewed and re-allocated when moving from one employment or workforce member arrangement to another within the same organization.
Level 1 Control Standard Mapping:	• CSA IS-10 • HIPAA § 164.312(a)(2)(i) • HIPAA § 164.312(a)(2)(ii) • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(3)(ii)(B) • HIPAA § 164.308(a)(3)(ii)(C) • HIPAA § 164.308(a)(4)(i) • HIPAA § 164.308(a)(4)(ii)(B) • HIPAA § 164.308(a)(5)(ii)(C) • HIPAA § 164.312(a)(1) • NIST Cybersecurity Framework PR.AC-4 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.03(2)(h) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall maintain a documented list of authorized users of information assets. In addition: i. all types of accounts shall be reviewed at least every 90 days; ii. critical system accounts shall be reviewed at least every 60 days; iii. user's access rights shall be reviewed at least every 90 days; iv. changes to access authorizations shall be reviewed at least every 90 days; and v. authorizations for special privileged access rights shall be reviewed at least every 60 days.
Level 2 Control Standard	• CMSRs 2013v2 AC-2 (HIGH) • COBIT 4.1 DS5.3

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Mapping:	• COBIT 4.1 DS5.4 • COBIT 5 DSS05.04 • IRS Pub 1075 v2014 9.3.1.2 • ISO/IEC 27002-2005 11.2.4 • ISO/IEC 27002-2013 A.9.2.5 • ISO 27799-2008 7.8.2.4 • MARS-E v1 AC-2 • NIST SP 800-53 R4 AC-2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	All information system accounts shall be reviewed to receive annual certification.

Health Information Exchange Requirements

Health Information Exchanges:	HIEs shall, for all employees and for all employees of connecting organizations, review users with access and the appropriateness of each user's role every 90 days. Any discrepancies shall be remediated immediately following the review.

Objective Name: 01.03 User Responsibilities

Control Objective:	To prevent unauthorized user access, and compromise or theft of information and information assets.

Control Reference: 01.f Password Use

Control Specification:	Users shall be made aware of their responsibilities for maintaining effective access controls and shall be required to follow good security practices in the

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	selection and use of passwords and security of equipment. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Authentication Awareness and Training Password Management

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to State of Massachusetts Data Protection Act, Subject to Joint Commission Accreditation, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	Users are made aware of the organization's password policies and requirements to: i. keep passwords confidential; ii. avoid keeping a record (e.g., paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved; iii. change passwords whenever there is any indication of possible system or password compromise; iv. not share individual user accounts or passwords; v. not provide their password to anyone for any reason (to avoid compromising their user credentials through social engineering attacks) vi. not use the same password for business and non-business purposes; and vii. select quality passwords (see requirements in 01.d). If users need to access multiple services, systems or platforms, and are required to maintain multiple separate passwords, they shall be advised that they may use a single, quality password for all services where the user is assured that a reasonable level of protection has been established for the storage of the password within each service, system or platform.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 IA-5 (HIGH) • HIPAA § 164.308(a)(5)(ii)(D) • IRS Pub 1075 v2014 9.3.7.5 • ISO/IEC 27002-2005 11.3.1 • ISO/IEC 27002-2013 A.9.3.1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• ISO 27799-2008 7.8.3 • JCAHO IM.02.01.03, EP 5 • MARS-E v1 IA-5 • NIST Cybersecurity Framework PR.AC-1 • NIST SP 800-53 R4 IA-5 • NRS 603A.215.1 • PCI DSS v3 8.2.6 • PCI DSS v3 8.4 • PCI DSS v3 8.2.4 • PCI DSS v3 8.2.5 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 1 CORE 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.1 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.04(1)(b) • (State of Mass.) 201 CMR 17.04(1)(e) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Implementation:	

Control Reference: 01.g Unattended User Equipment

Control Specification:	Users shall ensure that unattended equipment has appropriate protection.
Factor Type:	Organizational
Topics:	Awareness and Training Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	All users shall be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users shall be advised to: i. terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism (e.g., a password protected screen saver); ii. log-off mainframe computers, servers, and office PCs when the session is finished (e.g., not just switch off the PC screen or terminal); iii. secure PCs or terminals from unauthorized use by a key lock or an equivalent control (e.g., password access) when not in use. The organization shall safeguard information system output devices (e.g., printers) to help prevent unauthorized individuals from obtaining the output.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-11 (HIGH) • CMSRs 2013v2 PE-5 (HIGH) • CSA IS-16 • HIPAA § 164.310(a)(1) • HIPAA § 164.310(b) • HIPAA § 164.310(c) • HIPAA § 164.312(a)(2)(iii) • IRS Pub 1075 v2014 4.3.2 • IRS Pub 1075 v2014 9.3.1.9

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• IRS Pub 1075 v2014 9.3.11.5 • ISO/IEC 27002-2005 11.3.2 • ISO/IEC 27002-2013 A.11.2.8 • ISO 27799-2008 7.8.3 • MARS-E v1 AC-11 • MARS-E v1 PE-5 • NIST Cybersecurity Framework PR.AC-2 • NIST SP 800-53 R4 AC-11 • NIST SP 800-53 R4 PE-5 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

FTI Requirements

FTI Custodians:	Output from printers and fax machines should be in a controlled area and secured when not in use. Physical access to monitors displaying FTI should be controlled to prevent

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	unauthorized access to the display output.

Control Reference: 01.h Clear Desk and Clear Screen Policy

Control Specification:	A clear desk policy for papers and removable storage media and a clear screen policy for information assets shall be adopted. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Awareness and Training Data Loss Prevention Documentation and Records Media and Assets Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	A clear desk policy for papers and removable storage media and a clear screen policy for information assets shall be developed and adopted, and communicated to all users. The clear desk and clear screen policy shall take into account the information classifications, legal and contractual requirements, and the corresponding risks and cultural aspects of the organization. The following practices shall be established: i. covered or critical business information (e.g., on paper or on electronic storage media) shall be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated; ii. computers and terminals shall be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism that conceals information previously visible on the display when unattended and shall be protected by key locks, passwords or other controls when not in use; iii. incoming and outgoing mail points and unattended facsimile machines shall be protected;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	iv. unauthorized use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) shall be prevented; v. documents containing covered or classified information shall be removed from printers, copiers, and facsimile machines immediately; and vi. when transporting documents with covered information within facilities and through inter-office mail, information shall not be visible through envelope windows, and envelopes shall be marked according to its classification level (e.g., "Confidential").
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-11 (HIGH) • CSA IS-17 • HIPAA § 164.310(b) • HIPAA § 164.312(a)(2)(i) • IRS Pub 1075 v2014 9.3.1.9 • ISO/IEC 27002-2005 11.3.3 • ISO/IEC 27002-2013 A.11.2.9 • ISO 27799-2008 7.8.3 • MARS-E v1 AC-11 • NIST Cybersecurity Framework PR.PT-2 • NIST SP 800-53 R4 AC-11 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Objective Name: 01.04 Network Access Control

Control Objective:	To prevent unauthorized access to networked services.

Control Reference: 01.i Policy on the Use of Network Services

Control Specification:	Users shall only be provided with access to internal and external network services that they have been specifically authorized to use. Authentication and authorization mechanisms shall be applied for users and equipment. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Authentication Authorization Network Segmentation User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance
Level 1 Implementation:	The organization shall specify the networks and network services to which users are authorized access.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-1 (HIGH) • HIPAA § 164.308(a)(3)(i) • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(4)(i) • HIPAA § 164.308(a)(4)(ii)(B)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• HIPAA § 164.308(a)(4)(ii)(C) • HIPAA § 164.312(a)(1) • IRS Pub 1075 v2014 9.3.1.1 • ISO/IEC 27001-2005 A.11.4.1 • ISO/IEC 27001:2013 9.1.2 • MARS-E v1 AC-1 • NIST Cybersecurity Framework PR.PT-3 • NIST SP 800-53 R4 AC-1 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall: i. determine who is allowed to access which network and networked services (see 01.i, level 1); and ii. specify the means that can be used to access networks and network services (e.g., the conditions for allowing access to a remote system). The use of network services shall be consistent with the organization's business access control requirements. Use of external information systems shall be managed effectively including: i. information systems or components of information systems that are outside of the accreditation boundary established by the organization shall be identified as external information systems including: a. information systems or components of information systems for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness shall be identified as external information systems; b. personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants) shall be

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	identified as external information systems; and c. privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports) shall be identified as external information systems. ii. authorized individuals shall be prohibited from using an external information system to access the information system or to process, store or transmit organization-controlled information except in situations where the organization: a. can verify the employment of required security controls on the external system as specified in the organization's information security policy and system security plan; or b. has approved information system connection or processing agreements with the organizational entity hosting the external information system. The organization shall identify ports, services, and similar applications (e.g., protocols) necessary for business and provide the rationale or identify compensating controls implemented for those protocols considered to be insecure.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-20 (HIGH) • CMSRs 2013v2 CM-7 (HIGH) • CSA IS-08 • CSA SA-08 • IRS Pub 1075 v2014 9.3.1.15 • IRS Pub 1075 v2014 9.3.5.7 • ISO/IEC 27002-2005 11.4.1 • ISO/IEC 27002-2013 A.9.1.2 • ISO 27799-2008 7.8.4 • MARS-E v1 AC-20 • MARS-E v1 CM-7 • NIST Cybersecurity Framework ID.AM-4 • NIST Cybersecurity Framework PR.IP-1 • NIST SP 800-53 R4 AC-20 • NIST SP 800-53 R4 CM-7

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation:	No additional requirements

Control Reference: 01.j User Authentication for External Connections

Control Specification:	Appropriate authentication methods shall be used to control access by remote users. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Authentication Authorization Third Parties and Contractors User Access Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FTC Red Flags Rule Compliance
Level 1 Implementation:	Authentication of remote users shall be implemented using a password or passphrase and at least one of the following methods: i. a cryptographic based technique; ii. biometric techniques; iii. hardware tokens; iv. software tokens; v. a challenge/response protocol; or vi. certificate agents. The organization shall protect wireless access to systems containing sensitive information by authenticating users and devices. Remote access to business information across public networks shall only take place after successful identification and authentication. Remote access by vendors and business partners (e.g., maintenance, reports or other data access) shall be disabled unless specifically authorized by management. If remote maintenance is performed, the organization shall closely monitor and control any activities, with immediate deactivation after use. Remote access to business partner accounts shall also be immediately deactivated after use.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Use Radius or Kerberos to enable user privilege/resources to access the organization's network. For dial-up connections, use CHAP negotiation for encryption of user authentication. Configure CHAP instead of PAP for user authentication in dialup connection for encryption and security. If encryption is not used for dial-up connections, the CIO or his/her designated representative must provide specific written authorization.
Level 1 Control Standard Mapping:	• 16 CFR Part §681 Appendix A III(b) • CMSRs 2013v2 AC-18 (HIGH) • CMSRs 2013v2 AC-18(1) (HIGH) • CSA SA-07 • HIPAA § 164.310(b) • IRS Pub 1075 v2014 9.3.1.13 • MARS-E v1 AC-18 • MARS-E v1 AC-18(1) • NIST Cybersecurity Framework PR.AC-1 • NIST Cybersecurity Framework PR.AC-3 • NIST Cybersecurity Framework PR.PT-4 • NIST Cybersecurity Framework DE.CM-1 • NIST SP 800-53 R4 AC-18 • NIST SP 800-53 R4 AC-18(1) • PCI DSS v3 8.3 • PCI DSS v3 8.1.5 • PCI DSS v3 12.3.9 • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(3)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: Authentication of remote users shall be implemented via virtual private network (VPN) solutions that support a cryptographic based technique, hardware tokens, or a challenge/response protocol. Dedicated private lines

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	may also be used to provide assurance of the source of connections. Control all remote access through a limited number of managed access control points. Periodic monitoring shall be implemented to ensure that installed equipment does not include unanticipated dial-up capabilities. Require callback capability with re-authentication to verify connections from authorized locations. For application systems and turnkey systems that require the vendor to log-on, the vendor shall be assigned a User ID and password and enter the network through the standard authentication process. Access to such systems shall be authorized and logged. User IDs assigned to vendors will be reviewed in accordance with the organization's access review policy, at a minimum annually. Node authentication may serve as an alternative means of authenticating groups of remote users where they are connected to a secure, shared computer facility. Cryptographic techniques (e.g., based on machine certificates) can be used for node authentication. This is part of several VPN based solutions.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-17 (HIGH) • CMSRs 2013v2 AC-17(3) (HIGH) • CMSRs 2013v2 IA-8 (HIGH) • CMSRs 2013v2 IA-8(1) (HIGH) • CMSRs 2013v2 IA-8(2) (HIGH) • CMSRs 2013v2 IA-8(3) (HIGH) • CMSRs 2013v2 IA-8(4) (HIGH) • IRS Pub 1075 v2014 9.3.1.12 • IRS Pub 1075 v2014 9.3.7.8 • ISO/IEC 27002-2005 11.4.2 • ISO 27799-2008 7.8.4 • MARS-E v1 AC-17 • MARS-E v1 AC-17(3) • MARS-E v1 IA-8 • NIST SP 800-53 R4 AC-17 • NIST SP 800-53 R4 AC-17(3) • NIST SP 800-53 R4 IA-8 • NIST SP 800-53 R4 IA-8(1) • NIST SP 800-53 R4 IA-8(2) • NIST SP 800-53 R4 IA-8(3) • NIST SP 800-53 R4 IA-8(4)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Pharmaceutical Companies: > 70,000,000 Prescriptions Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to PCI Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: The information system monitors and controls remote access methods. The execution of privileged commands and access to security-relevant information via remote access shall only be authorized for compelling operational needs and rationale documented.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 AC-17(1) (HIGH) • CMSRs 2013v2 AC-17(4) (HIGH) • IRS Pub 1075 v2014 9.4.13 • IRS Pub 1075 v2014 9.4.18 • MARS-E v1 AC-17(1) • NIST SP 800-53 R4 AC-17(1) • NIST SP 800-53 R4 AC-17(4) • NRS 603A.215.1 • PCI DSS v3 2.3

CMS Contractor Requirements

CMS Contractors:	If e-authentication is implemented as a remote access solution or associated with remote access, refer to the Risk Management Handbook (RMH), Volume III, Standard 3.1, "CMS Authentication Standards". Remote sessions authorized for use for remote administration shall employ additional security measures (e.g., Secure Shell [SSH]], Virtual Private Networking [VPN] with blocking mode enabled) and encryption.

Federal Requirements

Federal Agencies and Contractors:	The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies. The information system accepts only Federal Identity, Credential, and Access Management (FICAM)-approved third-party credentials. The organization employs only FICAM-approved information system components in information systems that authenticate non-organizational users

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	0(7!0**#+,!,/&$7H0$,S!*$#7#(,&06%9 ! ?/#!&(-'$B0,&'(!%S%,#B!*'(-'$B%!,'!;<.2U H&%%3#7!+$'-&6#%9

'

3#"'$,J.0/,*,+1= '

'

3#"'(.=1)E04+=

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 01.l Remote Diagnostic and Configuration Port Protection

Control Specification:	Physical and logical access to diagnostic and configuration ports shall be controlled.
Factor Type:	Organizational
Topics:	Authorization Media and Assets Physical and Facility Security Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Access to network equipment shall be physically protected (e.g., a router must be stored in a room that is only accessible by authorized employees or contractors).
Level 1 Control Standard	• NIST Cybersecurity Framework PR.PT-3

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Mapping:	

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: Controls for the access to diagnostic and configuration ports shall include the use of a key lock. Ports, services, and similar applications installed on a computer or network systems, which are not specifically required for business functionality, shall be disabled or removed. Supporting procedures to control physical access to the port shall be implemented including ensuring that diagnostic and configuration ports are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access.
Level 2 Control Standard:	• CMSRs 2013v2 MA-4 (HIGH) • CMSRs 2013v2 MA-4(2) (HIGH) • CMSRs 2013v2 MA-4(3) (HIGH) • COBIT 4.1 DS5.7 • COBIT 5 DSS05.05 • CSA IS-30 • IRS Pub 1075 v2014 9.3.9.4 • ISO/IEC 27002-2005 11.4.4 • ISO 27799-2008 7.8.4 • MARS-E v1 MA-4 • MARS-E v1 MA-4(2) • MARS-E v1 MA-4(3) • NIST Cybersecurity Framework PR.IP-1 • NIST SP 800-53 R4 MA-4 • NIST SP 800-53 R4 MA-4(2) • NIST SP 800-53 R4 MA-4(3)

Level 3 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Pharmaceutical Companies: > 70,000,000 Prescriptions Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: The organization shall review the information system within every three hundred sixty-five (365) days to identify and disable unnecessary and non-secure functions, ports, protocols, and/or services. The information system prevents program execution in accordance with the list of authorized software programs and rules authorizing the terms and conditions of software program usage. The organization shall disable Bluetooth and peer-to-peer networking protocols within the information system determined unnecessary or non-secure. The organization shall identify unauthorized software on the information system; employ an allow-all, deny-by-exception policy to prohibit the execution of known unauthorized software on the information system; and review and update the list of unauthorized software periodically but no less than annually.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 CM-7 (HIGH) • CMSRs 2013v2 CM-7(1) (HIGH) • CMSRs 2013v2 CM-7(2) (HIGH) • CMSRs 2013v2 CM-7(5) (HIGH) • IRS Pub 1075 v2014 9.3.5.7 • IRS Pub 1075 v2014 9.4.9 • MARS-E v1 CM-2(4) • MARS-E v1 CM-7 • MARS-E v1 CM-7(1) • NIST SP 800-53 R4 AC-17(5) • NIST SP 800-53 R4 CM-7 • NIST SP 800-53 R4 CM-7(1) • NIST SP 800-53 R4 CM-7(2)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST SP 800-53 R4 CM-7(4)

CMS Contractor Requirements

CMS Contractors:	A list of specifically needed system services, ports, and network protocols will be maintained and documented in the security plan. If collaborative computing is authorized, the information system shall provide physical disconnect of collaborative computing devices in a manner that supports ease of use. The organization shall employ automated mechanisms to prevent program execution in accordance with list of authorized or unauthorized software programs and rules authorizing the terms and conditions of software program usage. The organization: i. identifies defined software programs (defined in the applicable security plan) authorized to execute on the information system; ii. employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and iii. reviews and updates the list of authorized software programs within every ninety (90) days.

FTI Requirements

FTI Custodians:	Least functionality controls that must be in place that include disabling all unneeded network protocols, services, and assigning a dedicated static IP address to Multifunctional Devices (MFDs).

Control Reference: 01.m Segregation in Networks

Control Specification:	Groups of information services, users, and information systems should be segregated on networks. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Network Segmentation Network Security

Level 1 Implementation Requirements

Level 1 Organizational	Applicable to all organizations

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance
Level 1 Implementation:	Security gateways (e.g., a firewall) shall be used between the internal network, external networks (Internet and 3rd party networks), and any demilitarized zone (DMZ). An internal network perimeter shall be implemented by installing a secure gateway (e.g., a firewall) between two interconnected networks to control access and information flow between the two domains. This gateway shall be capable of enforcing security policies, be configured to filter traffic between these domains, and block unauthorized access in accordance with the organization's access control policy. Wireless networks shall be segregated networks from internal and private networks. The organization shall require a firewall between any wireless network and the covered information systems environment.
Level 1 Control Standard Mapping:	• CSA SA-08 • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(3)(ii)(B) • HIPAA § 164.310(b) • IRS Pub 1075 v2014 9.4.10 • PCI DSS v3 1.1 • PCI DSS v3 1.1.4 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Geographic Scope: Multi-state, BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Implementation:	Level 1 plus: The criteria for segregation of networks into domains shall be based on the access control policy and access requirements, and also takes account of the relative cost and performance impact of incorporating suitable network routing or gateway technology. In addition, segregation of networks shall be based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption. Networks shall be divided into separate logical network domains (e.g., an organization's internal network domains and external network domains) each protected by a defined security perimeter. A graduated set of controls shall be applied in different logical network domains to further segregate the network security environments (e.g., publicly accessible systems, internal networks, and critical assets). Segregations of separate logical domains shall be achieved by restricting network access using virtual private networks for user groups within the organization. Networks shall also be segregated using network device functionality (e.g., IP switching). A baseline of network operations and expected data flows for users and systems shall be established and managed. Separate domains shall then be implanted by controlling the network data flows using routing/switching capabilities, including access control lists, according to applicable flow control policies. The domains shall be defined based on a risk assessment and the different security requirements within each of the domains. The organization shall implement subnetworks for publicly accessible system components that are logically separated from internal organizational networks.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-4 (HIGH) • CMSRs 2013v2 SC-7 (HIGH) • CMSRs 2013v2 SC-32 (HIGH) • COBIT 4.1 DS5.10 • COBIT 5 DSS05.02 • CSA SA-09 • IRS Pub 1075 v2014 9.3.1.4 • IRS Pub 1075 v2014 9.3.16.5 • IRS Pub 1075 v2014 9.4.5 • IRS Pub 1075 v2014 9.4.11 • IRS Pub 1075 v2014 9.4.13 • IRS Pub 1075 v2014 9.4.14 • IRS Pub 1075 v2014 9.4.15

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• IRS Pub 1075 v2014 9.4.18 • ISO/IEC 27002-2005 11.4.5 • ISO/IEC 27002-2013 A.13.1.3 • MARS-E v1 AC-4 • MARS-E v1 SC-7 • MARS-E v1 SC-7(1) • MARS-E v1 SC-7(2) • MARS-E v1 SC-32 • NIST Cybersecurity Framework ID.AM-3 • NIST Cybersecurity Framework DE.AE-1 • NIST Cybersecurity Framework PR.AC-4 • NIST Cybersecurity Framework PR.AC-5 • NIST Cybersecurity Framework PR.DS-5 • NIST Cybersecurity Framework PR.IP-1 • NIST Cybersecurity Framework PR.PT-4 • NIST SP 800-53 R4 AC-4 • NIST SP 800-53 R4 SC-7

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization shall partition the information system into defined information system components (defined in the applicable security plan) residing in separate physical domains or environments based on defined circumstances (defined in the applicable security plan) for physical separation of components.

FTI Requirements

FTI Custodians:	To use an Integrated Voice Response (IVR) system that provides FTI over the telephone to a customer, the agency must ensure the LAN segment where the

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	IVR system resides is firewalled (segmented) to prevent direct access from the Internet to the IVR system. To use FTI in a SAN environment, the agency must ensure FTI is segregated from other agency data within the SAN environment. To use Virtual Desktop Infrastructure (VDI) to provide FTI to a customer, the agency muse ensure VDI components are segregated so that boundary protections can be implemented and access controls are sufficiently granular. To use a virtual environment that receives, processes, stores or transmits FTI, separation between VMs must be enforced, and functions that allow one VM to share data with the hypervisor or another VM, such as clipboard sharing or shared disks, must be disabled. To use a VoIP network that provides FTI to a customer, VoIP traffic that contains FTI should be segmented off from non-VoIP traffic through segmentation. If complete segmentation is not feasible, the agency must have compensating controls in place and properly applied that restrict access to VoIP traffic that contains FTI. VoIP-ready firewalls must be used to filter VoIP traffic on the network. To use FTI in an 802.11 WLAN, the agency must architect the WLAN environment to provide logical separation between WLANs with different security profiles and from the wired LAN.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.

Control Reference: 01.n Network Connection Control

Control Specification:	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network shall be restricted, in line with the access control policy and requirements of the business applications. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Network Segmentation User Access Network Security

Level 1 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	At managed interfaces, network traffic is denied by default and allowed by exception (i.e., deny all, permit by exception). The organization shall restrict the ability of users to connect to the internal network in accordance with the access control policy and the requirements of the clinical and business applications.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 SC-7 (HIGH) • CMSRs 2013v2 SC-7(5) (HIGH) • CSA DG-07 • IRS Pub 1075 v2014 9.3.16.5 • HIPAA § 164.310(b) • MARS-E v1 SC-7 • MARS-E v1 SC-7(5) • NIST Cybersecurity Framework DE.AE-1 • NIST Cybersecurity Framework PR.AC-3 • NIST Cybersecurity Framework PR.DS-5 • NIST SP 800-53 R4 SC-7 • NIST SP 800-53 R4 SC-7(5) • NRS 603A.215.1 • (State of Mass.) 201 CMR 17.04(6) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	Requirements
Level 2 Implementation:	Level 1 plus: The connection capability of users shall be restricted through network gateways (e.g., a firewall) that filter traffic by means of pre-defined tables or rules. Restrictions shall be applied to: i. messaging (e.g., electronic mail); ii. file transfer (e.g., peer-to-peer, FTP); iii. interactive access (e.g., where a user provides input to the system); and iv. common Windows applications. Review exceptions to the traffic flow policy within every three hundred sixty-five (365) days or implementation of a major new systems. Linking network access rights to certain times of day or dates shall be implemented. The organization shall limit the number of external network connections to the information system (e.g., prohibiting desktop modems) to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. The organization shall: i. implement a managed interface for each external telecommunication service, i.e., transmissions of data to or from other entities external to the secure site, including to other secure sites using networks or any other communications resources outside of the physical control of the secure site to transmit information; ii. establish a traffic flow policy for each managed interface; iii. employ security controls as needed to protect the confidentiality and integrity of the information being transmitted; iv. document each exception to the traffic flow policy with a supporting mission/business need and duration of that need; v. review exceptions to the traffic flow policy within every three hundred sixty-five (365) days; and vi. remove traffic flow policy exceptions that are no longer supported by an explicit mission/business need. Remote devices that have established a non-remote connection shall be prevented from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-17 (HIGH) • CMSRs 2013v2 AC-17(3) (HIGH) • CMSRs 2013v2 SC-7(3) (HIGH)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• CMSRs 2013v2 SC-7(4) (HIGH) • CMSRs 2013v2 SC-7(8) (HIGH) • CMSRs 2013v2 SC-7(7) (HIGH) • CSA SA-08 • CSA SA-11 • IRS Pub 1075 v2014 9.3.1.12 • IRS Pub 1075 v2014 9.3.16.5 • IRS Pub 1075 v2014 9.4.10 • IRS Pub 1075 v2014 9.4.16 • IRS Pub 1075 v2014 9.4.17 • ISO/IEC 27002-2005 11.4.6 • ISO/IEC 27002-2005 12.5.4 • ISO 27799-2008 7.8.4 • MARS-E v1 AC-17 • MARS-E v1 AC-17(3) • MARS-E v1 SC-7(3) • MARS-E v1 SC-7(4) • MARS-E v1 SC-7(7) • NIST Cybersecurity Framework DE.CM-1 • NIST Cybersecurity Framework PR.AC-5 • NIST Cybersecurity Framework PR.PT-4 • NIST SP 800-53 R4 AC-17 • NIST SP 800-53 R4 AC-17(3) • NIST SP 800-53 R4 SC-7(3) • NIST SP 800-53 R4 SC-7(4) • NIST SP 800-53 R4 SC-7(7)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The information system shall route all user-initiated internal communications traffic to untrusted external networks through authenticated proxy servers at

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	managed interfaces.

FTI Requirements

FTI Custodians:	FTI must be transmitted securely in a Virtual Desktop Infrastructure (VDI) environment using end-to-end encryption. To use an external Web-based system or website that provides FTI over the Internet to a customer, the agency must ensure access to the database through the Web application is limited by configuring the system architecture as a three-tier architecture with physically separate systems that provide layered security of the FTI. To access FTI using a Web browser, the agency must deploy a Web gateway to inspect Web traffic and protect the user workstation from direct exposure to the Internet.

Control Reference: 01.o Network Routing Control

Control Specification:	Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Network Segmentation Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Security gateways (e.g., a firewall) shall be used between internal and external networks (Internet and 3rd party networks). The organization implements routing controls at the network perimeter.
Level 1 Control	• HIPAA § 164.308(a)(3)(ii)(A)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Standard Mapping:	• HIPAA § 164.308(a)(4)(ii)(B) • HIPAA § 164.310(b) • IRS Pub 1075 v2014 9.4.10 • NIST Cybersecurity Framework PR.AC-5 • NIST Cybersecurity Framework PR.DS-5 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to State of Massachusetts Data Protection Act, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Security gateways (e.g., a firewall) shall be used to validate source and destination addresses at internal and external network control points if proxy and/or network address translation technologies (e.g. DNS) are employed. The requirements for network routing control shall be based on the access control policy. Routing controls shall also be based on positive source and destination address checking mechanisms. Internal directory services and internal IP addresses shall be protected and hidden from any external access.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-4 (HIGH) • IRS Pub 1075 v2014 9.3.1.4 • IRS Pub 1075 v2014 9.4.10 • ISO/IEC 27002-2005 11.4.7 • ISO 27799-2008 7.8.4 • MARS-E v1 AC-4 • NIST Cybersecurity Framework ID.AM-3 • NIST Cybersecurity Framework PR.PT-4 • NIST SP 800-53 R4 AC-4 • NRS 603A.215.1 • PCI DSS v3 1.2

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• PCI DSS v3 1.2.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Objective Name: 01.05 Operating System Access Control

Control Objective:	To prevent unauthorized access to operating systems.

Control Reference: 01.p Secure Log-on Procedures

Control Specification:	Access to operating systems shall be controlled by a secure log-on procedure.
Factor Type:	System
Topics:	Authorization Policies and Procedures User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to PCI Compliance; Subject to FTI Requirements
Level 1 Implementation:	A secure log-on procedure shall: i. display a general notice warning that the computer shall only be

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	accessed by authorized users; ii. limit the number of unsuccessful log-on attempts allowed to six attempts; iii. enforce recording unsuccessful and successful attempts; iv. force a time delay of 30 minutes before further log-on attempts are allowed or rejecting any further attempts without specific authorization from an administrator; and v. not display the password being entered by hiding the password characters with symbols.
Level 1 Control Standard Mapping:	• HIPAA § 164.308(a)(5)(ii)(D) • NIST Cybersecurity Framework PR.AC-1 • NRS 603A.215.1 • PCI DSS v3 8.1.6 • PCI DSS v3 8.1.7 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Exchanges Data with a Business Partner: Yes, Third Party Support (Vendor Access or Maintenance): Yes, Publicly Accessible: Yes, System Connects with or Exchanges Data with an HIE: Yes
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: The procedure for logging into an operating system shall be designed to minimize the opportunity for unauthorized access. The log-on procedure shall therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance. The log-on procedures shall: i. limit the number of unsuccessful log-on attempts allowed to three attempts, and enforce: a. disconnecting data link connections; b. sending an alarm message to the system console if the maximum number of log-on attempts is reached; and c. setting the number of password retries in conjunction with the minimum length of the password and the value of the system being protected; ii. limit the maximum and minimum time allowed for the log-on procedure, if exceeded, the system shall terminate the log-on;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	iii. not transmit passwords in clear text over the network; iv. not display system or application identifiers until the log-on process has been successfully completed; v. not provide help messages during the log-on procedure that would aid an unauthorized user; and vi. validate the log-on information only on completion of all input data. If an error condition arises, the system shall not indicate which part of the data is correct or incorrect.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-7 (HIGH) • CMSRs 2013v2 IA-6 (HIGH) • IRS Pub 1075 v2014 9.3.1.7 • IRS Pub 1075 v2014 9.3.7.6 • MARS-E v1 AC-7 • MARS-E v1 IA-6 • NIST SP 800-53 R4 AC-7 • NIST SP 800-53 R4 IA-6

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	Processing PHI: Yes - AND -, Accessible from the Internet: Yes
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements
Level 3 Implementation:	Level 2 plus: Configure the information system to lock out the user account automatically after three failed log-on attempts by a user during a one hour time period. Require the lock out to persist for a minimum of three hours. Training shall include reporting procedures and responsibility for authorized users to report unauthorized log-ons and unauthorized attempts to log-on. The number of concurrent sessions shall be limited to a specified number for all account types defined by the organization.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 AC-9 (HIGH) • CMSRs 2013v2 AC-9(1) (HIGH) • CMSRs 2013v2 AC-10 (HIGH) • ISO/IEC 27002-2005 11.5.1 • ISO/IEC 27002-2013 A.9.4.2 • ISO 27799-2008 7.8.4 • MARS-E v1 AC-10

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST SP 800-53 R4 AC-10

CMS Contractor Requirements

CMS Contractors:	The number of concurrent network sessions for a user shall be limited and enforced to one (1) session. The number of concurrent application/process sessions shall be limited and enforced to the number of sessions expressly required for the performance of job duties. The requirement and use of more than one (1) application/process session for each user shall be documented in the system security profile. The information system notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access). The organization shall configure the information system to lock out the user account automatically after three (3) invalid login attempts during a one (1) hour time period. The lock out shall persist for a minimum of three (3) hours unless unlocked by an administrator. The control applies whether the login occurs via a local or network connection.

FTI Requirements

FTI Custodians:	Automatically lock the account/node until an authorized system administrator reinstates the account.

Control Reference: 01.q User Identification and Authentication

Control Specification:	All users shall have a unique identifier (user ID) for their personal use only, and an authentication technique shall be implemented to substantiate the claimed identity of a user. *Required for HITRUST Certification 2015
Factor Type:	System
Topics:	Authentication User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	Before allowing access to system components or data, the organization shall require verifiable unique ID's for all types of users including, but not limited to: i. technical support personnel; ii. operators; iii. network administrators; iv. system programmers; and v. database administrators. The following shall be required for each category of User ID: i. regular User IDs: a. user IDs shall be used to trace activities to the responsible individual; and b. regular user activities shall not be performed from privileged accounts. ii. shared user / group IDs: a. in exceptional circumstances, where there is a clear business/clinical benefit, the use of a shared user ID for a group of users or a specific job can be used; b. approval by management shall be documented for such cases; and c. additional controls are required to maintain accountability. iii. generic IDs: a. generic IDs for use by an individual shall only be allowed either where the functions accessible or actions carried out by the ID do not need to be traced (e.g., read only access). The organization shall ensure that redundant user IDs are not issued to other users. Non-organizational users (all information system users other than organizational users, such as patients or customers), or processes acting on behalf of non-organizational users, determined to need access to information residing on the organization's information systems, shall be uniquely identified and authenticated in accordance with the requirements outlined above and CSF control 01.d. Users shall be uniquely identified and authenticated for both local and remote accesses to information systems.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 IA-4 (HIGH) • CMSRs 2013v2 IA-8 (HIGH) • COBIT 4.1 DS5.3 • COBIT 5 DSS05.04 • HIPAA § 164.308(a)(3)(i)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• HIPAA § 164.312(a)(2)(i) • HIPAA § 164.312(d) • IRS Pub 1075 v2014 9.3.7.4 • IRS Pub 1075 v2014 9.3.7.8 • MARS-E v1 IA-4 • MARS-E v1 IA-8 • NIST Cybersecurity Framework PR.AC-1 • NIST SP 800-53 R4 IA-2 • NIST SP 800-53 R4 IA-4 • NIST SP 800-53 R4 IA-8 • NRS 603A.215.1 • PCI DSS v3 8.1 • PCI DSS v3 8.1.1 • PCI DSS v3 8.5 • PCI DSS v3 12.3.2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 1 CORE 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.1 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.04(1)(a) • (State of Mass.) 201 CMR 17.04(2)(b) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Accessible from the Internet: Yes, Third Party Support (Vendor Access or Maintenance): Yes
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: Appropriate authentication methods including strong authentication methods in addition to passwords shall be used for communicating through an external, non-organization-controlled network (e.g., the Internet). Help desk support shall require user identification for any transaction that has information security implications. During the registration process to provide new or replacement hardware tokens, in-person verification shall be required in front of a designated

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	registration authority with authorization by a designated organizational official (e.g., a supervisor). The information system, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements discussed in NIST SP 800-63-2, Electronic Authentication Guideline. When PKI-based authentication is used, the information system: validates certificates by constructing a certification path with status information to an accepted trust anchor; i. validates certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; ii. enforces authorized access to the corresponding private key; iii. maps the authenticated identity to the account of the individual or group; and iv. implements a local cache of revocation data to support path discovery and validation in case of an inability to access revocation information via the network. The information system shall use replay-resistant authentication mechanisms such as nonce, one-time passwords, or time stamps (e.g., Kerberos, TLS, etc.) for network access to privileged accounts. The information system
Level 2 Control Standard Mapping:	• CMSRs 2013v2 IA-2 (HIGH) • CMSRs 2013v2 IA-2(8) (HIGH) • CMSRs 2013v2 IA-5 (HIGH) • CMSRs 2013v2 IA-5(2) (HIGH) • CMSRs 2013v2 IA-5(3) (HIGH) • CMSRs 2013v2 IA-5(11) (HIGH) • CSA SA-07 • IRS Pub 1075 v2014 9.3.7.2 • IRS Pub 1075 v2014 9.3.7.5 • ISO/IEC 27002-2005 11.5.2 • ISO/IEC 27002-2013 A.9.2.1 • ISO 27799-2008 7.8.4 • ISO 27799-2008 7.8.5.1 • MARS-E v1 IA-2 • MARS-E v1 IA-2(8) • MARS-E v1 IA-5 • MARS-E v1 IA-5(2) • MARS-E v1 IA-5(3) • NIST SP 800-53 R4 IA-2(8) • NIST SP 800-53 R4 IA-5 • NIST SP 800-53 R4 IA-5(2) • NIST SP 800-53 R4 IA-5(3) • NIST SP 800-53 R4 IA-5(11) • PCI DSS v3 8.2.2

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• PCI DSS v3 8.5.1 • PCI DSS v3 8.6

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: The organization shall employ multifactor authentication for remote network access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access. The organization shall employ multifactor authentication for local access to privileged accounts (including those used for non-local maintenance and diagnostic sessions).
Level 3 Control Standard Mapping	• CMSRs 2013v2 IA-2(1) (HIGH) • CMSRs 2013v2 IA-2(2) (HIGH) • CMSRs 2013v2 IA-2(3) (HIGH) • CMSRs 2013v2 IA-2(4) (HIGH) • CMSRs 2013v2 IA-2(9) (HIGH) • CMSRs 2013v2 IA-2(11) (HIGH) • CMSRs 2013v2 IA-2(12) (HIGH) • IRS Pub 1075 v2014 9.3.7.2 • IRS Pub 1075 v2014 9.4.2 (E.10) • MARS-E v1 IA-2(1) • MARS-E v1 IA-2(2) • MARS-E v1 IA-2(3) • NIST SP 800-53 R4 IA-2(1) • NIST SP 800-53 R4 IA-2(2) • NIST SP 800-53 R4 IA-2(3) • NIST SP 800-53 R4 IA-2(11) • NIST SP 800-53 R4 IA-2(12)

CMS Contractor Requirements

CMS Contractors:	The information system shall use multifactor authentication for local access to non-privileged accounts.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The information system shall use replay-resistant authentication mechanisms such as nonce, one-time passwords, or time stamps (e.g., Kerberos, TLS, etc.) for network access to non-privileged accounts. A risk assessment is used in determining the authentication needs of the organization. The information system, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements discussed in the Risk Management Handbook (RMH), Volume III, Standard 3.1, CMS Authentication Standards.

Federal Requirements

Federal Agencies and Contractors:	The information system accepts and electronically verifies Personal Identity Verification (PIV) credentials.

FTI Requirements

FTI Custodians:	Complete section 2.10 (e-Authentication level) in the SSP Template. Two-factor authentication is required whenever FTI is being accessed from an alternative work location or if accessing FTI via agency's web portal by an employee or contractor. The agency shall configure the Web services to be authenticated before access is granted to users via an authentication server. All Web portal and two-factor authentication requirements apply in a data warehouse environment. Authentication shall be required both at the operating system level and at the application level, whenever the data warehousing environment is accessed.

PCI-DSS Requirements

PCI Data:	The organization shall not use group, shared, or generic IDs, passwords, or other authentication methods as follows: i. generic user IDs are disabled or removed. ii. shared user IDs do not exist for system administration and other critical functions. iii. shared and generic user IDs are not used to administer any system components. Where other authentication mechanisms are used (e.g., physical or logical security tokens, smart cards, and certificates), use of these mechanisms shall be assigned as follows: i. authentication mechanisms must be assigned to an individual account

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	and not shared among multiple accounts. ii. Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access. Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase for each customer.)

Control Reference: 01.r Password Management System

Control Specification:	Systems for managing passwords shall be interactive and shall ensure quality passwords. *Required for HITRUST Certification 2015
Factor Type:	System
Topics:	Cryptography Password Management

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Refer to Sections 1.b and 1.f for a full list of password controls. In addition, a password management system shall be implemented to: i. require the use of individual user IDs and passwords to maintain accountability; ii. allow users to select and change their own passwords and include a confirmation procedure to allow for input errors; iii. force users to change temporary passwords at the first log-on (see 01.b); iv. not display passwords on the screen when being entered; and v. always change vendor-supplied defaults before installing a system on the network including passwords, simple network management protocol (SNMP) community strings and the elimination of unnecessary accounts.
Level 1 Control Standard	• HIPAA § 164.308(a)(5)(ii)(D) • NIST Cybersecurity Framework PR.AC-1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Mapping:	• PCI DSS v3 2.1 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 1 CORE 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.1 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.04(1)(b) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Accessible from the Internet: Yes, Number of Users: > 500, Exchanges Data with a Business Partner: Yes, Third Party Support (Vendor Access or Maintenance): Yes, Publicly Accessible: Yes, Number of Interfaces to Other Systems: > 25, System Connects with or Exchanges Data with an HIE: Yes
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to State of Massachusetts Data Protection Act, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Refer to Sections 1.b and 1.f for a full list of password controls. The password management system shall: i. store and transmit passwords in protected (e.g., encrypted or hashed) form; ii. store password files separately from application system data; iii. enforce a choice of quality passwords (see 01.b); iv. enforce password changes (see 01.b); and v. maintain a record of previous user passwords and prevent re-use (see 01.b).
Level 2 Control Standard Mapping:	• CMSRs 2013v2 IA-5 (HIGH) • IRS Pub 1075 v2014 9.3.7.5 • ISO/IEC 27002-2005 11.5.3 • ISO/IEC 27002-2013 A.9.4.3 • ISO 27799-2008 7.8.4 • MARS-E v1 IA-5 • NIST SP 800-53 R4 IA-5 • NRS 603A.215.1 • PCI DSS v3 8.2.1 • (State of Mass.) 201 CMR 17.04(1)(c)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The CMS information system for PKI-based authentication shall: i. validate certificates by constructing a certification path with status information to an accepted trust anchor; ii. enforce authorized access to the corresponding private key; and iii. map the authenticated identity to the user account.

Control Reference: 01.s Use of System Utilities

Control Specification:	The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.
Factor Type:	System
Topics:	Authorization Monitoring Network Segmentation

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Implementation:	The use of system utilities (e.g., administrative tools in Windows, the settings section--specifically network/device/security configuration--on VoIP phones, etc.) shall be controlled by implementing the following: i. use of identification, authentication, and authorization procedures for system utilities; ii. segregation of system utilities from applications software; and iii. limitation of the use of system utilities to the minimum practical number of trusted, authorized users (see CSF control 01.b thru 01.o).
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-6 (HIGH) • CSA IS-34 • HIPAA § 164.308(a)(3)(i) • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(4)(i) • HIPAA § 164.308(a)(4)(ii)(A) • HIPAA § 164.308(a)(4)(ii)(B) • HIPAA § 164.308(a)(4)(ii)(C) • HIPAA § 164.310(a)(2)(iii) • HIPAA § 164.310(b) • HIPAA § 164.312(a)(1) • HIPAA § 164.312(a)(2)(i) • HIPAA § 164.312(a)(2)(ii) • HIPAA § 164.312(a)(2)(iv) • IRS Pub 1075 v2014 9.3.1.6 • MARS-E v1 AC-6 • NIST Cybersecurity Framework PR.AC-4 • NIST Cybersecurity Framework PR.DS-5 • NIST Cybersecurity Framework PR.PT-3 • NIST SP 800-53 R4 AC-6 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Accessible from the Internet: Yes, Exchanges Data with a Business Partner: Yes, Third Party Support (Vendor Access or Maintenance): Yes, Publicly Accessible: Yes, Number of Interfaces to Other Systems: > 25, System Connects with or Exchanges Data with an HIE: Yes
Level 2 Regulatory Factors:	Subject to PCI Compliance; Subject to FISMA Compliance; Requirements (High)Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The use of system utilities shall be controlled by implementing the following:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	i. authorization for ad hoc use of systems utilities; ii. limitation of the availability of system utilities (e.g., limitation of availability by setting restrictive file system level permissions for the access and execution of system utilities such as cmd.exe, ping, tracert, ipconfig, ifconfig, etc.); iii. disable public "read" access to files, objects, and directories; iv. logging of all use of system utilities; v. defining and documenting authorization levels for system utilities; vi. deletion of, or file system file execution permission denial of, all unnecessary software based utilities and system software; and vii. not making system utilities available to users who have access to applications on systems where segregation of duties is required. The information system owner shall regularly review the system utilities available to identify and eliminate unnecessary functions, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. Public "read" and "write" access to all system files, objects, and directories shall be disabled.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-3 (HIGH) • COBIT 4.1 DS5.7 • COBIT 5 DSS05.05 • IRS Pub 1075 v2014 9.3.1.3 • ISO/IEC 27002-2005 11.5.4 • ISO/IEC 27002-2013 A.9.4.4 • ISO 27799-2008 7.8.4 • MARS-E v1 AC-3 • NIST SP 800-53 R4 AC-3 • NRS 603A.215.1 • PCI DSS v3 2.2.5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	None
Level 3 Control Standard Mapping:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 01.t Session Time-out

Control Specification:	Inactive sessions shall shut down after a defined period of inactivity.
Factor Type:	System
Topics:	User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance
Level 1 Implementation:	A time-out system that conceals information previously visible on the display with a publically viewable image (e.g., a screen saver) shall pause the session screen after 15 minutes of inactivity and closes network sessions after 30 minutes of inactivity. The system shall require the user to reestablish access using appropriate identification and authentication procedures. A limited form of time-out system can be provided for legacy systems that cannot be modified to accommodate this requirement, which clears the screen and prevents unauthorized access through re-authentication requirements to continue the active session but does not close down the application or network sessions.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-11 (HIGH) • CMSRs 2013v2 AC-11(1) (HIGH) • CMSRs 2013v2 AC-12 (HIGH) • CSA SA-03 • HIPAA § 164.310(b) • HIPAA § 164.312(a)(2)(iii) • IRS Pub 1075 v2014 9.3.1.9 • IRS Pub 1075 v2014 9.3.1.10 • ISO/IEC 27002-2005 11.5.5 • ISO/IEC 27002-2013 A.9.4.2 • ISO 27799-2008 7.8.4 • MARS-E v1 AC-11 • NIST SP 800-53 R4 AC-11 • NIST SP 800-53 R4 AC-11(1) • NIST SP 800-53 R4 AC-12

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST SP 800-53 R4 SC-10 • NRS 603A.215.1 • PCI DSS v3 8.1.8 • PCI DSS v3 12.3.8 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

CMS Contractors:	The organization requires that users log out when the time-period of expected inactivity exceeds ninety (90) minutes. The information system shall automatically terminate the network connection associated with a communications session at the end of the session (as specified by the appropriate CSF level), OR: i. forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days or other organization-defined time period; AND ii. forcibly disconnects inactive Virtual Private Network (VPN) connections after thirty (30) minutes of inactivity or other organization-defined time period.

FTI Requirements

FTI Custodians:	The organization forcibly disconnects inactive VPN connections after 15 minutes of inactivity. The information system must automatically terminate a user session after 15 minutes of inactivity.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The information system automatically terminates the network connection associated with a communications session at the end of the session, or: i. Forcibly de-allocates communications session Dynamic Host Configuration Protocol (DHCP) leases after seven (7) days; and ii. Forcibly disconnects inactive Virtual Private Network (VPN) connections after thirty (30) minutes of inactivity.

Control Reference: 01.u Limitation of Connection Time

Control Specification:	Restrictions on connection times shall be used to provide additional security for high-risk applications.
Factor Type:	System
Topics:	Authentication Authorization User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 System Factors:	Processing PHI: Yes -AND-, Accessible from the Internet: Yes, Exchanges Data with a Business Partner: Yes, Third Party Support (Vendor Access or Maintenance): Yes, Publicly Accessible: Yes, System Connects with or Exchanges Data with an HIE: Yes
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Connection time controls shall be implemented for sensitive computer applications, especially from high risk locations (e.g., public or external areas that are outside the organization's security management) including: i. using predetermined time slots (e.g., for batch file transmissions or regular interactive sessions of short duration); ii. restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation; and iii. re-authentication at timed intervals.
Level 1 Control Standard Mapping:	• ISO/IEC 27002-2005 11.5.6 • ISO/IEC 27002-2013 A.9.4.2 • ISO 27799-2008 7.8.4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Implementation:	

Objective Name: 01.06 Application and Information Access Control

Control Objective:	To prevent unauthorized access to information held in application systems.

Control Reference: 01.v Information Access Restriction

Control Specification:	Logical and physical access to information and application systems and functions by users and support personnel shall be restricted in accordance with the defined access control policy. *Required for HITRUST Certification 2015
Factor Type:	System
Topics:	Authentication Policies and Procedures User Access Viruses and Malware

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Restrictions to access shall be based on individual business application requirements and in accordance with the access control policy. The following guidelines shall be implemented in order to support access restriction requirements: i. providing menus to control access to application system functions; and ii. controlling the access rights of users (e.g., read, write, delete, and execute). Associated identification and authentication controls shall be developed, disseminated, and periodically reviewed and updated, including: i. specific user actions that can be performed on the information system without identification or authentication shall be identified and supporting rationale documented;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	ii. actions to be performed without identification and authentication shall be permitted only to the extent necessary to accomplish mission objectives;
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-6 (HIGH) • CSA IS-08 • CSA SA-11 • HIPAA § 164.308(a)(3)(i) • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(4)(i) • HIPAA § 164.308(a)(4)(ii)(A) • HIPAA § 164.308(a)(4)(ii)(B) • HIPAA § 164.308(a)(4)(ii)(C) • HIPAA § 164.310(a)(2)(iii) • HIPAA § 164.310(b) • HIPAA § 164.312(a)(1) • HIPAA § 164.312(a)(2)(i) • HIPAA § 164.312(a)(2)(ii) • HIPAA § 164.312(a)(2)(iv) • IRS Pub 1075 v2014 9.3.1.6 • ISO/IEC 27002-2005 11.6.1 • ISO/IEC 27002-2013 A.9.4.1 • MARS-E v1 AC-6 • NIST Cybersecurity Framework PR.AC-4 • NIST Cybersecurity Framework PR.DS-5 • NIST Cybersecurity Framework PR.PT-3 • NIST SP 800-53 R4 AC-6 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to FISMA Compliance; Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The following guidelines shall be implemented in order to support access restriction requirements:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	i. controlling access rights to other applications according to applicable access control policies; ii. ensuring that outputs from application systems handling covered information contain only the information relevant to the use of the output and are sent only to authorized terminals and locations; and iii. periodic reviews of such outputs to ensure that redundant information is removed. When encryption of stored information is employed as an access enforcement mechanism, it shall be encrypted using validated cryptographic modules (see 06.d). Data stored in the information system shall be protected with system access controls and shall be encrypted when residing in non-secure areas. Specific user actions that can be performed on the information system without identification or authentication shall be identified and supporting rationale documented. Actions to be performed without identification and authentication shall be permitted only to the extent necessary to accomplish mission objectives.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-3 (HIGH) • CMSRs 2013v2 AC-14 (HIGH) • CMSRs 2013v2 SC-15 (HIGH) • IRS Pub 1075 v2014 9.3.1.3 • IRS Pub 1075 v2014 9.3.1.11 • IRS Pub 1075 v2014 9.3.16.10 • IRS Pub 1075 v2014 9.4.2 (E.10) • IRS Pub 1075 v2014 9.4.14 • MARS-E v1 AC-3 • MARS-E v1 AC-14 • MARS-E v1 AC-14(1) • MARS-E v1 SC-15 • NIST SP 800-53 R4 AC-3 • NIST SP 800-53 R4 AC-14 • NIST SP 800-53 R4 SC-15

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	Processing PHI: Yes - AND -, Accessible from the Internet: Yes, Third Party Support (Vendor Access or Maintenance): Yes
Level 3 Regulatory Factors:	Subject to PCI Compliance,

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation:	Level 2 plus: For individuals accessing sensitive information (e.g., covered information, cardholder data) from a remote location, prohibit the copy, move, print (and print screen) and storage of this information onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. The organization shall restrict the use of database management utilities to only authorized database administrators. Users shall be prevented from accessing database data files at the logical data view, field, or field-value levels. Column-level access controls shall be implemented to restrict database access.
Level 3 Control Standard Mapping:	• NRS 603A.215.1 • PCI DSS v3 8.7 • PCI DSS v3 12.3.10

CMS Contractor Requirements

CMS Contractors:	Encryption as access enforcement shall extend to all government and non-government furnished desktop computers that store sensitive information. While encryption is the preferred technical solution for protection of sensitive information on all desktop computers, adequate physical security controls and other management controls are acceptable mitigations for the protection of desktop computers with the approval of the CIO or his/her designated representative. If encryption is used as an access control mechanism it must meet CMS approved (FIPS 140-2 compliant and a NIST validated module) encryption standards.

FTI Requirements

FTI Custodians:	Access to FTI must be explicitly authorized on a strictly on a need-to-know basis. FTI must never be indiscriminately disseminated, even within the recipient agency, body, or commission. No person should be given more FTI than is needed for performance of his/her duties. Document and provide supporting rationale in the SSR for the information system the user actions not requiring identification or authentication. The organization shall ensure that only authorized users with a demonstrated need-to-know can query FTI data within a data warehouse. To use a virtual environment that receives, processes, stores, or transmits FTI, the agency must restrict access to FTI to authorized users when FTI is stored in

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	a shared location.

PCI-DSS Requirements

PCI Data:	Where there is an authorized business need to allow the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media for personnel accessing cardholder data via remote-access technologies, the organization's usage policies shall require the data be protected in accordance with all applicable PCI DSS requirements. All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: i. all user access to, user queries of, and user actions on databases are through programmatic methods. ii. only database administrators have the ability to directly access or query databases. Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

Control Reference: 01.w Sensitive System Isolation

Control Specification:	Sensitive systems shall have a dedicated and isolated computing environment. *Required for HITRUST Certification 2015
Factor Type:	System
Topics:	IT Organization and Management Roles and Responsibilities Network Segmentation Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The sensitivity of an application system shall be explicitly identified and documented by the application owner.
Level 1 Control	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Standard Mapping:	

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: The sensitive application system shall run on a dedicated computer, or only share resources with trusted applications systems. Isolation shall be achieved using physical or logical methods. When a sensitive application is to run in a shared environment, the application systems with which it will share resources and the corresponding risks should be identified and accepted by the owner of the sensitive application.
Level 2 Control Standard Mapping:	• ISO/IEC 27002-2005 11.6.2 • ISO 27799-2008 7.8.5.2 • NIST Cybersecurity Framework PR.AC-5 • NIST SP 800-53 R4 SC-4

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 5,500
Level 3 Regulatory Factors:	Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements; Subject to PCI Compliance
Level 3 Implementation:	Level 2 plus: Users of shared system resources cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user. System resources shared between two (2) or more users are released back to

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	the information system, and are protected from accidental or purposeful disclosure. Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) If virtualization technologies are used, verify that one component or primary function is implemented per virtual system device. The information system maintains a separate execution domain for each executing process.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 SC-4 (HIGH) • CMSRs 2013v2 SC-7(21) (HIGH) • CMSRs 2013v2 SC-39 (HIGH) • IRS Pub 1075 v2014 9.3.16.3 • IRS Pub 1075 v2014 9.4.1 • MARS-E v1 SC-4 • PCI DSS v3 2.2.1 • 1 TAC § 390.2(a)(4)(A)(xi)

CMS Contractor Requirements

CMS Contractors:	The organization employs boundary protection mechanisms to separate defined information system components (defined in the applicable security plan) supporting CMS missions and/or business functions. The organization ensures that system resources shared between two (2) or more users are released back to the information system, and are protected from accidental or purposeful disclosure.

FTI Requirements

FTI Custodians:	When authorized to make further disclosures is present (e.g., agents/contractors), information disclosed outside the organization must be recorded on a separate list that reflects to whom the disclosure was made, what was disclosed, and why and when it was disclosed. Organizations transmitting FTI from one computer to another need only identify the bulk records transmitted. This identification will contain the approximate number of personal records, the date of the transmissions, the best possible description of the records, and the name of the individual making/receiving the transmission. Software, data, and services that receive, process, store, or transmit FTI must be isolated within a cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The organization ensures that system resources shared between two (2) or more users are released back to the information system, and are protected from accidental or purposeful disclosure.

Objective Name: 01.07 Mobile Computing and Teleworking

Control Objective:	To ensure the security of information when using mobile computing devices and teleworking facilities.

Control Reference: 01.x Mobile Computing and Communications

Control Specification:	A formal policy shall be in place, and appropriate security measures shall be adopted to protect against the risks of using mobile computing and communication devices. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Communications and Transmissions Cryptography Data Loss Prevention Media and Assets Physical and Facility Security Policies and Procedures Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Mobile Devices Used: Yes, Processing PHI: Yes
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to State of Massachusetts Data Protection Act, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	The organization shall use full-disk encryption to protect the confidentiality of information on laptops and other mobile devices that support full-disk encryption. Encryption shall be required for all other mobile computing devices in accordance with the organization's data protection policy (see

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	06.d). If it is determined that encryption is not reasonable and appropriate, the organization shall document its rationale and acceptance of risk. A mobile computing policy shall be developed and include the requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection. This policy shall also include rules and advice on connecting mobile devices to networks and guidance on the use of these devices in public places. Protection shall be in place when using mobile computing devices in public places, meeting rooms and other unprotected areas outside of the organization's premises to avoid the unauthorized access to or disclosure of the information stored and processed by these devices (e.g., using cryptographic techniques). Users of mobile computing devices in public places shall take care to avoid the risk of overlooking by unauthorized persons. The organization shall install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network. Suitable protection shall be given to the use of mobile devices connected to networks. The organization shall only authorize connections of mobile devices meeting organizational usage restrictions, configuration requirements, connection requirements, and implementation guidance; enforce requirements for the connection of mobile devices to sensitive information systems; and monitor for unauthorized connections. Information system functionality on mobile devices that provides the capability for automatic execution of code without user direction shall be disabled. Individuals shall be issued specifically configured mobile devices for travel to locations the organization deems to be of significant risk in accordance with organizational policies and procedures. The devices shall be checked for malware and physical tampering upon return from these locations. Mobile computing devices shall also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers, and meeting places. A specific procedure taking into account legal, insurance and other security requirements of the organization shall be established for cases of theft or loss of the mobile computing devices. Equipment carrying important, covered, and/or critical business information shall not be left unattended without being physically protected. Training shall be arranged for personnel using mobile computing to raise their awareness on the additional risks resulting from this way of working and the

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	controls that shall be implemented.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-19 (HIGH) • CMSRs 2013v2 AC-19(5) (HIGH) • CMSRs 2013v2 CM-2(7) (HIGH) • CSA IS-32 • HIPAA § 164.310(b) • ISO/IEC 27002-2005 11.7.1 • ISO/IEC 27002-2013 A.6.2.1 • IRS Pub 1075 v2014 4.5 • IRS Pub 1075 v2014 9.3.1.14 • IRS Pub 1075 v2014 9.4.8 • ISO 27799-2008 7.8.6.1 • MARS-E v1 AC-19 • NIST Cybersecurity Framework PR.DS-1 • NIST Cybersecurity Framework PR.IP-1 • NIST SP 800-53 R4 AC-19 • NIST SP 800-53 R4 AC-19(5) • NIST SP 800-53 R4 CM-2(7) • NRS 603A.215.1 • PCI DSS v3 1.4 • (State of Mass.) 201 CMR 17.04(5) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization ensures the CIO authorizes the connection of mobile devices to organizational information systems.

FTI Requirements

FTI Custodians:	Purge/wipe information from mobile devices based on 10 consecutive, unsuccessful device logon attempts (e.g., personal digital assistants, smartphones and tablets). Laptop computers are excluded from this requirement. To use FTI in a mobile device environment, including BYOD, the agency must meet the following mandatory requirements: i. Mobile device management controls must be in place that include security policies and procedures, inventory, and standardized security configurations for all devices; ii. An annual risk assessment must be conducted of the security controls in place on all devices in the mobile environment used for receiving, processing, storing, or transmitting FTI; iii. Protection mechanisms must be in place in case a mobile device is lost or stolen—all data stored on the device must be encrypted, including internal storage and removable media storage, such as Micro Secure Digital (SD) cards; iv. All data communication with the agency's internal network must be encrypted using a cryptographic module that is FIPS 140-2 compliant; v. The agency must control end user ability to download only authorized vi. applications to the device and must limit the accessibility to FTI by applications to only authorized applications; vii. All mobile device management servers that receive, process, store, or transmit FTI must be hardened; viii. A centralized mobile device management solution must be used to authenticate agency-issued and personally owned mobile devices prior to allowing access to the internal network; ix. Security events must be logged for all mobile devices and the mobile device management server; x. The agency must disable wireless personal area networks that allow a mobile device to connect to a computer via Bluetooth or near field communication (NFC) for data synchronization and storage; xi. Access to hardware, such as the digital camera, global positioning

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	system (GPS), and universal serial bus (USB) interface, must be disabled to the extent possible; and xii. Disposal of all mobile device component hardware follows the same media sanitization and disposal procedures as other media.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	If the connection of portable and mobile devices is authorized, the organization: i. Employs an approved method of cryptography (see SC-13) to protect information residing on portable and mobile information devices, and utilizes whole-disk encryption solution for laptops; ii. Monitors for unauthorized connections of mobile devices to information systems; iii. Enforces requirements for the connection of mobile devices to information systems; iv. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction; v. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and vi. Protects the storage and transmission of information on portable and mobile information devices with activities such as scanning the devices for malicious code, virus protection software.

Control Reference: 01.y Teleworking

Control Specification:	A policy, operational plans and procedures shall be developed and implemented for teleworking activities. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Authorization Communications and Transmissions IT Organization and Management Roles and Responsibilities Media and Assets Personnel User Access Network Security

Level 1 Implementation Requirements

Level 1 Organizational	Applicable to all organizations

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance
Level 1 Implementation:	Organizations shall only authorize teleworking activities if they are satisfied that appropriate security arrangements and controls are in place, and that these comply with the organization's security policy. Suitable protection of the teleworking site shall be in place to protect against the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse of facilities. The following matters shall be addressed: i. the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and pass over the communication link and the sensitivity of the internal system; ii. the use of home networks and requirements or restrictions on the configuration of wireless network services including encryption (WPA at a minimum); iii. anti-virus protection, operating system and application patching, and firewall requirements consistent with corporate policy; and iv. revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated. Verifiable unique IDs shall be required for all teleworkers accessing the organization's network via a remote connection. The connection between the organization and the teleworker's location shall be secured via an encrypted channel. The organization shall maintain ownership over the assets used by the teleworker in order to achieve the requirements of this control (e.g., issuance of a USB device to allow for remote access via an encrypted tunnel). Teleworking activities shall both be authorized and controlled by management, and it shall be ensured that suitable arrangements are in place for this way of working. Training on security awareness, privacy and teleworker responsibilities shall be required prior to authorization and training methods shall be reviewed in accordance with the organization's policy (see 02.e).
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-17 (HIGH) • HIPAA § 164.310(a)(2)(i) • HIPAA § 164.310(b) • IRS Pub 1075 v2014 9.3.1.12 • MARS-E v1 AC-17 • NIST Cybersecurity Framework PR.AC-3 • NIST Cybersecurity Framework PR.DS-1 • NIST Cybersecurity Framework PR.DS-3

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST Cybersecurity Framework PR.IP-1 • NIST SP 800-53 R4 AC-17 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: The following matters shall be addressed prior to authorizing teleworking: i. the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment; ii. the proposed physical teleworking environment; and iii. the threat of unauthorized access to information or resources from other persons using the accommodation (e.g., family and friends).
Level 2 Control Standard Mapping:	• NIST SP 800-53 R4 PE-17

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to PCI Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation:	Level 2 plus: The following matters shall be addressed prior to authorizing teleworking: i. a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access; ii. the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the organization is not allowed; iii. the provision of suitable communication equipment, including methods for securing remote access; iv. rules and guidance on family and visitor access to equipment and information; v. the provision of hardware and software support and maintenance; vi. the provision of insurance; vii. the procedures for back-up and business continuity; viii. the provision of a means for teleworkers to communicate with information security personnel in case of security incidents or problems; and ix. audit and security monitoring. The organization shall instruct all personnel working from home to implement fundamental security controls and practices, including but not limited to passwords, virus protection, personal firewalls, laptop cable locks, recording serial numbers and other identification information about laptops, and disconnecting modems at alternate worksites. Remote access shall be limited only to information resources required by home users to complete job duties. Any organization-owned equipment shall only be used only for business purposes by authorized employees.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 PE-17 (HIGH) • IRS Pub 1075 v2014 4.5 • IRS Pub 1075 v2014 4.7 • IRS Pub 1075 v2014 4.7.1 • IRS Pub 1075 v2014 4.7.2 • IRS Pub 1075 v2014 9.3.11.9 • ISO/IEC 27002-2005 11.7.2 • ISO/IEC 27002-2013 A.6.2.2 • ISO 27799-2008 7.8.6.2 • MARS-E v1 PE-17

FTI Requirements

FTI Custodians:	If the agency allows alternative work sites, such as an employee's home or other non-traditional work sites, the FTI remains subject to the same safeguard requirements as the agency's offices and the highest level of attainable security (see also IRS Pub 1075 v2014 4.5)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization addresses how it will meet its minimum protection standards for FTI at alternate worksites (e.g., employee's homes or other non-traditional work sites). The agency should conduct and fully document periodic inspections of alternative work sites during the year to ensure that safeguards are adequate. The agency must retain ownership and control, for all hardware, software, and end-point equipment connecting to public communication networks, where these are resident at all alternate work sites. Employees must have a specific room or area in a room that has the appropriate space and facilities for the type of work done. The agency must give employees locking file cabinets or desk drawers so that documents, disks, and tax returns may be properly secured when not in use. If agency furniture is not furnished to the employee, the agency must ensure that an adequate means of storage exists at the work site. The agency must provide "locking hardware" to secure automated data processing equipment to large objects, such as desks or tables. Smaller, agency-owned equipment must be locked in a filing cabinet or desk drawer when not in use. FTI may be stored on hard disks only if agency-approved security access control devices (hardware/software) have been installed; are receiving regularly scheduled maintenance, including upgrades; and are being used. Access control must include password security, an audit trail, encryption, virus detection, and data overwriting capabilities. Computers and electronic media that receive, process, store, or transmit FTI must be in a secure area with restricted access. In situations when requirements of a secure area with restricted access cannot be maintained, such as home work sites, remote terminals or other office work sites, the equipment must receive the highest level of protection practical, including full disk encryption. All computers and mobile devices that contain FTI and are resident in an alternate work site must employ encryption mechanisms to ensure that this data may not be accessed, if the computer is lost or stolen.

Control Category: 02.0 - Human Resources Security

Objective Name: 02.01 Prior to Employment

Control Objective:	To ensure that employees, contractors and third party users are suitable for the roles for which they are being considered, to reduce the risk of fraud,

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	theft, or misuse of facilities.

Control Reference: 02.a Roles and Responsibilities

Control Specification:	Security roles and responsibilities of employees, contractors and third party users shall be defined and documented in accordance with the organization's information security policy. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Awareness and Training Incident Response IT Organization and Management Roles and Responsibilities Personnel Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance
Level 1 Implementation:	The organization shall develop, disseminate, and review/update annually: i. a formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ii. formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls. iii. Security roles and responsibilities shall include the following requirements: iv. implement and act in accordance with the organization's information security policies; v. protect assets from unauthorized access, disclosure, modification, destruction or interference; vi. execute particular security processes or activities; vii. ensure responsibility is assigned to the individual for actions taken; and viii. report security events or potential events or other security risks to the organization.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Security roles and responsibilities shall be defined and clearly communicated to job candidates during the pre-employment process. Security roles and responsibilities, as laid down in the organization's information security policy, as well as any involvement in processing covered information shall be documented in relevant job descriptions.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PS-1 (HIGH) • CSA IS-13 • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(3)(ii)(B) • HIPAA § 164.308(a)(3)(ii)(C) • IRS Pub 1075 v2014 9.3.13.1 • ISO/IEC 27002-2005 8.1.1 • ISO/IEC 27002-2013 A.6.1.1 • ISO 27799-2008 7.5.1.1 • MARS-E v1 PS-1 • NIST Cybersecurity Framework ID.AM-6 • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework PR.IP-11 • NIST Cybersecurity Framework DE.DP-1 • NIST SP 800-53 R4 PS-1 • PCI DSS v3 12.4 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance; Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The pre-employment process shall be reviewed by recruitment to ensure security roles and responsibilities are defined and clearly communicated to job candidates. The organization shall assign risk designations to all organizational positions as appropriate, establish screening criteria, and review and revise designations every three hundred and sixty-five (365) days.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization shall define the roles, responsibilities and authority of all security personnel.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 PS-2 (HIGH) • IRS Pub 1075 v2014 9.3.13.2 • MARS-E v1 PS-2 • NIST SP 800-53 R4 PS-2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 02.b Screening

Control Specification:	Background verification checks on all candidates for employment, contractors, and third party users shall be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.
Factor Type:	Organizational
Topics:	Authorization IT Organization and Management Roles and Responsibilities Personnel Requirements (Legal and Contractual) Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1	Subject to PCI Compliance

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Regulatory Factors:	
Level 1 Implementation:	Verification checks shall take into account all relevant privacy, protection of covered data and/or employment based legislation, and where permitted and appropriate, include the following: i. availability of satisfactory character references (e.g., one business and one personal); ii. a check (for completeness and accuracy) of the applicant's curriculum vitae; iii. confirmation of claimed academic and professional qualifications; and iv. independent identity check (passport or similar document). All applicants shall be required to complete an I-9 form to verify that they are eligible to work in the United States. Where a job, either on initial appointment or on promotion, involves the person having access to information assets, and in particular those handling covered information (e.g. financial information, personal health information or highly confidential information) the organization shall, at a minimum, verify the identity, current address and previous employment of such staff. Procedures shall define criteria and limitations for verification checks (e.g., who is eligible to screen people, and how, when and why verification checks are carried out). Information on all candidates being considered for positions within the organization shall be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates shall be informed beforehand about the screening activities.
Level 1 Control Standard Mapping:	• CSA HR-01 • HIPAA § 164.308(a)(3)(ii)(B) • ISO/IEC 27002-2005 8.1.2 • ISO/IEC 27002-2013 A.7.1.1 • ISO 27799-2008 7.5.1.2 • NIST Cybersecurity Framework PR.DS-5 • NIST Cybersecurity Framework PR.IP-11 • NIST SP 800-53 R4 PS-3 • NRS 603A.215.1 • PCI DSS v3 12.7 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: >

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall have a HR representative as a single point of contact for performing the screening process on applicants. The organization shall develop a standard criteria screening process to be carried out on all applicants. The organization shall screen individuals requiring access to organizational information and before authorizing access. The organization shall assign risk designation to all positions and established criteria for individuals filling those positions. Applicants shall be screened in accordance with applicable regional policies/procedures that may require screening in the following areas: i. health screening; ii. drug screening; and iii. motor vehicle driving record (in accordance with job requirements). Criminal background checks shall be undertaken prior to employment. The organization shall rescreen individuals periodically, consistent with the criticality/sensitivity rating of the position and, when an employee moves from one position to another, any higher level of access (clearance) should be adjudicated. The organization shall consider applicable state and federal law (reference 02.b, level 1) with regards to information exchanged in the notification process with business associates described in 05.k, level 1, which is meant to ensure third party workforce members pass verification checks prior to employment. If there has been a long gap, at a minimum five years, between recruitment and the date of the employee starting, the organization shall repeat the screening process, or its key elements.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 PS-3 (HIGH) • IRS Pub 1075 v2014 9.3.13.3 • IRS Pub 1075 v2014 9.4.2 (E.10) • MARS-E v1 PS-3

Level 3 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	Level 2 plus: The organization shall specifically define an individual who performs all screening checks. The organization shall document and maintain a list of all screened applicants with assigned risk. Credit checks shall be carried out for personnel who will have access to financial information.
Level 3 Control Standard Mapping:	None

CMS Contractor Requirements

CMS Contractors:	Require that individuals with significant security responsibilities be assigned and hold, at a minimum, a Level 5 Public Trust sensitivity level clearance as defined in the HHS Personnel Security/Suitability Handbook. Assign other individuals with Public Trust positions the appropriate sensitivity level as defined in the HHS Personnel Security/Suitability Handbook.

FTI Requirements

FTI Custodians:	Individuals must be screened before authorizing access to information systems and devices containing FTI. Organizations should consider additional background checks for staff members with administrator access to the entire set of FTI records.

Objective Name: 02.02 During On-Boarding

Control	To ensure agreements are signed by employees, contractors and third party

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Objective:	users of information assets on their security roles and responsibilities at the time of their employment or engagement, prior to access being granted.

Control Reference: 02.c Terms and Conditions of Employment

Control Specification:	As part of their contractual obligation, employees, contractors and third party users shall agree and sign the terms and conditions of their employment contract, which shall include their responsibilities for information security.
Factor Type:	Organizational
Topics:	Documentation and Records IT Organization and Management Roles and Responsibilities Personnel Requirements (Legal and Contractual) Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	The terms and conditions of employment shall reflect the organization's security policy, in addition to clarifying and stating the following: i. that all employees, contractors and third party users who are given access to covered information shall sign a confidentiality or non-disclosure agreement prior to being given access to information assets; ii. the employee's, contractor's and any other user's legal responsibilities and rights (e.g., regarding copyright laws or data protection legislation); iii. responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor or third party user; iv. responsibilities of the employee, contractor or third party user for the handling of information received from other companies or external parties; v. responsibilities of the organization for the handling of covered information, including covered information created as a result of, or in the course of, employment with the organization; vi. responsibilities that are extended outside the organization's premises and outside normal working hours (e.g., in the case of home-working); vii. actions to be taken if the employee, contractor or third party user

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	disregards the organization's security requirements; and viii. ensure that conditions relating to security policy survive the completion of the employment in perpetuity. The organization shall ensure that employees, contractors and third party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services. The organization shall develop and document access agreements for organizational systems and privileges shall not be granted until the terms and conditions of employment have been satisfied and agreements have been signed.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PL-4 (HIGH) • CMSRs 2013v2 PS-6 (HIGH) • CSA HR-02 • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(3)(ii)(B) • HIPAA § 164.308(a)(4)(ii)(B) • HIPAA § 164.310(b) • HIPAA § 164.310(d)(2)(iii) • HIPAA § 164.314(a)(1) • HIPAA § 164.314(a)(2)(i) • HIPAA § 164.314(a)(2)(ii) • IRS Pub 1075 v2014 9.3.12.3 • IRS Pub 1075 v2014 9.3.13.6 • MARS-E v1 PL-4 • MARS-E v1 PS-6 • NIST Cybersecurity Framework ID.AM-6 • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework PR.DS-5 • NIST Cybersecurity Framework PR.IP-11 • NIST SP 800-53 R4 PL-4 • NIST SP 800-53 R4 PS-6 • NRS 603A.215.1 • PCI DSS v3 12.4 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: The organization shall maintain a list of all authorized signed non-disclosure agreement (NDA) forms. This list shall be kept up to date to reflect personnel changes and departures. Responsibilities contained within the terms and conditions of employment shall continue for a defined period after the end of the employment. The terms and conditions of employment should: i. include reference to the penalties that are possible when breach of the information security policy is identified; ii. ensure that conditions relating to confidentiality of personal health information survive the completion of the employment for the maximum period allowed under applicable federal and state laws and regulations. With respect to clinical staff, the terms and conditions of employment should specify what rights of access such staff will have to the records of subjects of care and to the associated health information systems in the event of third-party claims.
Level 2 Control Standard Mapping:	• ISO/IEC 27002-2005 8.1.3 • ISO/IEC 27002-2013 A.7.1.2 • ISO 27799-2008 7.5.1.3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements
Level 3 Control	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Standard Mapping:	

CMS Contractor Requirements

CMS Contractors:	The organization shall review/update the access agreements as part of the system security authorization or when a contract is renewed or extended, but minimally within every three hundred sixty-five (365) days, whichever occurs first. The organization shall: i. ensure that individuals requiring access to organizational information or information systems acknowledge (paper or electronic) appropriate access agreements prior to being granted access; and ii. re-acknowledge access agreements to maintain access to organizational information systems when access agreements have been updated.

FTI Requirements

FTI Custodians:	Agencies must review information system access authorizations and initiate appropriate actions when personnel are reassigned or transferred to other positions within the organization.

Objective Name: 02.03 During Employment

Control Objective:	To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

Control Reference: 02.d Management Responsibilities

Control Specification:	Management shall require employees, and where applicable contractors and third party users, to apply security in accordance with established policies and procedures of the organization. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	IT Organization and Management Roles and Responsibilities Personnel Policies and Procedures Third Parties and Contractors

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Management responsibilities shall include ensuring that employees, contractors and third party users: i. are properly briefed on their information security roles and responsibilities prior to being granted access to covered information or information systems; ii. are provided with guidelines to state security expectations of their role within the organization; iii. are motivated and comply with the security policies of the organization; iv. achieve a level of awareness on security relevant to their roles and responsibilities within the organization v. conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working; and vi. continue to have the appropriate skills and qualifications. The organization shall establish an information security workforce development and improvement program. The organization shall: i. implement a process for ensuring that organization plans for conducting security testing, training, and monitoring activities associated with organizational information systems: a. are developed and maintained; and b. continue to be executed in a timely manner; ii. review testing, training, and monitoring plans for consistency with the organization risk management strategy and organization-wide priorities for risk response actions. The organization shall develop usage policies for critical employee-facing technologies to define proper use of these technologies for all employees and contractors.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PM-13 (HIGH) • CMSRs 2013v2 PM-15 (HIGH) • CMSRs 2013v2 PS-7 (HIGH)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• CSA IS-14 • CSA IS-16 • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(4)(ii)(B) • HIPAA § 164.308(b)(1) • HIPAA § 164.314(a)(1) • HIPAA § 164.314(a)(2)(i) • HIPAA § 164.314(a)(2)(ii) • IRS Pub 1075 v2014 9.3.13.7 • ISO/IEC 27002-2005 8.2.1 • ISO/IEC 27002-2013 A.7.2.1 • MARS-E v1 PS-7 • NIST Cybersecurity Framework ID.AM-6 • NIST Cybersecurity Framework PR.AT-1 • NIST Cybersecurity Framework PR.AT-2 • NIST Cybersecurity Framework PR.AT-3 • NIST Cybersecurity Framework PR.AT-4 • NIST Cybersecurity Framework PR.AT-5 • NIST Cybersecurity Framework PR.IP-11 • NIST Cybersecurity Framework DE.CM-6 • NIST Cybersecurity Framework DE.DP-1 • NIST SP 800-53 R4 PM-13 • NIST SP 800-53 R4 PM-15 • NIST SP 800-53 R4 PS-7 • PCI DSS v3 12.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Requirements (High)Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall assign an individual or team to manage information security responsibilities of employees, contractors and third party users.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	For all system connections that allow customers to access the computing assets such as web sites, kiosks and public access terminals, the organization shall ensure the following: i. provide appropriate text or a link to the privacy policy for data use and protection as well as the customer's responsibilities when accessing the data; and ii. have a formal mechanism to authenticate the customer's identity prior to granting access to covered information. These usage policies shall address the following if applicable: i. explicit management approval (authorization) to use the technology; ii. authentication for use of the technology; iii. acceptable uses of the technologies (see 07.c), with special emphasis on the inappropriate access by health workers of personal health information of neighbors, colleagues and relatives; iv. acceptable network locations for the technologies; v. list of company- approved products; vi. activation of modems for vendors only when needed by vendors, with immediate deactivation after use; and vii. prohibition of storage of covered data onto local hard drives, floppy disks, or other external media.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 PL-4 (HIGH) • IRS Pub 1075 v2014 9.3.12.3 • ISO 27799-2008 7.5.2.1 • MARS-E v1 PL-4 • NIST SP 800-53 R4 PL-4 • NRS 603A.215.1 • PCI DSS v3 12.3.1 • PCI DSS v3 12.3.2 • PCI DSS v3 12.3.6 • PCI DSS v3 12.3.7

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 02.e Information Security Awareness, Education and Training

Control Specification:	All employees of the organization and contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Awareness and Training IT Organization and Management Roles and Responsibilities Personnel Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	Awareness training shall commence with a formal induction process designed to introduce the organization's security and privacy policies, state and federal laws, and expectations before access to information or services is granted and no later than 60 days after the date the employee is hired. Ongoing training shall include security and privacy requirements (e.g., objective, scope, roles and responsibilities, coordination, compliance, legal responsibilities and business controls) as well as training in the correct use of information assets and facilities (e.g., log-on procedures, use of software packages and information on the disciplinary process). The organization provides incident response and contingency training to information system users consistent with assigned roles and responsibilities: i. within ninety (90) days of assuming an incident response role or responsibility; ii. when required by information system changes; and iii. within every three hundred sixty-five (365) days thereafter. The organization shall document that the training has been provided to the individual.
Level 1 Control Standard	• CMSRs 2013v2 AT-1 (HIGH)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Mapping:	• CMSRs 2013v2 CP-3 (HIGH) • CMSRs 2013v2 CP-3(1) (HIGH) • CMSRs 2013v2 IR-2 (HIGH) • CMSRs 2013v2 PM-14 (HIGH) • CSA IS-11 • HIPAA § 164.308(a)(5)(i) • HIPAA § 164.308(a)(5)(ii)(A) • HIPAA § 164.308(a)(5)(ii)(B) • HIPAA § 164.308(a)(6)(i) • HIPAA § 164.308(a)(7)(ii)(D) • HIPAA § 164.414(a) • IRS Pub 1075 v2014 9.3.2.1 • IRS Pub 1075 v2014 9.3.6.3 • IRS Pub 1075 v2014 9.3.8.2 • ISO/IEC 27002-2005 8.2.2 • ISO/IEC 27002-2013 A.7.2.2 • ISO 27799-2008 7.5.2.2 • MARS-E v1 AT-1 • MARS-E v1 CP-3 • MARS-E v1 CP-4 • MARS-E v1 IR-2 • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework PR.AT-1 • NIST Cybersecurity Framework PR.AT-2 • NIST Cybersecurity Framework PR.AT-4 • NIST Cybersecurity Framework PR.AT-5 • NIST SP 800-53 R4 AT-1 • NIST SP 800-53 R4 CP-3 • NIST SP 800-53 R4 IR-2 • NIST SP 800-53 R4 PM-14 • NIST SP 800-53 R4 AR-5 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.04(8) • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(2) • HIPAA § 164.530(b)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	> 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FTC Red Flags Rule Compliance
Level 2 Implementation:	Level 1 plus: The organization formally creates dedicated security awareness training as part of a resource on-boarding process to the organization. The organization documents its formal induction security awareness training process. The organization conducts an internal annual review of the effectiveness of its security and privacy education and training program. The organization manages a security and privacy education and training program for all employees and contractors with tracking of completion and a requirement for refresher training at least every three hundred and sixty-five (365) days. Employees shall be required to acknowledge they have received training and are aware their responsibilities through signoff. The organization shall include security awareness training on recognizing and reporting potential indicators of an insider threat. The organization's security personnel, including organizational business unit security points of contact, shall receive specialized security education and training appropriate to their role/responsibilities. Train developers in secure coding techniques, including how to avoid common coding vulnerabilities. Ensure developers understand how sensitive data is handled in memory.
Level 2 Control Standard Mapping:	• 16 CFR Part §681.2(e)(3) • CMSRs 2013v2 AT-2 (HIGH) • CMSRs 2013v2 AT-2(2) (HIGH) • CMSRs 2013v2 IR-2(1) (HIGH) • CMSRs 2013v2 IR-2(2) (HIGH) • IRS Pub 1075 v2014 9.3.2.2 • MARS-E v1 AT-2 • NIST SP 800-53 R4 AT-2 • NIST SP 800-53 R4 AT-2(2) • NRS 603A.215.1 • PCI DSS v3 6.5 • PCI DSS v3 9.9 • PCI DSS v3 9.9.3 • PCI DSS v3 12.6 • PCI DSS v3 12.6.1 • PCI DSS v3 12.6.2 • 1 TAC § 390.2(a)(3)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Pharmaceutical Companies: > 70,000,000 Prescriptions Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: Personnel with significant information security roles and responsibilities shall be required to undergo appropriate role-based information system security training: i. prior to authorizing access to the organization's networks, systems, and/or applications; ii. when required by significant information system or system environment changes; iii. when an employee enters a new position that requires additional role-specific training; and iv. refresher training annually thereafter. The organization shall maintain a documented list of each individual who completes the on-boarding process. Training records shall be retained for at least five (5) years thereafter.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 AT-3 (HIGH) • CMSRs 2013v2 AT-4 (HIGH) • CMSRs 2013v2 SA-16 (HIGH) • IRS Pub 1075 v2014 9.3.2.3 • IRS Pub 1075 v2014 9.3.2.4 • IRS Pub 1075 v2014 9.4.2 (E.10) • MARS-E v1 AT-3 • MARS-E v1 AT-4 • NIST SP 800-53 R4 AT-3 • NIST SP 800-53 R4 AT-4

CMS Contractor Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

CMS Contractors:	The organization shall incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations. The organization employs automated mechanisms to provide a more thorough and realistic training environment The organization requires the developer of the information system, system component, or information system service to provide appropriate training (or training materials), for affected personnel, on the correct use and operation of the implemented security functions, controls, and/or mechanisms.

Federal Requirements

Federal Agencies and Contractors:	The organization shall establish and implement an Operations Security (OPSEC) program.

FTI Requirements

FTI Custodians:	Awareness training specific to protecting and disclosing FTI, including how FTI security requirements are communicated to end users, and the (possible) sanctions for misuse of FTI must be provided initially prior to granting access to FTI and annually thereafter. The disclosure awareness (training) requirements apply to all agency employees with access to FTI, including program and information technology personnel and contractors, such as case workers, managers, system administrators, database administrators and application developers. Training shall be user specific to ensure that all personnel receive appropriate training for a particular job, such as training required for administrators or auditors. Granting employees or contractors access to FTI must be preceded by each employee or contractor certifying his/her understanding of the agency's security policy and procedures for safeguarding FTI. The certification must be maintained for 5 years. The organization provides refresher training prior to access of FTI and annually thereafter on incident response policy and procedure regarding FTI. The agency must provide contingency and incident response training to information system users consistent with assigned roles and responsibilities prior to assuming a contingency role or responsibility.

PCI-DSS Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

PCI Data:	The organization shall ensure the importance of cardholder data security is included in a formal security awareness program for all personnel. The organization shall train personnel to be aware of attempted tampering or replacement of devices. Training should include the following: i. Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. ii. Do not install, replace, or return devices without verification. iii. Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). iv. Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).

Control Reference: 02.f Disciplinary Process

Control Specification:	There shall be a formal disciplinary process for employees who have violated security policies and procedures. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Documentation and Records Incident Response IT Organization and Management Roles and Responsibilities Personnel Policies and Procedures Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to State of Massachusetts Data Protection Act, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures and notifies defined personnel (e.g., supervisors) within a defined time frame (e.g., 24 hours) when a formal sanction process is initiated, identifying the individual sanctioned and the reason for the sanction. The disciplinary process

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	shall not be commenced without prior verification that a security breach has occurred. The formal disciplinary process shall ensure correct and fair treatment for employees who are suspected of committing breaches of security. The formal disciplinary process shall provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offense, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required. The organization shall include specific procedures for license, registration, and certification denial or revocation and other disciplinary action. The organization shall maintain a list or document an indication of employees involved in security incident investigations and the resulting outcome in their HR folder.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PS-8 (HIGH) • CSA IS-06 • HIPAA § 164.308(a)(1)(ii)(C) • HIPAA § 164.414(a) • IRS Pub 1075 v2014 9.3.13.8 • ISO/IEC 27002-2005 8.2.3 • ISO/IEC 27002-2013 A.7.2.3 • ISO 27799-2008 7.5.2.3 • MARS-E v1 PS-8 • NIST Cybersecurity Framework PR.IP-11 • NIST SP 800-53 R4 PS-8 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.03(2)(d) • 1 TAC § 390.2(a)(1) • 1 TAC § 3902.(a)(4)(B)(xviii)(I) • 1 TAC § 390.2(a)(4)(B)(xviii)(II) • 1 TAC § 390.2(a)(4)(B)(xviii)(III) • HIPAA § 164.530(e)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: The organization shall create a point of contact from HR to handle any incidents relating to employees. The organization shall notify the CISO or a designated representative of the application of a formal employee sanctions process, identifying the individual and the reason for the sanction.
Level 2 Control Standard Mapping:	None

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Objective Name: 02.04 Termination or Change of Employment

Control Objective:	To ensure that the access rights are properly removed, and assets recovered for terminated employees and contractors, and for employees who have changed employment.

Control Reference: 02.g Termination or Change Responsibilities

Control Specification:	Responsibilities for performing employment termination or change of employment shall be clearly defined and assigned.
Factor Type:	Organizational
Topics:	Awareness and Training IT Organization and Management Roles and Responsibilities

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Personnel Requirements (Legal and Contractual) Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Logical and physical access authorizations to systems and equipment shall be reviewed, updated or revoked when there is any change in responsibility or employment. The organization shall formally address: i. terminating access when the access is no longer needed, ii. assignment of responsibility for removing information system and/or physical access, and iii. timely communication of termination actions to ensure that the termination procedures are appropriately followed (see 02.i). When an employee or other workforce member moves to a new position of trust, logical and physical access controls must be re-evaluated as soon as possible but not to exceed thirty (30) days.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PS-5 (HIGH) • CSA HR-03 • HIPAA § 164.308(a)(3)(ii)(C) • IRS Pub 1075 v2014 9.3.13.5 • MARS-E v1 PS-5 • NIST Cybersecurity Framework PR.IP-11 • NIST SP 800-53 R4 PS-5 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year,

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall have a documented termination process for all employees and other workforce members. The organization shall have a process where exit interviews address organization-defined information and security items, all organization information system related property and access is retrieved and revoked, knowledge transfer/information transitioned, and provides appropriate personnel with access to official records created by a terminated employee or when the arrangement of a workforce member ends. The organization shall define any valid duties after termination employment or when the arrangement of a workforce member ends and shall be included in the employee's or workforce member's contract or other arrangement. The communication of termination responsibilities shall include ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement and the terms and conditions of employment or other workforce arrangement continuing for a defined period after the end of the employee's, contractor's or third party user's employment or other workforce arrangement.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 PS-4 (HIGH) • IRS Pub 1075 v2014 9.3.13.4 • ISO/IEC 27002-2005 8.3.1 • ISO/IEC 27002-2013 A.7.3.1 • ISO 27799-2008 7.5.3.1 • MARS-E v1 PS-4 • NIST SP 800-53 R4 PS-4

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	Level 2 plus: The organization shall have a documented termination checklist that identifies all the steps to be taken and assets collected.

CMS Contractor Requirements

CMS Contractors:	All access and privileges to CMS systems, networks, and facilities are suspended when employees or contractors temporarily separate from the organization (e.g., leave of absence). The organization: i. Initiates the following transfer or reassignment actions during the formal transfer process: a. re-issuing appropriate information system-related property (e.g., keys, identification cards, building passes); b. notification to security management; c. closing obsolete accounts and establishing new accounts; and ii. notifies defined personnel or roles (defined in the applicable security plan) within one (1) business day.

Control Reference: 02.h Return of Assets

Control Specification:	All employees, contractors and third party users shall return all of the organization's assets in their possession upon termination of their employment, contract or agreement.
Factor Type:	Organizational
Topics:	Media and Assets Personnel Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to State of Massachusetts Data Protection Act, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	The termination process shall include the return of all previously issued software, corporate documents, and equipment. Other organizational assets such as mobile computing devices, credit cards, access cards, manuals, and information stored on electronic media also shall be returned. In cases where an employee, contractor or third party user purchases the organization's equipment or uses their own personal equipment, procedures shall be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment. In cases where an employee, contractor or third party user has knowledge that is important to ongoing operations, that information shall be documented and transferred to the organization.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PS-4 (HIGH) • CSA IS-27 • HIPAA § 164.308(a)(3)(ii)(C) • IRS Pub 1075 v2014 9.3.13.4 • ISO/IEC 27002-2005 8.3.2 • ISO/IEC 27002-2013 A.8.1.4 • ISO 27799-2008 7.5.3.1 • MARS-E v1 PS-4 • NIST Cybersecurity Framework PR.IP-11 • NIST SP 800-53 R4 PS-4 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.03(2)(e) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 02.i Removal of Access Rights

Control Specification:	The access rights of all employees, contractors and third party users to information and information assets shall be removed upon termination of their employment, contract or agreement, or adjusted upon a change of employment (i.e. upon transfer within the organization). *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Authorization Personnel Third Parties and Contractors User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	Upon termination, the access rights for the terminated individual shall be disabled in a timely manner, at least within 24 hours. Changes of employment or other workforce arrangement (e.g., transfers) shall be reflected in removal of all access rights that were not approved for the new employment or workforce arrangement. Access changes due to personnel transfer shall be

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	managed effectively. Old accounts shall be closed after 90 days, and new accounts shall be opened. The access rights that shall be removed or adapted include physical and logical access, keys, identification cards, IT systems and application, subscriptions, and removal from any documentation that identifies them as a current member of the organization. If a departing employee, contractor, third party user or other workforce member has known passwords for accounts remaining active, these shall be changed upon termination or change of employment, contract, agreement, or other workforce arrangement. Access rights to information assets and facilities shall be reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors including: i. whether the termination or change is initiated by the employee, contractor, third party user, other workforce member, or by management and the reason of termination; ii. the current responsibilities of the employee, contractor, workforce member or any other user; and iii. the value of the assets currently accessible.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-2 (HIGH) • CMSRs 2013v2 PS-5 (HIGH) • CSA IS-09 • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(3)(ii)(B) • HIPAA § 164.308(a)(3)(ii)(C) • HIPAA § 164.308(a)(4)(i) • HIPAA § 164.308(a)(4)(ii)(B) • HIPAA § 164.308(a)(4)(ii)(C) • HIPAA § 164.308(a)(5)(ii)(C) • HIPAA § 164.312(a)(2)(i) • HIPAA § 164.312(a)(2)(ii) • IRS Pub 1075 v2014 9.3.1.2 • IRS Pub 1075 v2014 9.3.13.5 • ISO/IEC 27002-2005 8.3.3 • ISO/IEC 27002-2013 A.9.2.6 • MARS-E v1 AC-2 • MARS-E v1 PS-5 • NIST Cybersecurity Framework PR.AC-1 • NIST Cybersecurity Framework PR.AC-4 • NIST Cybersecurity Framework PR.IP-11 • NIST SP 800-53 R4 AC-2 • NIST SP 800-53 R4 PS-4 • NIST SP 800-53 R4 PS-5 • NRS 603A.215.1 • PCI DSS v3 8.1.3 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.03(2)(e) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization employs automated mechanisms to notify specific personnel or roles (formally defined by the organization) upon termination of an individual. Organizations shall immediately terminate the access rights following the supply of a resignation notice, notice of dismissal, etc., prior to or during the personnel termination process. Termination shall allow for immediate escorting out of the site, if necessary, wherever continued access is perceived to cause an increased risk, e.g., in the case of serious misconduct.
Level 2 Control Standard Mapping:	• IRS Pub 1075 v2014 9.3.13.4 • ISO 27799-2008 7.5.3.2 • MARS-E v1 PS-4 • CMSRs 2013v2 PS-4 (HIGH) • CMSRs 2013v2 PS-4(2) (HIGH)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 3 Implementation:	No additional requirements

Provider Requirements

Providers:	All organizations that process personal health information shall, as soon as possible, terminate the user access privileges with respect to such information for any departing permanent or temporary employee, third party contractor or volunteer upon termination of employment, contracting or volunteer activities.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Category: 03.0 - Risk Management

Objective Name: 03.01 Risk Management Program

Control Objective:	To develop and implement a Risk Management Program that addresses Risk Assessments, Risk Mitigation, and Risk Evaluations.

Control Reference: 03.a Risk Management Program Development

Control Specification:	Organizations shall develop and maintain a risk management program to manage risk to an acceptable level. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Policies and Procedures Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	The organization shall: i. develop a comprehensive strategy to manage risk to organizational operations and assets, individuals, and other organizations associated with the operation and use of information systems, including physical and environmental hazards; ii. implement the strategy consistently across the organization, and iii. ensure that their information protection programs do not apply safeguards unnecessarily, e.g., to de-identified information. Elements of the risk management program shall include: i. the creation of a risk management policy for information systems and paper records that is formally approved by management and shall include:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	a. objectives of the risk management process; b. management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and healthcare-specific risk analysis; c. the connection between the risk management policy and the organization's strategic planning processes; and d. documented risk assessment processes and procedures. ii. regular performance of risk assessments; iii. mitigation of risks identified from risk assessments; iv. reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk level changes in the environment; v. updating the risk management policy if any of these elements have changed; and vi. repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PM-9 (HIGH) • CMSRs 2013v2 PM-11 (HIGH) • CMSRs 2013v2 RA-1 (HIGH) • CSA RI-01 • HIPAA § 164.308(a)(1)(i) • HIPAA § 164.316(a) • IRS Pub 1075 v2014 9.3.14.1 • MARS-E v1 PM-9 • MARS-E v1 PM-11 • MARS-E v1 RA-1 • NIST Cybersecurity Framework ID.BE-3 • NIST Cybersecurity Framework ID.GV-4 • NIST Cybersecurity Framework ID.RM-1 • NIST Cybersecurity Framework ID.RM-2 • NIST Cybersecurity Framework ID.RM-3 • NIST Cybersecurity Framework RS.MI-3 • NIST SP 800-53 R4 PM-9 • NIST SP 800-53 R4 PM-11 • NIST SP 800-53 R4 RA-1 • NIST SP 800-53 R4 AR-2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(b)

Level 2 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: Formal risk assessment and risk treatment processes shall be implemented, including a repository and tracking system for risk assessments performed, and risk mitigation completed or underway.
Level 2 Control Standard Mapping:	None

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FTC Red Flags Rule Compliance
Level 3 Implementation:	Level 2 plus: The organization shall develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of an account or any existing account that involves or is designed to permit multiple payments or transactions. The organization shall define and incorporate existing policies and implement procedures to: i. identify relevant patterns, practices, or specific activities that indicate the possible existence of identity theft for the accounts , and incorporate those patterns, practices, and activities into its program;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	ii. detect patterns, practices, and activities that have been incorporated into the program; iii. respond appropriately to any patterns, practices, and activities that are detected to prevent and mitigate identity theft; and iv. ensure the program and patterns, practices, and activities are updated at least annually, to reflect changes in risks to customers and to the safety and soundness of the organization. 'Personal identifying information' (PII) [also personally identifiable information] means information that alone or in conjunction with other information identifies an individual, including an individual's : i. Name, social security number, date of birth, or government-issued identification number; ii. Mother's maiden name; iii. Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; iv. Unique electronic identification number, address, or routing code; and v. Telecommunication access device. The organization's identity theft program shall include protections for financial and medical identity theft.
Level 3 Control Standard Mapping:	• 16 CFR Part §681.1 (d)(1) • 16 CFR Part §681.1 (d)(2) • 16 CFR Part §681.1 (f) • 16 CFR Part §681 Appendix A I • 1 TAC § 390.2(a)(3)

Federal Requirements

Federal Agencies and Contractors:	The organization: i. documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and ii. conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The organization conducts a Privacy Impact Assessment (PIA) on the Exchange information system in accordance with OMB policy M-03-22.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 03.b Performing Risk Assessments

Control Specification:	Risk Assessments shall be performed to identify and quantify risks. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	Risk assessments shall be performed that address all the major domains of the HITRUST CSF. Risk assessments shall be consistent and identify information security risks to the organization. The organization shall account for risks from sources including prior incidents experienced, changes in the environment (e.g., new methods of attack, new sources of attack, new vulnerabilities), and any supervisory guidance (e.g., third party consultancy). They may be quantitative, semi- or quasi-quantitative, or qualitative but shall be consistent and comparable, so the prioritization of resources to manage risk can be performed. Risk assessments are to be performed at planned intervals, or when major changes occur in the environment, and the results reviewed annually. Risk assessments (analysis) used to determine whether a breach of unsecured protected health information (PHI)—as these terms are defined by the Secretary of Health and Human Services—is reportable to the Secretary must demonstrate there is a low probability of compromise (lo pro co) rather than a significant risk of harm. The methodology shall, at a minimum, address the following factors: i. the nature of the PHI involved, including the types of identifiers involved and the likelihood of re-identification; ii. the unauthorized person who used the PHI or to whom the disclosure was made; iii. whether the PHI was actually acquired or viewed; iv. the extent to which the risk to the PHI has been mitigated; and v. and other factors/guidance promulgated by the Secretary.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Control Standard Mapping:	• 16 CFR Part §681 Appendix A II(b) • CSA DG-08 • HIPAA § 164.308(a)(1)(ii)(A) • HIPAA § 164.308(a)(1)(ii)(B) • HIPAA § 164.308(a)(2) • HIPAA § 164.308(a)(7)(ii)(E) • HIPAA § 164.316(a) • HIPAA § 164.402 • ISO/IEC 27002-2005 4.1 • ISO/IEC 27002-2005 6.2.1 • ISO/IEC 27002-2005 12.6.1 • ISO/IEC 27002-2005 14.1.2 • ISO/IEC 27002-2013 A.12.6.1 • ISO/IEC 27002-2013 A.17.1.1 • NIST Cybersecurity Framework ID.RA-1 • NIST Cybersecurity Framework ID.RA-3 • NRS 603A.215.1 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.03(2)(b) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to FTC Red Flags Rule Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall update the results of a comprehensive risk assessment every two (2) years, or whenever there is a significant change to the information system or operational environment, assesses a subset of the security controls within every 365 days during continuous monitoring, and reviews the risk assessment results annually.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization shall employ assessors or assessment teams with an organization-defined level of independence to conduct security control assessments and ensure impartiality of the results. A formal, documented process shall be in place for identifying risks and performing risk assessments, and communicating the results of the risk assessments to the affected parties, and to management. A repository and tracking system shall be in place to manage risk assessments performed. The likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits shall be included in the risk assessment process. The likelihood and impact associated with inherent and residual risk should be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance). Information security risk assessments shall require knowledge of the following: i. external environment factors that could exacerbate or moderate any or all of the levels of the risk components described previously; ii. the types of accounts offered by the organization; iii. the methods the organization provides to open and access its accounts; iv. knowledge and experiences of incident histories and actual case impact scenarios; and v. systems architectures.
Level 2 Control Standard Mapping:	• 16 CFR Part §681.1 (c) • 16 CFR Part §681 Appendix A II(a) • CMSRs 2013v2 CA-2 (HIGH) • CMSRs 2013v2 CA-2(1) (HIGH) • CMSRs 2013v2 RA-3 (HIGH) • CSA RI-02 • IRS Pub 1075 v2014 9.3.4.2 • IRS Pub 1075 v2014 9.3.14.2 • IRS Pub 1075 v2014 9.4.1 • IRS Pub 1075 v2014 9.4.2 (E.10) • MARS-E v1 CA-2 • MARS-E v1 CA-2(1) • MARS-E v1 RA-3 • NIST Cybersecurity Framework ID.RA-4 • NIST Cybersecurity Framework ID.RA-5 • NIST Cybersecurity Framework ID.AE-4 • NIST SP 800-53 R4 CA-2 • NIST SP 800-53 R4 CA-2(1) • NIST SP 800-53 R4 RA-3 • PCI DSS v3 12.2 • 1 TAC § 390.2(a)(3)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization shall document the risk assessment results in the applicable security plan. The organization shall assess the security controls in the information system within every three hundred sixty-five (365) days to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The annual security risk assessment requirement as mandated by OMB requires all controls attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the CMSRs shall be tested each year so that all security controls are tested during a 3-year period. The Business Owner notifies the CMS CISO within thirty (30) days whenever updates are made to system security authorization artifacts or significant role changes occur (e.g., Business Owner, System Developer/Maintainer, ISSO). The organization disseminates risk assessment results to affected stakeholders, Business Owners(s), and the CMS CISO. The organization shall employ assessors or assessment teams with a CMS CISO-defined level of independence to conduct security control assessments and ensure impartiality of the results.

FTI Requirements

FTI Custodians:	The agency shall conduct, periodically, but at least annually, an assessment

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	of the security controls in the systems that receive, store, process or transmit FTI, including cloud environments immediately prior to implementation of the cloud environment and each annual risk assessment (or update to an existing risk assessment) thereafter. The agency shall ensure each aspect of a data warehouse is assessed for risk, including hardware, software, data transport, and data storage. Any risk documents shall identify and document all vulnerabilities, associated with a data warehousing environment.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The organization shall assess the security controls in the information system within every three-hundred-sixty-five (365) days in accordance with the Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. A security assessment of all security controls must be conducted prior to issuing the initial authority to operate for all newly implemented systems. The annual security assessment requirement mandated by CMS requires all Minimum Security Controls for States attributable to a system or application to be assessed over a 3-year period. To meet this requirement, a subset of the Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement shall be tested each year so that all security controls are tested during a 3-year period. The Business Owner notifies the CISO within thirty (30) days whenever updates are made to system security authorization artifacts or significant role changes occur (e.g., Business Owner, System Developer/Maintainer, ISSO). The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the Exchange information system.

PCI-DSS Requirements

PCI Data:	Formal risk assessments shall be performed at least annually and upon significant changes to the environment. The assessments shall identify critical assets, threats and vulnerabilities.

Control Reference: 03.c Risk Mitigation

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Specification:	Risks shall be mitigated to an acceptable level. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Documentation and Records IT Organization and Management Roles and Responsibilities Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance; Requirements (High)Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	Risks can be dealt with in one of four ways: i. Avoidance - This approach eliminates the risk by avoidance of the activity which provides the risk. For example, the risk associated with utilization of wireless technologies can be mitigated by deciding not to use wireless technologies at all. ii. Reduction - Risk can be reduced by way of controls that can reduce the likelihood or impact of a risk. An example would be encryption of network traffic to minimize risks that threaten the confidentiality of data. iii. Transference - Risk can be reduced by shifting it to an outside entity. An example would be the purchase of insurance against fire damage. iv. Acceptance - Organizations can choose to accept risk by not selecting any of the aforementioned approaches. When acceptance is selected, management acceptance must be documented. Organizations shall define and document the criteria to determine whether or not a risk shall be avoided, accepted, transferred or treated. The factors to be taken into account shall include the following: i. industry sector, industry or organizational laws, regulations and standards; ii. clinical or other priorities (in the case of health related organizations); iii. cultural fit; iv. patient reactions (in the case of health related organizations); v. coherence with IT, corporate risk acceptance, and clinical strategy (in

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	the case of health organizations); vi. cost; vii. effectiveness; viii. type of protection; ix. number of threats covered; x. risk level at which the controls become justified; xi. risk level that led to the recommendation being made; xii. alternatives already in place; and xiii. additional benefits derived. The organization implements a process for ensuring that corrective action plans for the security program and the associated organizational information systems are prioritized and maintained; and the remedial information security actions necessary to mitigate risk to organizational operations and assets, individuals, and other organizations are documented. The organization shall review corrective action plans (plans of action and milestones) for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. The organization shall update existing remediation or corrective action plans monthly based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. The covered entity mitigates any harmful effect that is known to the covered entity of a use or disclosure of PHI by the covered entity or its business associates, in violation of its policies and procedures.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 CA-5 (HIGH) • CMSRs 2013v2 CA-5(1) (HIGH) • CMSRs 2013v2 PM-4 (HIGH) • CSA RI-03 • HIPAA § 164.306(e) • HIPAA § 164.308(a)(1)(ii)(B) • HIPAA § 164.530(f) • IRS Pub 1075 v2014 9.3.4.4 • ISO/IEC 27002-2005 4.2 • ISO/IEC 27002-2005 6.2.1 • MARS-E v1 CA-5 • MARS-E v1 CA-5(1) • MARS-E v1 PL-5 • MARS-E v1 PM-4 • NIST Cybersecurity Framework ID.RA-6 • NIST Cybersecurity Framework PR.IP-7 • NIST Cybersecurity Framework PR.IP-12 • NIST Cybersecurity Framework RS.MI-3 • NIST SP 800-53 R4 CA-5 • NIST SP 800-53 R4 PM-4

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: The organization shall develop a formal mitigation plan that shall include: i. perform a cost/benefit analysis for identified countermeasures; ii. document a risk treatment plan which provides recommended countermeasures to management; iii. document and present risk treatment summary reports to management; iv. management shall approve countermeasures documented in the risk treatment plan; v. map decisions taken against the list of HITRUST CSF controls; vi. plans for implementations (current and future) shall be documented in the organization's security improvement plan; and vii. implement the management approved risk treatment plan.
Level 2 Control Standard Mapping:	• ISO/IEC 27002-2005 12.6.1 • ISO/IEC 27002-2005 14.1.2 • ISO/IEC 27002-2005 15.3.1 • ISO/IEC 27002-2013 A.12.6.1 • ISO/IEC 27002-2013 A.12.7.1 • ISO/IEC 27002-2013 A.17.1.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization shall employ automated mechanisms to help ensure that the POA&M for the information system is accurate, up to date, and readily available. The organization shall: i. develop and submit a Plan of Action and Milestones (POA&M) for the information system within thirty (30) days of the final results for every internal/external audit/review or test (e.g., ST&E, penetration test) to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and ii. update and submit existing POA&M monthly until all the findings are resolved based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

FTI Requirements

FTI Custodians:	The agency must submit an updated Corrective Action Plan (CAP) twice each year to address corrective actions identified during an on-site safeguards review until all findings are closed. The CAP is submitted as an attachment to the SAR, and on the CAP due date which is six months from the scheduled SAR due date.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The organization shall employ automated mechanisms to help ensure that the POA&M for the information system is accurate, up to date, and readily available.

Control Reference: 03.d Risk Evaluation

Control Specification:	Risks shall be continually evaluated and assessed.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factor Type:	Organizational
Topics:	IT Organization and Management Roles and Responsibilities Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The risk management program shall include the requirement that risk assessments be re-evaluated at least annually, or when there are significant changes in the environment.

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FTC Red Flags Rule Compliance, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The risk management process shall be integrated with the change management process within the organization, and risk assessments shall be conducted whenever there is a significant change in the environment, or a change that could have a significant impact. Results of the risk assessments shall be included in the change management process, so they may guide the decisions within the change management process (e.g., approvals for changes). The organization shall update the risk assessment: i. before issuing a new formal authorization to operate or

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	ii. within every three (3) years, whichever comes first, or iii. whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or iv. other conditions that may impact the security or authorization state of the system. The privacy, security and risk management program(s) shall be updated to reflect changes in risks based on: i. any experiences with security incidents, weaknesses, breaches or identity theft; ii. changes in the environment (e.g., new methods of attack, new sources of attack, new vulnerabilities); iii. changes in prevention, detection or response methods for security; iv. changes within the organization including: a. organizational mergers, acquisitions, alliances, joint ventures or service provider arrangements; b. new systems or facilities; c. new service offerings; and d. new types of accounts.
Level 2 Control Standard Mapping:	• 16 CFR Part §681 Appendix A V(a) • 16 CFR Part §681 Appendix A V(b) • 16 CFR Part §681 Appendix A V(c) • 16 CFR Part §681 Appendix A V(d) • 16 CFR Part §681 Appendix A V(e) • CSA RI-04 • CMSRs 2013v2 RA-3 (HIGH) • IRS Pub 1075 v2014 9.3.14.2 • MARS-E v1 RA-3 • NIST Cybersecurity Framework ID.GV-4 • NIST Cybersecurity Framework ID.RA-1 • NIST Cybersecurity Framework ID.RA-3 • NIST Cybersecurity Framework ID.RA-4 • NIST Cybersecurity Framework ID.RA-5 • NIST SP 800-53 R4 RA-3 • 1 TAC § 390.2(a)(3)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 3 Implementation:	No additional requirements

Control Category: 04.0 - Security Policy

Objective Name: 04.01 Information Security Policy

Control Objective:	To provide management direction in line with business objectives and relevant laws and regulations, demonstrate support for, and commitment to information security through the issue and maintenance of an information security policies across the organization.

Control Reference: 04.a Information Security Policy Document

Control Specification:	Information Security Policy documents shall be approved by management, and published and communicated to all employees and relevant external parties. Information Security Policy documents shall establish the direction of the organization and align to best practices, regulatory, federal/state and international laws where applicable. The Information Security policy documents shall be supported by a strategic plan and a security program with well-defined roles and responsibilities for leadership and officer roles. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Awareness and Training Contingency Planning Documentation and Records IT Organization and Management Roles and Responsibilities Policies and Procedures Requirements (Legal and Contractual) Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to Joint Commission Accreditation, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	Information security policy documents shall be developed, published, disseminated and implemented. The information security policy documents shall state the purpose and scope of the policy, communicate management's commitment, describe management and workforce member's roles and responsibilities, and establish the organization's approach to managing information security. As applicable to the focus of a particular document, policies shall contain: i. a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing; ii. a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives; iii. a framework for setting control objectives and controls, including the structure of risk assessment and risk management; iv. the need for information security; v. the goals of information security; vi. compliance scope; vii. legislative, regulatory, and contractual requirements, including those for the protection of covered information and the legal and ethical responsibilities to protect this information; viii. arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentially, without fear of blame or recrimination. ix. a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization , including but not limited to CSF control objectives such as: a. compliance with legislative, regulatory, and contractual requirements; b. security education, training, and awareness requirements; c. business continuity management; d. consequences of information security policy violations; and e. coordination among organizational entities; x. a definition of general and specific responsibilities for information security management, including reporting information security incidents; xi. prescribes the development, dissemination, and review/update of formal, documented procedures to facilitate the implementation of security policy and associated security controls; and xii. references to documentation which may support the policy (e.g., more detailed security policies and procedures for specific information systems or security rules users shall comply with).

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	This information security policy documents shall be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader. In the instance of any acquisitions, re-organizations or mergers, or where the organization obtains support from third party organizations or collaborates with third parties, and especially if these activities involve other jurisdictions, the policy framework shall include documented policy, controls and procedures that cover such interactions and that specify the responsibilities of all parties.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-1 (HIGH) • CMSRs 2013v2 AT-1 (HIGH) • CMSRs 2013v2 AU-1 (HIGH) • CMSRs 2013v2 CA-1 (HIGH) • CMSRs 2013v2 CM-1 (HIGH) • CMSRs 2013v2 CP-1 (HIGH) • CMSRs 2013v2 IA-1 (HIGH) • CMSRs 2013v2 IR-1 (HIGH) • CMSRs 2013v2 MA-1 (HIGH) • CMSRs 2013v2 MP-1 (HIGH) • CMSRs 2013v2 PE-1 (HIGH) • CMSRs 2013v2 PL-1 (HIGH) • CMSRs 2013v2 PM-1 (HIGH) • CMSRs 2013v2 PS-1 (HIGH) • CMSRs 2013v2 RA-1 (HIGH) • CMSRs 2013v2 SA-1 (HIGH) • CMSRs 2013v2 SC-1 (HIGH) • CMSRs 2013v2 SI-1 (HIGH) • COBIT 4.1 DS5.2 • COBIT 5 APO13.02 • CSA IS-03 • HIPAA § 164.312(c)(1) • HIPAA § 164.316(b)(2)(i) • HIPAA § 164.316(b)(2)(ii) • HIPAA § 164.530(i) • HIPAA § 164.414(a) • IRS Pub 1075 v2014 9.3.1.1 • IRS Pub 1075 v2014 9.3.2.1 • IRS Pub 1075 v2014 9.3.3.1 • IRS Pub 1075 v2014 9.3.4.1 • IRS Pub 1075 v2014 9.3.5.1 • IRS Pub 1075 v2014 9.3.6.1 • IRS Pub 1075 v2014 9.3.7.1 • IRS Pub 1075 v2014 9.3.8.1 • IRS Pub 1075 v2014 9.3.9.1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• IRS Pub 1075 v2014 9.3.10.1 • IRS Pub 1075 v2014 9.3.11.1 • IRS Pub 1075 v2014 9.3.12.1 • IRS Pub 1075 v2014 9.3.13.1 • IRS Pub 1075 v2014 9.3.14.1 • IRS Pub 1075 v2014 9.3.15.1 • IRS Pub 1075 v2014 9.3.16.1 • IRS Pub 1075 v2014 9.3.17.1 • IRS Pub 1075 v2014 9.4.2 (E.10) • ISO/IEC 27002-2005 5.1.1 • ISO/IEC 27002-2013 A.5.1.1 • ISO 27799-2008 7.2.1 • JCAHO IM.02.01.03, EP 1 • MARS-E v1 AC-1 • MARS-E v1 AT-1 • MARS-E v1 AU-1 • MARS-E v1 CA-1 • MARS-E v1 CM-1 • MARS-E v1 CP-1 • MARS-E v1 IA-1 • MARS-E v1 IR-1 • MARS-E v1 MA-1 • MARS-E v1 PE-1 • MARS-E v1 PL-1 • MARS-E v1 PM-1 • MARS-E v1 PS-1 • MARS-E v1 RA-1 • MARS-E v1 SA-1 • MARS-E v1 SC-1 • MARS-E v1 SI-1 • NIST Cybersecurity Framework ID.GV-1 • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework ID.GV-4 • NIST SP 800-53 R4 AC-1 • NIST SP 800-53 R4 AT-1 • NIST SP 800-53 R4 AU-1 • NIST SP 800-53 R4 CA-1 • NIST SP 800-53 R4 CM-1 • NIST SP 800-53 R4 CP-1 • NIST SP 800-53 R4 IA-1 • NIST SP 800-53 R4 IR-1 • NIST SP 800-53 R4 MA-1 • NIST SP 800-53 R4 PE-1 • NIST SP 800-53 R4 PL-1 • NIST SP 800-53 R4 PM-1 • NIST SP 800-53 R4 PS-1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST SP 800-53 R4 RA-1 • NIST SP 800-53 R4 SA-1 • NIST SP 800-53 R4 SC-1 • NIST SP 800-53 R4 SI-1 • NRS 603A.215.1 • PCI DSS v3 1.5 • PCI DSS v3 2.5 • PCI DSS v3 3.7 • PCI DSS v3 4.3 • PCI DSS v3 5.4 • PCI DSS v3 6.7 • PCI DSS v3 7.3 • PCI DSS v3 8.8 • PCI DSS v3 9.10 • PCI DSS v3 10.8 • PCI DSS v3 11.6 • PCI DSS v3 12.1 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(4)(A)(xi)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Regulatory Factors:	
Level 3 Implementation:	No additional requirements

FTI Requirements

FTI Custodians:	The organization shall develop and disseminate a formal, documented, system and services acquisition policy that includes IRS documents received and identified by: i. taxpayer name ii. tax year(s) iii. type of information (e.g., revenue agent reports, Form 1040, work papers) iv. the reason for the request v. date requested vi. date received vii. exact location of the FTI viii. who has had access to the data, and ix. if disposed of, the date and method of disposition. The organization shall describe the purpose or function of a data warehouse in organizational policy.

PCI-DSS Requirements

PCI Data:	The organization shall ensure policies are documented, communicated (known to all parties) and in use for the following: i. managing firewalls, ii. managing vendor defaults and other security parameters, iii. protecting stored cardholder data, iv. encrypting transmissions of cardholder data, v. protecting systems against malware, vi. developing and maintaining secure systems and applications, vii. restricting access to cardholder data, viii. identification and authentication, ix. restricting physical access to cardholder data, x. monitoring access to network resources and cardholder data, and xi. security monitoring and testing.

Control Reference: 04.b Review of the Information Security Policy

Control Specification:	The information security policy documents shall be reviewed at planned intervals or if significant changes occur to ensure its continuing adequacy and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	effectiveness. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Audit and Accountability Documentation and Records IT Organization and Management Roles and Responsibilities Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance
Level 1 Implementation:	The information security policy documents shall be reviewed at planned intervals or if significant changes occur to ensure the policies' continuing adequacy and effectiveness. Additional factors when developing or changing a security policy document shall include, but are not limited to, regulatory mandates, accreditation requirements, and industry best practices, e.g., for system and services development and acquisition. A process shall be defined and implemented for individuals to make complaints concerning the information security policies and procedures or the organization's compliance with the policies and procedures. All complaints and requests for changes shall be documented, and their disposition, if any.
Level 1 Control Standard Mapping:	• CSA IS-05 • HIPAA § 164.316(a) • HIPAA § 164.530(i) • HIPAA § 164.414(a) • ISO/IEC 27002-2005 5.1.2 • ISO/IEC 27002-2013 A.5.1.2 • NIST Cybersecurity Framework ID.GV-1 • NIST Cybersecurity Framework ID.GV-3 • NIST SP 800-53 R4 AC-1 • NIST SP 800-53 R4 AT-1 • NIST SP 800-53 R4 AU-1 • NIST SP 800-53 R4 CA-1 • NIST SP 800-53 R4 CM-1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST SP 800-53 R4 CP-1 • NIST SP 800-53 R4 IA-1 • NIST SP 800-53 R4 IR-1 • NIST SP 800-53 R4 MA-1 • NIST SP 800-53 R4 PE-1 • NIST SP 800-53 R4 PL-1 • NIST SP 800-53 R4 PM-1 • NIST SP 800-53 R4 PS-1 • NIST SP 800-53 R4 RA-1 • NIST SP 800-53 R4 SA-1 • NIST SP 800-53 R4 SC-1 • NIST SP 800-53 R4 SI-1 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(4)(A)(xi)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The information security policy documents shall be reviewed at planned intervals, at a minimum every three hundred sixty-five (365) days, or if significant changes occur in the operating or business environment to ensure its continuing adequacy and effectiveness and that the totality of the policy has been addressed at least every three hundred sixty-five (365) days. The information security policy documents shall have an owner who has approved management responsibility for the development, review, and evaluation of the security policy. The review shall include assessing opportunities for improvement of the organization's information security policy documents and approach to managing information security in response to changes to the organizational environment, business circumstances, legal

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	conditions, or technical environment. The input to the management review shall include information on: i. feedback from interested parties; ii. results of independent reviews (see 5.h); iii. status of preventive and corrective actions (see 5.h and 6.g); iv. results of previous management reviews; v. process performance and information security policy compliance; vi. changes that could affect the organization's approach to managing information security, including changes to the organizational environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment; vii. trends related to threats and vulnerabilities; viii. reported information security incidents (see 11.a); and ix. recommendations provided by relevant authorities (see 5.f). The output from the management review shall include any decisions and actions related to: i. improvement of the organization's approach to managing information security and its processes; ii. improvement of control objectives and controls; and iii. improvement in the allocation of resources and/or responsibilities. A record of the management review shall be maintained. Management approval for the revised policy documents shall be obtained.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-1 (HIGH) • CMSRs 2013v2 AT-1 (HIGH) • CMSRs 2013v2 AU-1 (HIGH) • CMSRs 2013v2 CA-1 (HIGH) • CMSRs 2013v2 CM-1 (HIGH) • CMSRs 2013v2 CP-1 (HIGH) • CMSRs 2013v2 IA-1 (HIGH) • CMSRs 2013v2 IR-1 (HIGH) • CMSRs 2013v2 MA-1 (HIGH) • CMSRs 2013v2 MP-1 (HIGH) • CMSRs 2013v2 PE-1 (HIGH) • CMSRs 2013v2 PL-1 (HIGH) • CMSRs 2013v2 PM-1 (HIGH) • CMSRs 2013v2 PS-1 (HIGH) • CMSRs 2013v2 RA-1 (HIGH) • CMSRs 2013v2 SA-1 (HIGH) • CMSRs 2013v2 SC-1 (HIGH) • CMSRs 2013v2 SI-1 (HIGH) • IRS Pub 1075 v2014 9.3.1.1 • IRS Pub 1075 v2014 9.3.2.1 • IRS Pub 1075 v2014 9.3.3.1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• IRS Pub 1075 v2014 9.3.4.1 • IRS Pub 1075 v2014 9.3.5.1 • IRS Pub 1075 v2014 9.3.6.1 • IRS Pub 1075 v2014 9.3.7.1 • IRS Pub 1075 v2014 9.3.8.1 • IRS Pub 1075 v2014 9.3.9.1 • IRS Pub 1075 v2014 9.3.10.1 • IRS Pub 1075 v2014 9.3.11.1 • IRS Pub 1075 v2014 9.3.12.1 • IRS Pub 1075 v2014 9.3.13.1 • IRS Pub 1075 v2014 9.3.14.1 • IRS Pub 1075 v2014 9.3.15.1 • IRS Pub 1075 v2014 9.3.16.1 • IRS Pub 1075 v2014 9.3.17.1 • MARS-E v1 AC-1 • MARS-E v1 AT-1 • MARS-E v1 AU-1 • MARS-E v1 CA-1 • MARS-E v1 CM-1 • MARS-E v1 CP-1 • MARS-E v1 IA-1 • MARS-E v1 IR-1 • MARS-E v1 MA-1 • MARS-E v1 PE-1 • MARS-E v1 PL-1 • MARS-E v1 PM-1 • MARS-E v1 PS-1 • MARS-E v1 RA-1 • MARS-E v1 SA-1 • MARS-E v1 SC-1 • MARS-E v1 SI-1 • NRS 603A.215.1 • PCI DSS v3 12.1.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Regulatory Factors:	None
Level 3 Implementation:	Level 2 plus: The review shall address the following: i. the changing nature of the organization's operations and thus risk profile and risk management needs; ii. the changes made to the IT infrastructure of the organization, with the changes these bring to the organization's risk profile; iii. the changes identified in the external environment that similarly impact the organizations risk profile; iv. the latest controls, compliance and assurance requirements and arrangements of national bodies and of new legislation or regulation; v. the latest guidance and recommendations from professional associations and from information privacy commissioners regarding the protection of covered information; vi. the results of legal cases tested in courts, that thereby establish or cancel precedents and established practices; and vii. the challenges and issues regarding the policy, as expressed to the organization by its staff, customers, and their partners and care givers, researchers, and governments, e.g., privacy commissioners.
Level 3 Control Standard Mapping:	• ISO 27799-2008 7.2.2

FTI Requirements

FTI Custodians:	The organization shall periodically review/update a formal, documented, system and services acquisition policy that includes IRS documents received and identified by: i. taxpayer name ii. tax year(s) iii. type of information (e.g., revenue agent reports, Form 1040, work papers) iv. the reason for the request v. date requested vi. date received vii. exact location of the FTI viii. who has had access to the data, and ix. if disposed of, the date and method of disposition.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Category: 05.0 - Organization of Information Security

Objective Name: 05.01 Internal Organization

Control Objective:	To maintain the security of the organization's information and information assets (data centers or offices that process covered information).

Control Reference: 05.a Management Commitment to Information Security

Control Specification:	Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Audit and Accountability Awareness and Training IT Organization and Management Roles and Responsibilities Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to State of Massachusetts Data Protection Act, Subject to Joint Commission Accreditation, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	The organization's senior management shall: i. appoint a senior-level information security official; ii. ensure that the organization's information security processes are in place, are communicated to all stakeholders, and consider and address organizational requirements; iii. formally assign an organization single point of contact or group to evaluate and accept information security risk on behalf of the organization (e.g., CEO, COO, Security Steering Committee, etc.); iv. formulate, review, and approve information security policies and a

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	policy exception process; v. periodically, at a minimum, annually, review and assess the effectiveness of the implementation of the information security policy; vi. provide clear direction and visible management support for security initiatives; vii. provide the resources needed for information security; viii. initiate plans and programs to maintain information security awareness; ix. ensure that all appropriate measures are taken to avoid cases of identity theft targeted at patients, employees and third parties; x. ensure that the implementation of information security controls is coordinated across the organization; and xi. determine and coordinate, as needed, internal or external information security specialists, and review and coordinate results of the specialists' advice throughout the organization. The organization shall: i. ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; ii. employ a business case/Exhibit 300/Exhibit 53 to record the resources required; and iii. ensure that information security resources are available for expenditure as planned.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PM-2 (HIGH) • CMSRs 2013v2 PM-3 (HIGH) • COBIT 4.1 DS5.1 • COBIT 5 APO13.01 • COBIT 5 APO13.02 • CSA IS-02 • HIPAA § 164.316(a) • IRS Pub 1075 v2014 9.3.13.1 • IRS Pub 1075 v2014 9.3.18.1 • JCAHO IM.02.01.03, EP 5 • MARS-E v1 PM-2 • MARS-E v1 PM-3 • NIST SP 800-53 R4 PM-2 • NIST SP 800-53 R4 PM-3 • NRS 603A.215.1 • PCI DSS v3 12.5 • PCI DSS v3 12.5.1 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.03(2)(a) • 1 TAC § 390.2(a)(1)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FTC Red Flags Rule Compliance,
Level 2 Implementation:	Level 1 plus: i. ensure that organization's information security strategy and goals are identified and considered, and address organizational and healthcare-specific requirements, and verify that appropriate processes are in place to meet the organization's strategy and goals; ii. formally review and approve in writing the establishment and administration of any information privacy, security and risk management programs; iii. formally approve in writing the assignment of specific roles and responsibilities for information security across the organization; iv. formally appoint an employee or group as the point of contact for oversight, development, implementation and administration of security matters., and the appointed lead shall demonstrate professional competency in security matters via a recognized security industry certification, appropriate vendor certifications or a minimum of five years of security related experience; v. document its risk acceptance process; and vi. conduct an annual review (may be performed by a third party) of the effectiveness of its security program. The organization shall formally appoint in writing non-professional or professional security contacts by name in each major organizational area or business unit.
Level 2 Control Standard Mapping:	• 16 CFR Part §681.1 (e)(1) • 16 CFR Part §681.1 (e)(2) • ISO/IEC 27002-2005 6.1.1 • NIST Cybersecurity Framework ID.BE-2 • NIST Cybersecurity Framework ID.BE-3 • 1 TAC § 390.2(a)(3)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	Level 2 plus: i. the organization formally creates a dedicated security management forum and publishes the forum's member list and charter. Such responsibilities can be handled by a Security Advisory Board, Security Steering Committee or by an existing management body, such as the board of directors; ii. the organization conducts an annual assessment of the effectiveness of its security program performed by a qualified outside organization; iii. the organization shall publish security guidelines and/or daily operational procedures relating to processes that complement, clarify and enforce security policies.
Level 3 Control Standard Mapping:	• ISO 27799-2008 7.3.2.1

Control Reference: 05.b Information Security Coordination

Control Specification:	Information security activities shall be coordinated by representatives from different parts of the organization with relevant roles and job functions. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Awareness and Training IT Organization and Management Roles and Responsibilities Personnel Third Parties and Contractors

Level 1 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to Joint Commission Accreditation
Level 1 Implementation:	The organization shall: i. determine information security requirements for the information system in mission/business process planning; ii. determine, document and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process; and iii. establish a discrete line item for information security in organizational programming and budgeting information. Information security coordination shall involve the active cooperation and collaboration across the entire organization. This activity shall: i. ensure that security activities across the entire organization are executed in compliance with the information security policy and that deviations are identified and reviewed; ii. identify how to handle non-compliance (such as sanctions or disciplinary action); iii. assess the adequacy and coordinate the implementation of information security controls; iv. effectively promote information security education, training and awareness throughout the organization. If the organization does not use a separate cross-functional group because such a group is not appropriate for the organization's size, the actions described above shall be undertaken by another suitable management body or individual security representative.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 SA-2 (HIGH) • COBIT 4.1 DS5.1 • COBIT 5 APO13.01 • COBIT 5 APO13.02 • HIPAA § 164.308(a)(1)(ii)(B) • HIPAA § 164.310(a)(2)(ii) • HIPAA § 164.316(a) • HIPAA § 164.316(b)(1) • HIPAA § 164.316(b)(2)(iii) • IRS Pub 1075 v2014 9.3.15.2 • JCAHO IM.02.01.03, EP 8 • MARS-E v1 SA-2

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST Cybersecurity Framework ID.GV-2 • NIST SP 800-53 R4 SA-2 • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(4)(A)(xi)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Information security coordination shall involve the active cooperation and collaboration across the entire organization to include managers, users, administrators, application designers, auditors and security personnel. Information security coordination shall also include specialist skills in areas such as insurance, legal issues, human resources, privacy, IT or risk management. This activity shall: i. address deviations via a risk acceptance process; ii. approve methodologies and processes for information security management activities (e.g., risk acceptance, information classification, security incidents); iii. identify and promptly report to senior management significant threat changes and exposure of information and information processing resources to threats; iv. evaluate information received from the monitoring and reviewing of information security incidents to conduct "lessons learned" activities, and recommend to senior management appropriate actions in response to identified information security incidents. v. create an internal security information sharing mechanism, such as an e-mail group, periodic conference call or standing meeting; vi. establish an internal reporting mechanism, such as a telephone hotline or dedicated e-mail address, to allow security contacts to report information security incidents or obtain security policy clarifications

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	on a timely basis. The organization develops a security plan for the information system that: i. is consistent with the organization's enterprise architecture; ii. explicitly defines the authorization boundary for the system; iii. describes the operational context of the information system in terms of missions and business processes; iv. provides the security categorization of the information system including supporting rationale; v. describes the operational environment for the information system; vi. describes relationships with or connections to other information systems; vii. provides an overview of the security requirements for the system; viii. identifies any relevant overlays, if applicable; ix. describes the security controls in place or planned for meeting those requirements including a rationale for tailoring and supplementation decisions; and x. is reviewed and approved by the authorizing official or designated representative prior to plan implementation. The organization shall update the system security plan: i. at least every three (3) years; ii. when substantial changes are made to the system; iii. when changes in requirements result in the need to process data of a higher sensitivity; iv. after the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and v. prior to expiration of a previous security authorization. The organization shall plan and coordinate security-related activities affecting the information system before conducting such activities in order to reduce the impact on other organizational entities. The organization shall: i. distribute copies of the information system's security plan to appropriate individuals and offices (e.g., CCO, CIO, business units); ii. communicate any changes to the security plans to appropriate individuals and offices; and iii. protect the plan from unauthorized disclosure and modification.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 PL-2 (HIGH) • CMSRs 2013v2 PL-2(3) (HIGH) • IRS Pub 1075 v2014 7.4 • IRS Pub 1075 v2014 9.3.1 • IRS Pub 1075 v2014 9.3.12.2 • IRS Pub 1075 v2014 9.4.1 • IRS Pub 1075 v2014 9.4.14 • ISO/IEC 27002-2005 6.1.2

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• MARS-E v1 PL-2 • MARS-E v1 PL-6 • NIST Cybersecurity Framework DE.DP-4 • NIST SP 800-53 R4 PL-2 • NIST SP 800-53 R4 PL-2(3) • NRS 603A.215.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	Level 2 plus: The organization shall convene an internal meeting for the organization's security single point of contact and the organizational area/business unit security contacts (see 05.a) on a monthly or near to monthly basis.
Level 3 Control Standard Mapping:	• ISO 27799-2008 7.3.2.1

CMS Requirements

CMS Contractors:	The organization shall establish a discrete line item in CMS' programming and budgeting documentation for the implementation and management of information systems security. The organization shall develop a security plan for the information system that is consistent with the CMS System Security Plan (SSP) Procedure.

FTI Requirements

FTI Custodians:	The organization shall develop and submit to designated agency officials and the Office of Safeguards a Safeguard Procedures Report (SPR) that describes the procedures established and used by the organization for ensuring the

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	confidentiality of the information received from the IRS. Annually thereafter, the organization must file a Safeguard Activity Report (SAR). Whenever significant changes occur in the safeguard program the SPR will be updated and resubmitted to designated agency officials and the Office of Safeguards. It also advises the IRS of future actions that will affect the organization's current efforts to ensure the confidentiality of FTI, and certifies that the organization is protecting FTI pursuant to IRC Section 6103(p)(4) and the organization's own security requirements. Agencies must notify the IRS prior to executing any agreement to disclose FTI to a contractor (e.g., cloud computing providers, consolidated data centers, off-site storage facilities, shred companies, information technology support, or tax modeling or revenue forecasting providers), or at least 45 days prior to the disclosure of FTI, to ensure that appropriate contractual language is included and that contractors are held to safeguarding requirements. Further, any contractors authorized access to or possession of FTI must notify and secure the approval of the IRS prior to making any redisclosures to subcontractors. (See IRS Pub 1075 v2014 Exhibit 6.)

Control Reference: 05.c Allocation of Information Security Responsibilities

Control Specification:	All information security responsibilities shall be clearly defined.
Factor Type:	Organizational
Topics:	Authorization IT Organization and Management Roles and Responsibilities Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance
Level 1 Implementation:	The organization's senior-level information security official shall coordinate, develop, implement, and maintain an organization-wide information security program. The organization shall formally assign the following specific information

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	security responsibilities to an individual or team: i. establishment, documentation and distribution of security policies and procedures; ii. monitoring and analyzing security alerts and information, and distributing security alerts, information and analysis to appropriate personnel; iii. establishment, documentation and distribution of security incident response and escalation procedures to ensure timely and effective handling of all situations; iv. administering user accounts, including additions, deletions and modifications; and v. monitoring and controlling all access to data. Information security roles & responsibilities shall be coordinated and aligned with internal roles and external partners. The organization shall clearly assign responsibilities to identify all IT assets that need protection and apply controls to meet security policy. The allocation of information security responsibilities shall be done in accordance with the information security policy. Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly identified. This responsibility shall be supplemented, where necessary, with more detailed guidance for specific assets and facilities. Individuals with allocated security responsibilities may delegate security tasks to others. Nevertheless they remain accountable and shall determine that any delegated tasks have been correctly performed.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PM-2 (HIGH) • COBIT 4.1 DS5.1 • COBIT 5 APO13.01 • COBIT 5 APO13.02 • CSA IS-13 • HIPAA § 164.308(a)(2) • IRS Pub 1075 v2014 9.3.18.1 • ISO/IEC 27002-2005 6.1.3 • ISO/IEC 27002-2013 A.6.1.1 • ISO 27799-2008 7.3.2.1 • MARS-E v1 PM-2 • NIST Cybersecurity Framework ID.GV-2 • NIST SP 800-53 R4 PM-2 • NRS 603A.215.1 • PCI DSS v3 12.4 • PCI DSS v3 12.5 • PCI DSS v3 12.5.1 • PCI DSS v3 12.5.2 • PCI DSS v3 12.5.3

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• PCI DSS v3 12.5.4 • PCI DSS v3 12.5.5 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to FTC Red Flags Rule Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall identify by name or position non-professional or professional security contacts in each major organizational area or business unit. The organization shall clearly define the roles, responsibilities and authority of each security contact including the administration and implementation of the organization's security programs. Each security contact shall annually document compliance related to identified legal requirements (see CSF 06.a) and report to the organization's single point of contact for security. The reports shall include: i. evaluations on the effectiveness of the policies and procedures implemented in addressing risk; ii. evaluations of service provider arrangements (see CSF 09.e, 09.f, 09.g); iii. significant incidents and the response; and iv. recommendations for material changes to the security programs for which they are responsible. The organization's single point of contact for security matters shall provide supplemental security awareness and training. The contact for security shall be responsible for review reports related to the security organization, network, systems and programs implemented. Any material changes to these items shall be formally approved by the contact for security prior to implementation.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Local responsibilities for the protection of assets and for carrying out specific security processes, such as business continuity planning, shall be clearly defined. Additionally, the following shall take place: i. the assets and security processes associated with each particular system shall be identified and clearly defined; ii. the entity responsible (owner) for each asset or security process shall be assigned and the details of this responsibility shall be documented (see 07.b); iii. authorization levels shall be clearly defined and documented; and iv. to be able to fulfil responsibilities in the information security area, the appointed individuals should be competent in the area and be given opportunities to keep up to date with developments.
Level 2 Control Standard Mapping:	• 16 CFR Part §681 Appendix A VI (a) • 16 CFR Part §681 Appendix A VI (b) • 1 TAC § 390.2(a)(3)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	Level 2 plus: The organization shall specifically define the roles, responsibilities of each security contact in writing.
Level 3 Control Standard Mapping:	None

Control Reference: 05.d Authorization Process for Information Assets and Facilities

Control Specification:	A management authorization process for new information assets (e.g., systems and applications) (see Other Information), and facilities (e.g. data

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	centers or offices where covered information is to be processed) shall be defined and implemented.
Factor Type:	Organizational
Topics:	Authorization IT Organization and Management Roles and Responsibilities Media and Assets Physical and Facility Security Policies and Procedures Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The following shall be required for the authorization process: i. new information processing assets (internal to the organization or via a service provided by a third party) shall have appropriate user management authorization of their purpose and use, and authorization shall also be obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met; ii. information assets shall have appropriate security measures commensurate with the type of information it will store, process or transmit; iii. the assets shall comply with all applicable laws, regulations, standards policies and other applicable sections of the HITRUST Common Security Framework; iv. hardware and software shall be checked to ensure that they are compatible with other system components; and v. necessary controls for the use of personal or privately owned information processing equipment (e.g., laptops, home-computers or hand-held devices) for processing business information, which may introduce new vulnerabilities, shall be identified and implemented.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PM-10 (HIGH) • CSA RM-01 • HIPAA § 164.308(a)(2) • HIPAA § 164.308(a)(8) • ISO/IEC 27002-2005 6.1.4 • ISO 27799-2008 7.3.2.2

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• MARS-E v1 PM-10 • NIST Cybersecurity Framework ID.BE-1 • NIST SP 800-53 R4 PM-10 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: Management formally authorizes (approves) new information assets and facilities for processing (use) before commencing operations and periodically reviews and updates authorizations (approvals) at a frequency defined by the organization but no less than 3 years.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CA-6 (HIGH) • IRS Pub 1075 v2014 9.3.4.5 • MARS-E v1 CA-6 • NIST SP 800-53 R4 CA-6

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation:	Level 2 plus: All new facilities shall undergo a site security survey by the organization's security department or a trusted third party, and resolve all security shortcomings before any covered information is processed at that location. All sites that process covered information shall be reviewed on an annual basis to ensure their continued suitability to process covered information. This process shall also be invoked if the site undergoes a significant change in mission or makes substantive physical changes in its facilities or workforce.
Level 3 Control Standard Mapping:	None

CMS Requirements

CMS Contractors:	The organization: i. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and ii. Updates the security authorization: a. Within every three (3) years; b. When significant changes are made to the system; c. When changes in requirements result in the need to process data of a higher sensitivity; d. When changes occur to authorizing legislation or federal requirements; e. After the occurrence of a serious security violation which raises questions about the validity of an earlier security authorization; and f. Prior to expiration of a previous security authorization.

FTI Requirements

FTI Custodians:	Owners of FTI shall accredit the security controls used to protect FTI before initiating operations. This shall be done for any infrastructure associated with FTI. The authorization shall occur every three (3) years or whenever there is a significant change to the control structure. A senior agency official shall sign and approve the authorization.

Control Reference: 05.e Confidentiality Agreements

Control Specification:	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified and regularly reviewed.
Factor Type:	Organizational
Topics:	Documentation and Records

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Personnel Requirements (Legal and Contractual) Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Confidentiality or non-disclosure agreements shall address the requirement to protect confidential information using legally enforceable terms. Confidentiality or nondisclosure agreements shall include, but are not limited to, the following: i. a definition of the information to be protected (e.g., confidential information); ii. expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely; iii. required actions when an agreement is terminated; iv. responsibilities and actions of signatories to avoid unauthorized information disclosure (such as 'need to know'); v. disclosures required to be limited to the limited data set (see 07.d) or the minimum necessary to accomplish the intended purpose of such use, disclosure, or request; vi. ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information; vii. the permitted use of confidential information, and rights of the signatory to use information; viii. individuals' rights to obtain a copy of the individual's information in an electronic format; ix. individuals' rights to have the individual's information transmitted to another entity or person designated by the individual, provided the request is clear, conspicuous, and specific; x. the right to audit and monitor activities that involve confidential information; xi. the process for notification and reporting of unauthorized disclosure or confidential information breaches; xii. terms for information to be returned or destroyed at agreement cessation; and xiii. expected actions to be taken (i.e. penalties that are possible) in case of a breach of this agreement.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The confidentiality agreement shall be applicable to all personnel accessing covered information. Confidentiality and non-disclosure agreements shall comply with all applicable laws and regulations for the jurisdiction to which it applies (see 6.a). Requirements for confidentiality and non-disclosure agreements shall be reviewed at least annually and when changes occur that influence these requirements.
Level 1 Control Standard Mapping:	• CSA LG-01 • ISO/IEC 27002-2005 6.1.5 • ISO/IEC 27002-2013 A.13.2.4 • ISO 27799-2008 7.3.2.3 • NIST Cybersecurity Framework PR.DS-5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: The organization shall publish a list of representatives who are authorized to sign a non-disclosure agreement on behalf of the organization. This list shall be kept up to date to reflect personnel changes and departures.
Level 2 Control Standard Mapping:	None

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Regulatory Factors:	
Level 3 Implementation:	No additional requirements

Health Information Exchange Requirements

Health Information Exchanges:	As part of the agreement with the connecting organizations, the HIE shall specify which organization owns the data and any restrictions as part of that ownership such as retention, integrity, and accuracy of data. If the HIE is the owner of the data, all federal and state requirements associated with the patients' information shall be met.

Control Reference: 05.f Contact with Authorities

Control Specification:	Appropriate contacts with relevant authorities shall be maintained.
Factor Type:	Organizational
Topics:	Documentation and Records Incident Response Policies and Procedures Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The organization should define a plan with associated contact information for reporting security incidents to law enforcement if it is expected that laws may have been broken. The organization shall include key contacts including phone numbers and e-mail addresses as part of its incident management and/or business continuity plan. The organization shall designate a point of contact to review the list at least annually to keep it current. Organizations under attack from the Internet may need external third parties (e.g., an Internet service provider or telecommunications operator) to take action against the attack source. The appropriate contact information for these third parties shall be documented, and instances when they must be contacted

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	to take action shall be communicated.
Level 1 Control Standard Mapping:	• CSA CO-04 • NIST Cybersecurity Framework DE.DP-4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: Each group within the organization (e.g., information security) shall have procedures documented and implemented that specify when and by whom authorities (e.g., law enforcement, fire department, supervisory authorities) shall be contacted, and how identified information security incidents shall be reported in a timely manner if it is suspected that laws may have been broken. The organization shall include key contacts including phone numbers and e-mail addresses as part of its incident management and/or business continuity plan. The organization shall designate a point of contact to review the list at least quarterly to keep it current. The organization shall conduct an exercise at least annually and make contact with a majority (at least 80 percent) of the listed contacts. During this incident/continuity plan exercise the organization shall document that the contact person and information are current.
Level 2 Control Standard Mapping:	• ISO/IEC 27002-2005 6.1.6 • ISO/IEC 27002-2013 A.6.1.3 • ISO 27799-2008 7.3.2.4 • NIST Cybersecurity Framework RS.CO-2 • NIST Cybersecurity Framework RS.CO-3

Level 3 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 05.g Contact with Special Interest Groups

Control Specification:	Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.
Factor Type:	Organizational
Topics:	Incident Response Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Membership in organization-defined special interest groups or forums shall be considered as a means to: i. improve knowledge about best practices and staying up to date with relevant security information; ii. ensure the understanding of the information security environment is current and complete; iii. receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities; iv. gain access to specialist information security advice; v. share and exchange information about new technologies, products, threats, or vulnerabilities; vi. provide suitable liaison points when dealing with information security incidents (see 11.c).
Level 1 Control	• CSA CO-04

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Standard Mapping:	• CSA IS-12 • HIPAA § 164.308(a)(5)(ii)(A) • ISO/IEC 27002-2005 6.1.7 • ISO/IEC 27002-2013 A.6.1.4 • ISO 27799-2008 7.3.2.4 • NIST Cybersecurity Framework RS.CO-5 • NIST Cybersecurity Framework ID.RA-2 • NIST SP 800-53 R4 SI-5 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Membership in special interest groups or forums shall be required and actively maintained. The organization shall have a process to quickly identify newly discovered security vulnerabilities such as a credible subscription service. The organization shall have a process to map new vulnerabilities into its security policies, guidelines and daily operational procedures.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 PM-15 (HIGH) • CMSRs 2013v2 SI-5 (HIGH) • CMSRs 2013v2 SI-5(1) (HIGH) • IRS Pub 1075 v2014 9.3.17.5 • MARS-E v1 SI-5 • NIST SP 800-53 R4 PM-15 • NIST SP 800-53 R4 SI-5(1)

Level 3 Implementation Requirements

Level 3	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Organizational Factors:	
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization shall implement security directives in accordance with established time frames, or notifies CMS of the degree of noncompliance. The organization shall employ automated mechanisms to make security alert and advisory information available throughout the organization as needed.

Control Reference: 05.h Independent Review of Information Security

Control Specification:	The organization's approach to managing information security and its implementation (control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, at a minimum annually, or when significant changes to the security implementation occur.
Factor Type:	Organizational
Topics:	Audit and Accountability Documentation and Records IT Organization and Management Roles and Responsibilities

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance; Subject to CMS Minimum Security Requirements (High); Subject to MARS-E Requirements; Subject to FTI Compliance
Level 1 Implementation:	The independent review shall be initiated by management. Such an independent review is necessary to ensure the continuing suitability, adequacy, and effectiveness of the organization's approach to managing

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	information security and privacy. The review shall: i. include an assessment of opportunities for improvement; ii. address the need for changes to the approach to security, including the policy and control objectives. iii. be carried out by individuals independent of the area under review (e.g., the internal audit function, an independent manager or a third party organization specializing in such reviews); and iv. be carried out by individuals who have the appropriate skills and experience. The results of the independent review shall: i. be recorded and reported to the management who initiated the review; and ii. be maintained for a predetermined period of time as determined by the organization, but not less than three years. If the independent review identifies that the organization's approach and implementation to managing information security is inadequate or not compliant with the direction for information security stated in the information security policy document (see 4.a), management shall take corrective actions.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 CA-7 (HIGH) • CMSRs 2013v2 CA-7(1) (HIGH) • COBIT 4.1 DS5.5 • COBIT 5 DSS05.07 • CSA CO-02 • HIPAA § 164.308(a)(1)(ii)(D) • HIPAA § 164.308(a)(8) • IRS Pub 1075 v2014 9.3.4.6 • ISO/IEC 27002-2005 6.1.8 • ISO/IEC 27002-2013 A.18.2.1 • ISO 27799-2008 7.3.2.4 • MARS-E v1 CA-7 • MARS-E v1 CA-7(1) • NIST Cybersecurity Framework ID.GV-4 • NIST Cybersecurity Framework PR.IP-7 • NIST Cybersecurity Framework PR.IP-8 • NIST Cybersecurity Framework ID.RM-1 • NIST Cybersecurity Framework ID.RM-2 • NIST Cybersecurity Framework ID.RM-3 • NIST SP 800-53 R4 CA-7 • NIST SP 800-53 R4 CA-7(1) • NIST SP 800-53 R4 AR-4 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act
Level 2 Implementation:	Level 1 plus: The independent review of the information security management program and information security controls shall be conducted at least annually or whenever there is a material change to the business practices that may implicate the security or integrity of records containing personal information.
Level 2 Control Standard Mapping:	• (State of Mass.) 201 CMR 17.03(2)(a)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Objective Name: 05.02 External Parties

Control Objective:	To ensure that the security of the organization's information and information assets, are not reduced by the introduction of external party products or services.

Control Reference: 05.i Identification of Risks Related to External Parties

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Specification:	The risks to the organization's information and information assets from business processes involving external parties shall be identified, and appropriate controls implemented before granting access. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Authorization Communications and Transmissions Requirements (Legal and Contractual) Risk Management and Assessments Third Parties and Contractors User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FTC Red Flags Rule Compliance; Subject to FISMA Compliance; Subject to CMS Minimum Security Requirements (High); Subject to MARS-E Requirements; Subject to FTI Compliance
Level 1 Implementation:	Due diligence, including an evaluation of the information security risks posed by external parties, shall be carried out to identify any requirements for specific controls where access to sensitive information (e.g., covered information, cardholder data) by external parties is required prior to establishing a formal relationship with the service provider. The identification of risks related to external party access shall take into account the following issues: i. the information asset(s) an external party is required to access; ii. the type of access the external party will have to the information and information asset(s), such as: a. physical access (e.g., to offices, computer rooms, filing cabinets); b. logical access (e.g., to an organization's databases, information systems); c. network connectivity between the organization's and the external party's network(s) (e.g., permanent connection, remote access); d. whether the access is taking place on-site or off-site; iii. the value and sensitivity of the information involved, and its criticality for business operations;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	iv. the controls necessary to protect information that is not intended to be accessible by external parties; v. the external party personnel involved in handling the organization's information; vi. how the organization or personnel authorized to have access can be identified, the authorization verified, and how often this needs to be reconfirmed; vii. the different means and controls employed by the external party when storing, processing, communicating, sharing and exchanging information; viii. the impact of access not being available to the external party when required, and the external party entering or receiving inaccurate or misleading information; ix. practices and procedures to deal with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident; x. legal and regulatory requirements and other contractual obligations relevant to the external party that shall be taken into account; xi. how the interests of any other stakeholders may be affected by the arrangements. Access by external parties to the organization's information shall not be provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. All security requirements resulting from work with external parties or internal controls shall be reflected by the agreement with the external party (see 5.i and 5.j). All remote access connections between the organization and all external parties shall be secured via encrypted channels (e.g., VPN). Any covered information shared with an external party shall be encrypted prior to transmission. External parties shall be granted minimum necessary access to the organization's information assets to minimize risks to security. All access granted to external parties shall be limited in duration and revoked when no longer needed. It shall be ensured that the external party is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information assets.
Level 1 Control Standard Mapping:	• 16 CFR Part §681.1 (e)(4) • CSA RI-05 • HIPAA § 164.308(b)(1) • HIPAA § 164.308(b)(3) • HIPAA § 164.314(a)(2)(ii) • ISO/IEC 27002-2005 6.2.1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST Cybersecurity Framework ID.AM-3 • NIST Cybersecurity Framework DE.AE-1 • PCI DSS v3 12.8.3 • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(3)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: The organization shall conduct due diligence of the external party via interviews, document review, checklists, review certifications (e.g., HITRUST) or other remote means. The process for conducting external party due diligence shall be integrated with the execution of a non-disclosure agreement (NDA) (see 05.e).
Level 2 Control Standard Mapping:	• ISO 27799-2008 7.3.3.1 • NRS 603A.215.1 • PCI DSS v3 2.6

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 05.j Addressing Security When Dealing with Customers

Control Specification:	All identified security requirements shall be addressed before giving customers access to the organization's information or assets.
Factor Type:	Organizational
Topics:	Authentication Incident Response Requirements (Legal and Contractual) Third Parties and Contractors User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance; Subject to CMS Minimum Security Requirements (High); Subject to MARS-E Requirements; Subject to FTI Requirements
Level 1 Implementation:	The following security terms shall be addressed prior to giving customers access to any of the organization's assets: i. description of the product or service to be provided; ii. the right to monitor, and revoke, any activity related to the organization's assets; and iii. the respective liabilities of the organization and the customer. It shall be ensured that the customer is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information assets. The organization shall permit an individual to request to restrict the disclosure of the individual's covered information to a business associate for purposes of carrying out payment or health care operations, and is not for purposes of carrying out treatment. The organization shall respond to any requests from an individual on the disclosure of the individual's covered information, providing the individual with records (see 06.c) of disclosures of covered information that are made by the organization and either: i. records (see 06.c) of disclosures of covered information made by a business associate acting on behalf of the organization; or

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	ii. a list of all business associates acting on behalf of the covered entity, including contact information for such associates (such as mailing address, phone, and email address). The organization shall ensure that the public has access to information about its privacy activities and is able to communicate with its senior privacy official (e.g., Chief Privacy Officer , Chief Data Protection Officer).
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PL-4 (HIGH) • CSA SA-01 • IRS Pub 1075 v2014 9.3.12.3 • IRS Pub 1075 v2014 9.4.5 • IRS Pub 1075 v2014 9.4.13 • IRS Pub 1075 v2014 9.4.16 • MARS-E v1 PL-4 • NIST Cybersecurity Framework PR.AC-3 • NIST Cybersecurity Framework PR.AT-3 • NIST SP 800-53 R4 PL-4 • NIST SP 800-53 R4 TR-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: The following security terms shall be addressed prior to giving customers access to any of the organization's assets: i. asset protection, including: a. procedures to protect the organization's assets, including information and software, and management of known vulnerabilities; b. procedures to determine whether any compromise of the assets (e.g., loss or modification of data) has occurred; c. integrity; and d. restrictions on copying and disclosing information;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	ii. access control policy, covering: a. permitted access methods, and the control and use of unique identifiers such as user IDs and passwords; b. an authorization process for user access and privileges; c. a statement that all access that is not explicitly authorized is forbidden; d. a process for revoking access rights or interrupting the connection between systems; iii. arrangements for reporting, notification, and investigation of information inaccuracies (e.g., of personal details), information security incidents and security breaches; iv. a description of each service to be made available; v. the target level of service and unacceptable levels of service; vi. the different reasons, requirements, and benefits for customer access; vii. responsibilities with respect to legal matters and how it is ensured that the legal requirements are met (e.g., data protection legislation), especially taking into account different national legal systems if the agreement involves co-operation with customers in other countries (see 06.i); and viii. intellectual property rights (IPRs) and copyright assignment (see 06.b) and protection of any collaborative work (see 05.e). Access by customers to the organization's information shall not be provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. All security requirements resulting from work with external parties or internal controls shall be reflected by the agreement with the external party. For all system connections that allow customers to access the organization's computing assets such as Web Sites, kiosks and public access terminals, the organization shall provide appropriate text or a link to the organization's privacy policy for data use and protection as well as the customer's responsibilities when accessing the data. The organization shall have a formal mechanism to authenticate (see 01.b) the customer's identity prior to granting access to covered information.
Level 2 Control Standard Mapping:	• ISO/IEC 27002-2005 6.2.2 • ISO 27799-2008 7.3.3.2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

FTI Requirements

FTI Custodians:	To use (1) an Integrated Voice Response (IVR) system that provides FTI over the telephone to a customer or (2) a Web-based system or Website to access FTI, the agency must ensure access to FTI via the IVR system requires a strong identity verification process. The authentication must use a minimum of two pieces of information although more than two are recommended to verify the identity. One of the authentication elements must be a shared secret only known to the parties involved and issued by the agency directly to the customer (but not a case number or similar piece of information). The organization's access control system must be specifically configured to address the complicated nature of the environment to ensure only authorized clients who conform to agency security policy are permitted access to the Virtual Desktop Infrastructure (VDI).

Control Reference: 05.k Addressing Security in Third Party Agreements

Control Specification:	Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information assets, or adding products or services to information assets shall cover all relevant security requirements. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Authorization Awareness and Training Documentation and Records IT Organization and Management Roles and Responsibilities Policies and Procedures Requirements (Legal and Contractual) Third Parties and Contractors User Access

Level 1 Implementation Requirements

Level 1 Organizational	Applicable to all organizations

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to State of Massachusetts Data Protection Act, Subject to the State of Nevada Security of Personal Information Requirements
Level 1 Implementation:	The organization shall identify and mandate information security controls to specifically address supplier access to the organization's information and information assets. The organization shall maintain written agreements (contracts) that includes an acknowledgement that the third party (e.g., a service provider) is responsible for the security of the data the third party possesses or otherwise stores, processes or transmits on behalf of the organization, or to the extent that they could impact the security of the organization's information environment. Agreements shall include requirements to address the information security risks associated with information and communications technology services (e.g., cloud computing services) and product supply chain. The agreement shall ensure that there is no misunderstanding between the organization and the third party. Organizations shall satisfy themselves as to the indemnity of the third party. The following terms shall be implemented for inclusion in the agreement in order to satisfy the identified security requirements (see 05.i): i. the information security policy; ii. controls to ensure asset protection, including: a. procedures to protect organizational assets, including information, software and hardware; b. any required physical protection controls and mechanisms; c. controls to ensure protection against malicious software (see 9.j); d. procedures to determine whether any compromise of the assets (e.g., loss or modification of information, software and hardware) has occurred; e. controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during the agreement; f. confidentiality, integrity, availability, and any other relevant property of the assets; and g. restrictions on copying and disclosing information, and using confidentiality agreements (see 05.b); iii. user and administrator training in methods, procedures, and security; iv. ensuring user awareness for information security responsibilities and issues; v. provision for the transfer of personnel, where appropriate; vi. responsibilities regarding hardware and software installation and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	maintenance; vii. a clear reporting structure and agreed reporting formats; viii. a clear and specified process of change management; ix. access control policy, covering: a. the different reasons, requirements, and benefits that make the access by the third party necessary; b. permitted access methods, and the control and use of unique identifiers such as user IDs and passwords; c. an authorization process for user access and privileges; d. a requirement to maintain a list of individuals authorized to use the services being made available, and what their rights and privileges are with respect to such use; e. a statement that all access that is not explicitly authorized is forbidden; and f. a process for revoking access rights or interrupting the connection between systems; x. arrangements for reporting, notification (e.g., how when and to whom), and investigation of information security incidents and security breaches, as well as violations of the requirements stated in the agreement, stating: a. the third party, following the discovery of a breach of unsecured covered information, shall notify the organization of such breach, including the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach; b. all notifications shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach if the BA is an agent of the covered entity, otherwise the timing of the notification should be explicitly addressed in the contract if the BA is not an agent of the covered entity ; c. evidence shall be maintained demonstrating that all notifications were made without unreasonable delay; and d. any other information that may be needed in the notification to individuals, either at the time notice of the breach is provided or promptly thereafter as information becomes available. xi. a description of the product or service to be provided, and a description of the information to be made available along with its security classification (see CSF 07.d); xii. the target level of service and unacceptable levels of service; xiii. the definition of verifiable performance criteria, their monitoring and reporting; xiv. the right to monitor, and revoke, any activity related to the organization's assets; xv. the right to audit responsibilities defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors; xvi. the penalties exacted in the event of any failure in respect of the above;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	xvii. the establishment of an escalation process for problem resolution; xviii. service continuity requirements, including measures for availability and reliability, in accordance with an organization's business priorities; xix. the respective liabilities of the parties to the agreement; xx. responsibilities with respect to legal matters and how it is ensured that the legal requirements are met (e.g., data protection legislation) especially taking into account different national legal systems if the agreement involves co-operation with organizations in other countries (see 6.1); xxi. intellectual property rights (IPRs) and copyright assignment (see 6. b) and protection of any collaborative work (see 5.e); and xxii. conditions for renegotiation/termination of agreements: a. a contingency plan shall be in place in case either party wishes to terminate the relation before the end of the agreements; b. renegotiation of agreements if the security requirements of the organization change; and c. current documentation of asset lists, licenses, agreements or rights relating to them. The organization shall establish and document personnel security requirements including security roles and responsibilities for third-party providers that are coordinated and aligned with internal security roles and responsibilities and monitor provider compliance. A screening process shall also be carried out for contractors and third party users. Where contractors are provided through an organization the contract with the organization shall clearly specify the organization's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern. In the same way, the agreement with the third party shall clearly specify all responsibilities and notification procedures for screening. The organization requires third-party providers to notify a designated individual or role (e.g., a member of the contracting or supply chain function) of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within fifteen (15) calendar days.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PS-7 (HIGH) • CSA LG-02 • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(4)(ii)(B) • HIPAA § 164.308(b)(1) • HIPAA § 164.314(a)(1) • HIPAA § 164.314(a)(2)(i) • HIPAA § 164.314(a)(2)(ii) • HIPAA § 164.314(b)(1) • HIPAA § 164.314(b)(2)(i)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• HIPAA § 164.314(b)(2)(ii) • HIPAA § 164.314(b)(2)(iii) • HIPAA § 164.314(b)(2)(iv) • HIPAA § 164.404(b) • HIPAA § 164.410(a)(1) • HIPAA § 164.410(a)(2) • HIPAA § 164.410(b) • HIPAA § 164.410(c)(1) • HIPAA § 164.410(c)(2) • HIPAA § 164.414(b) • IRS Pub 1075 v2014 9.3.13.7 • ISO/IEC 27002-2005 6.2.3 • ISO/IEC 27002-2013 A.15.1.1 • ISO/IEC 27002-2013 A.15.1.2 • ISO/IEC 27002-2013 A.15.1.3 • MARS-E v1 PS-7 • NIST Cybersecurity Framework ID.AM-6 • NIST Cybersecurity Framework ID.GV-2 • NIST Cybersecurity Framework PR.AT-3 • NIST Cybersecurity Framework PR.IP-11 • NIST Cybersecurity Framework DE.CM-6 • NIST SP 800-53 R4 PS-7 • NRS 603A.210.2 • NRS 603A.215.1 • PCI DSS v3 2.6 • PCI DSS v3 12.8.2 • PCI DSS v3 12.8.5 • PCI DSS v3 12.9 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.03(2)(f) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Regulatory Factors:	Subject to FTC Red Flags Rule Compliance, Subject to FISMA Compliance; Subject to CMS Minimum Security Requirements (High), Subject to FTI Compliance, Subject to MARS-E Requirements
Level 2 Implementation:	Level 1 plus: Organizations shall employ formal contracts that, at a minimum, specify: i. the confidential nature and value of the covered information; ii. the security measures to be implemented and/or complied with, including the organization's information security requirements as well as appropriate controls required by applicable federal laws, Executive Orders, directives, policies, regulations, standards and guidance; iii. limitations to access to these services by third parties; iv. the service levels to be achieved in the services provided; v. the format and frequency of reporting to the organization's Information Security Management Forum; vi. the arrangement for representation of the third party in appropriate organization meetings and working groups; vii. the arrangements for compliance auditing of the third parties; viii. the penalties exacted in the event of any failure in respect of the above; and ix. the requirement to notify a specified person or office of any personnel transfers or terminations of third-party personnel working at organizational facilities with organizational credentials, badges, or information system privileges within one (1) business day.
Level 2 Control Standard Mapping:	• 16 CFR Part §681.1 (e)(4) • CMSRs 2013v2 SA-9 (HIGH) • IRS Pub 1075 v2014 9.3.15.7 • IRS Pub 1075 v2014 9.4.1 • ISO 27799-2008 7.3.3.3 • NIST SP800-54 R4 SA-9 • MARS-E v1 SA-9 • 1 TAC § 390.2(a)(3)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

FTI Requirements

FTI Custodians:	Organizations shall ensure acquisition contracts contain appropriate language from IRS Pub 1075 v2014 Exhibit 7, Safeguarding Contract Language. Organizations must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled, and accessed inside the cloud through a legally binding contract or Service Level Agreement (SLA) with its third-party cloud provider. Additional SLA requirements include but are not limited to: i. FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate using the FIPS 140-2 compliant module. ii. FTI may need to be encrypted while at rest in the cloud, depending upon the security protocols inherent in the cloud. If the cloud environment cannot appropriately isolate FTI, encryption is a potential compensating control. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant and operate using the FIPS 140-2 compliant module. iii. Storage devices where FTI has resided must be securely sanitized or destroyed using methods acceptable by NSA and Central Security Service (CSS). Organization-defined security controls for third-party arrangements (e.g., in cloud service providers) must be identified, documented (e.g., in a legally-binding contract or SLA), and implemented. The defined security controls, as implemented, must comply with the requirements specified in IRS Pub 1075 v2014.

Health Information Exchange Requirements

Health Information Exchanges:	As part of the agreement with the connecting organizations, the HIE shall specify the requirements of the connecting organization to define and communicate to the HIE access roles for the connecting organization's employees. The agreement shall specify that it is the sole responsibility of the connecting organization to appropriately restrict access in accordance with federal and state requirements (e.g., mental health information). As part of the agreement with the connecting organizations, the HIE shall specify the requirements of connecting organizations to request and receive detailed access logs (see 09.aa) related to the connecting organization's records.

Health Insurance Exchange Requirements

Health Insurance	The organization ensures that service level agreements define expectations of

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Exchanges:	performance, describe measurable outcomes, and identify remedies and response requirements for any identified instance of non-compliance.

PCI-DSS Requirements

PCI Data:	The organization shall identify and document information about which PCI DSS requirements are managed by each service provider, and which are managed by the organization.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Category: 06.0 – Compliance

Objective Name: 06.01 Compliance with Legal Requirements

Control Objective:	To ensure that the design, operation, use, and management of information systems adheres to applicable laws, statutory, regulatory or contractual obligations, and any security requirements.

Control Reference: 06.a Identification of Applicable Legislation

Control Specification:	All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organization.
Factor Type:	Organizational
Topics:	Awareness and Training Documentation and Records Policies and Procedures Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FTC Red Flags Rule Compliance, Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	All relevant statutory, regulatory and contractual requirements shall be explicitly defined and formally documented for each information system type. The specific controls and individual responsibilities to meet these requirements shall be similarly defined and documented. These controls shall be communicated to the user community through the documented security training and awareness programs.
Level 1 Control Standard Mapping:	• 16 CFR Part §681 Appendix A VII(a) • 16 CFR Part §681 Appendix A VII(b) • 16 CFR Part §681 Appendix A VII(c)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• 16 CFR Part §681 Appendix A VII(d) • CSA CO-05 • ISO/IEC 27002-2005 15.1.1 • ISO/IEC 27002-2013 A.18.1.1 • ISO 27799-2008 7.12.2.1 • NIST Cybersecurity Framework ID.GV-3 • (State of Mass.) 201 CMR 17.03(1) • 1 TAC § 390.2(a)(3) • 1 TAC § 390.2(a)(4)(B)(xviii)(I)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: Join industry trade associations, subscribe to thought leadership and market research organizations, or establish some other reliable process to stay abreast of business sector, industry, technology, infrastructure, legal and regulatory environment trends that may impact your organization security policies. Incorporate the consequences of these trends into the development or update of the IT policies and procedures.
Level 2 Control Standard Mapping:	None

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Regulatory Factors:	
Level 3 Implementation:	No additional requirements

Control Reference: 06.b Intellectual Property Rights

Control Specification:	Detailed procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.
Factor Type:	Organizational
Topics:	Documentation and Records Policies and Procedures Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Procedures shall be developed and implemented to ensure compliance with any legislative, regulatory, or contractual requirements that may place restrictions on the copying of proprietary material including copyrights, design rights, or trademarks. Specifically, the following controls shall be in place: i. acquiring software only through known and reputable sources, to ensure that copyright is not violated; ii. maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.; iii. implementing controls to ensure that any maximum number of users permitted is not exceeded; iv. carrying out annual checks that only authorized software and licensed products are installed; v. developing and providing a policy for maintaining agreed upon license conditions; vi. using manual audit tools; vii. complying with terms and conditions for software and information

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	obtained from public networks; and viii. use of proprietary software must also be in compliance with encryption, export and local data privacy regulations.
Level 1 Control Standard Mapping:	• CSA CO-06

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: The following controls shall be in place: i. publishing an intellectual property rights compliance policy which defines the legal use of software and information products; ii. maintaining awareness of policies to protect intellectual property rights, and giving notice of the intent to take disciplinary action against personnel breaching them; iii. maintaining appropriate asset registers, and identifying all assets with requirements to protect intellectual property rights; iv. developing and providing a policy for disposing or transferring software to others; v. not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law; and vi. not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.
Level 2 Control Standard Mapping:	• ISO/IEC 27002-2005 15.1.2 • ISO/IEC 27002-2013 A.18.1.2 • ISO 27799-2008 7.12.2.1

Level 3 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: The organization shall control and document the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. Software license tracking can be accomplished by manual methods (e.g., simple spreadsheets) or automated methods (e.g., specialized tracking applications) depending on organizational needs.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 CM-10 (HIGH) • IRS Pub 1075 v2014 9.3.5.10 • MARS-E v1 SA-6 • NIST Cybersecurity Framework DE.CM-3 • NIST SP 800-53 R4 CM-10

FTI Requirements

FTI Custodians:	The organization must establish restrictions on the use of open source software, and any open source software used by the organization must: i. Be legally licensed; ii. Approved by the agency IT department; and iii. iii. Adhere to a secure configuration baseline checklist from the U.S. Government or industry.

Control Reference: 06.c Protection of Organizational Records

Control Specification:	Important records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
Factor Type:	Organizational
Topics:	Cryptography Data Loss Prevention

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Documentation and Records Policies and Procedures Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act, Subject to the State of Nevada Security of Personal Information Requirements, Subject to Joint Commission Accreditation
Level 1 Implementation:	Important records, such as contracts, personnel records, financial information, patient records, etc., of the organization shall be protected from loss, destruction and falsification. Security controls, such as access controls, encryption, backups, electronic signatures, locked facilities or containers, etc., shall be implemented to protect these essential records and information. Guidelines shall be issued by the organization on the ownership, classification, retention, storage, handling and disposal of all records and information. Designated senior management within the organization shall review and approve the security categorizations and associated guidelines. All regulatory and legislative retention requirements shall be met. The organization's formal policies and procedures, other critical records (e.g., results from a risk assessment) and disclosures of individuals' protected health information made shall be retained for a minimum of 6 years. For electronic health records, the organization must retain records of disclosures to carry out treatment, payment and health care operations for a minimum of 3 years. The covered entity documents compliance with the notice requirements by retaining copies of the notices issues by the covered entity for a period of 6 years and, if applicable, any written acknowledgements of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgement. The covered entity shall document restrictions in writing and formally maintain such writing, or an electronic copy of such writing, as an organizational record for a period of six (6) years. The covered entity documents and maintains the designated record sets that are subject to access by individuals and the titles of the persons or office responsible for receiving and processing requests for access by individuals as

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	organizational records for a period of six (6) years. The covered entity documents and maintains accountings of disclosure as organizational records for a period of six (6) years, including the information required for disclosure, the written accounting provided to the individual, and the titles of the persons or offices responsible for receiving and processing requests for an accounting. The covered entity ensures, if retained, PHI is safeguarded for a period of 50 years following the death of the individual.
Level 1 Control Standard Mapping:	• HIPAA § 164.530(j) • HIPAA § 164.520(e) • HIPAA § 164.522(a)(3) • HIPAA § 164.524(e) • HIPAA § 164.528(d) • HIPAA § 164.502(f) • HIPAA § 164.414(a) • IRS Pub 1075 v2014 4.2 • IRS Pub 1075 v2014 9.3.6.7 • JCAHO IM.02.01.03, EP 6 • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework PR.PT-1 • NIST SP 800-53 R4 AU-11 • NRS 603A.210.1 • NRS 603A.210.3 • (State of Mass.) 201 CMR 17.03(2)(g) • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(3)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements, Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization shall establish a formal record retention program that addresses: i. the secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of covered information (see 09.p and 08.l); ii. coverage over all storage of covered information; and iii. a programmatic review process (automatic or manual) to identify and remove covered information that exceeds the requirements of the data retention policy on a quarterly basis. Detailed procedures for record storage, access, retention, and destruction shall be implemented. In doing so, the following controls shall be implemented: i. a retention schedule shall be drawn up identifying essential record types and the period of time for which they must be retained; ii. an inventory of sources of key information shall be maintained; iii. any related cryptographic keys shall be kept securely and made available only when necessary; and iv. any related cryptographic keying material and programs associated with encrypted archives or digital signatures, shall also be stored to enable decryption of the records for the length of time the records are retained.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AU-11 (HIGH) • CMSRs 2013v2 SI-12 (HIGH) • IRS Pub 1075 v2014 9.3.3.11 • IRS Pub 1075 v2014 9.3.17.9 • ISO/IEC 27002-2005 15.1.3 • ISO/IEC 27002-2013 A.18.1.3 • ISO 27799-2008 7.12.2.1 • MARS-E v1 AU-11 • MARS-E v1 SI-12 • NIST SP 800-53 R4 DM-2 • NIST SP 800-53 R4 DM-2(1) • NRS 603A.215.1 • PCI DSS v3 3.1 • NIST SP 800-53 R4 SI-12 • 1 TAC § 390.2(a)(4)(A)(xi)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization shall retain output, including but not limited to audit records, system records, business and financial reports, and business records, from the information system in accordance with CMS Policy and all applicable National Archives and Records Administration (NARA) requirements.

Federal Requirements

Federal Agencies and Contractors:	The organization shall, where feasible, configure its information systems to record the date PII/PHI is collected, created, or updated and when PII/PHI is to be deleted or archived under an approved record retention schedule.

FTI Requirements

FTI Custodians:	The organization shall employ a permanent system of standardized records of request for disclosure of FTI and maintain the records for five (5) years or the applicable records control schedule, whichever is longer. To support the audit of FTI activities, all organizations must ensure that audit information is archived for seven (7) years to enable the recreation of computer-related accesses to both the operating system and to the application wherever FTI is stored, support after-the-fact investigations of security incidents, and meet regulatory and agency information retention requirements.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The organization shall retain output, including but not limited to audit records, system records, business and financial reports, and business records, from the information system in accordance with Policy and all applicable National Archives and Records Administration (NARA) requirements.

PCI-DSS Requirements

PCI Data:	The organization shall keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	i. Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements ii. Processes for secure deletion of data when no longer needed iii. Specific retention requirements for cardholder data iv. A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.

Control Reference: 06.d Data Protection and Privacy of Covered Information

Control Specification:	Data protection and privacy shall be ensured as required in relevant legislation, regulations, and contractual clauses. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Awareness and Training Data Loss Prevention IT Organization and Management Roles and Responsibilities Monitoring Requirements (Legal and Contractual) Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to the State of Nevada Security of Personal Information Requirements, Subject to Joint Commission Accreditation
Level 1 Implementation:	An organizational data protection and privacy policy shall be developed and implemented. This policy shall be communicated to all persons involved in the processing of covered information. Compliance with this policy and all relevant data protection legislation and regulations shall be supported by management structure and control. Responsibility for handling covered information and ensuring awareness of the data protection principles shall be dealt with in accordance with relevant legislation and regulations. Technical security controls, including access controls and monitoring, and organizational measures to protect covered information shall be implemented. There shall be an appointment of a person responsible, such as a data protection officer, who shall provide guidance to managers, users, and service

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	providers on their individual responsibilities and the specific procedures that shall be followed. Where required by legislation, consent shall be obtained before any protected information (e.g., about a patient) is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the organization. The information system protects the confidentiality and integrity of information at rest. Covered information, at minimum, shall be rendered unusable, unreadable, or indecipherable anywhere it is stored, including on personal computers (laptops, desktops) portable digital media, backup media, servers, databases, or in logs, by using any of the following approaches: i. full disk encryption (mandatory for laptops and other mobile devices that support full-disk encryption, see 01.x) ii. virtual disk encryption iii. volume disk encryption iv. file and folder encryption The encryption approach shall be implemented using one or a combination of the following: i. one-way hashes based on strong cryptography ii. truncation iii. strong cryptography with associated key-management processes and procedures The system shall implement one of the following encryption algorithms: i. AES-CBC (AES in Cipher Block Chaining mode) with a 128-bit key minimum ii. Triple DES (3DES-CBC) If encryption is not applied because it is determined to not be reasonable or appropriate, the organization shall document its rationale for its decision. If disk encryption is used (rather than file- or column-level database encryption), logical access shall be managed independently of native operating system access control mechanisms, and decryption keys shall not be tied to user accounts. See NIST SP800-111 Guide to Storage Encryption Technologies for End User Devices for more information on implementing strong cryptography technologies. Organizations shall explicitly identify and ensure the implementation of security and privacy protections for the transfer of organizational records, or extracts of such records, containing sensitive personal information to a state or federal agency or other regulatory body that lawfully collects such information.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 SC-28 (HIGH) • CSA IS-18 • Guidance to render PHI unusable, unreadable, or indecipherable (1)(i) • Guidance to render PHI unusable, unreadable, or indecipherable (1)(ii)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• HIPAA § 164.530(a) • ISO/IEC 27002-2005 15.1.4 • ISO/IEC 27002-2013 A.18.1.4 • ISO 27799-2008 7.12.2.2 • IRS Pub 1075 v2014 4.2 • IRS Pub 1075 v2014 8.3 • IRS Pub 1075 v2014 9.3.6.7 • IRS Pub 1075 v2014 9.3.16.15 • JCAHO IM.02.01.03, EP 2 • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework DE.DP-2 • NIST SP 800-53 R4 AR-1 • MARS-E v1 SC-28 • NRS 603A.210.1 • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(4)(A)(i) • 1 TAC § 390.2(a)(4)(A)(xv)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements, Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: Covered information storage shall be kept to a minimum. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 SI-12 (HIGH) • IRS Pub 1075 v2014 11.1 • IRS Pub 1075 v2014 9.3.17.9 • IRS Pub 1075 v2014 9.4.2 (E.10) • MARS-E v1 SI-12 • NIST Cybersecurity Framework PR.DS-1 • NIST SP 800-53 R4 SI-12 • NIST SP 800-53 R4 AR-2 • ISO 27799-2008 7.9.2.1 • NRS 603A.215.1 • PCI DSS v3 3.4

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• PCI DSS v3 3.4.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

FTI Requirements

FTI Custodians:	Organizations are not allowed to make further disclosures of FTI to their agents or to a contractor unless authorized by statute. Organizations shall ensure that FTI will not be subject to public disclosure. FTI stored on deployed user workstations, in non-volatile storage, shall be encrypted with FIPS-validated or National Security Agency (NSA)-approved encryption during storage (regardless of location) except when no approved encryption technology solution is available that addresses the specific technology.

PCI-DSS Requirements

PCI Data:	The organization shall render the PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: i. One-way hashes based on strong cryptography, (hash must be of the entire PAN) ii. Truncation (hashing cannot be used to replace the truncated segment of the PAN) iii. Index tokens and pads (pads must be securely stored) iv. Strong cryptography with associated key management processes and procedures. If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.

Control Reference: 06.e Prevention of Misuse of Information Assets

Control Specification:	Users shall be deterred from using information assets for unauthorized purposes. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Authorization Awareness and Training Documentation and Records IT Organization and Management Roles and Responsibilities Media and Assets Personnel Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance
Level 1 Implementation:	The following procedures shall be implemented to ensure proper authorization and use of computer information assets: i. notification to all employees that their actions may be monitored and that they consent to such monitoring (Note: the legality of such monitoring must be verified in each legal jurisdiction); ii. acceptable use agreements that shall be signed by all employees of an organization, contractors, and third party users indicating that they have read, understand, and agree to abide by the rules of behavior before management authorizes access to the information system and its resident information and retained by the organization; iii. reviews and updates the rules of behavior every three hundred and sixty-five (365) days; and iv. requires individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge when the rules of behavior are revised/updated. Management shall approve the use of information assets. If any unauthorized

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	activity is identified by monitoring or other means, this activity shall be brought to the attention of the individual manager concerned for consideration of appropriate disciplinary and/or legal action. All employees and contractors are informed in writing (e.g., when they sign rules of behavior or an acceptable use agreement) that violations of security policies may result in sanctions or disciplinary action (see 02.f).
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PL-4 (HIGH) • CMSRs 2013v2 PS-8 (HIGH) • HIPAA § 164.308(a)(1)(ii)(C) • HIPAA § 164.310(b) • IRS Pub 1075 v2014 9.3.12.3 • IRS Pub 1075 v2014 9.3.13.8 • MARS-E v1 PL-4 • MARS-E v1 PS-8 • NIST Cybersecurity Framework DE.CM-3 • NIST Cybersecurity Framework PR.IP-11 • NIST SP 800-53 R4 PL-4 • NIST SP 800-53 R4 PS-8 • NRS 603A.215.1 • PCI DSS v3 12.3.1 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Computer login banners shall be displayed stating: i. the computer being accessed is private; ii. unauthorized access is prohibited; iii. conditions for access (including consent to monitoring and recording), acceptable use, and access limitations; and iv. privacy and security notices.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The user shall be required to acknowledge the login banner to continue with the log-on.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-8 (HIGH) • IRS Pub 1075 v2014 9.3.1.8 • ISO/IEC 27002-2005 12.5.4 • ISO/IEC 27002-2005 15.1.5 • ISO/IEC 27002-2013 A.12.6.2 • ISO 27799-2008 7.12.2.3 • MARS-E v1 AC-8 • NIST SP 800-53 R4 AC-8

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Requirements

CMS Contractors:	The approved banner for CMS information systems shall read: i. you are accessing a U.S. Government information system, which includes: a. this computer, b. this computer network, c. all computers connected to this network, and d. all devices and storage media attached to this network or to a computer on this network, and ii. this information system is provided for U.S. Government-authorized use only. iii. unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. iv. by using this information system, you understand and consent to the following: a. you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system, and, at any time, and for any lawful Government

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system. b. any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose. For publicly accessible systems: i. displays the system use information when appropriate, before granting further access; ii. displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and iii. includes in the notice given to public users of the information system, a description of the authorized uses of the system.

FTI Requirements

FTI Custodians:	The IRS-approved warning banner must be applied at the application, database, operating system, and network device levels for all systems that receive, process, store, or transmit FTI. For publicly accessible systems, the information system must: i. Display the IRS-approved warning banner granting further access; ii. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and iii. Include a description of the authorized uses of the system. The warning banner must contain reference to the civil and criminal penalty sections of Title 26 Sections 7213, 7213A and 7431.

Control Reference: 06.f Regulation of Cryptographic Controls

Control Specification:	Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.
Factor Type:	Organizational
Topics:	Cryptography IT Organization and Management Roles and Responsibilities Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational	Applicable to all organizations

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Legal advice shall be sought in relation to all relevant regulations by the organization. Compliance with all relevant regulations shall be reviewed on an annual basis at a minimum.
Level 1 Control Standard Mapping:	• HIPAA § 164.308(a)(1)(ii)(D) • HIPAA § 164.312(a)(2)(iv) • HIPAA § 164.312(e)(2)(ii) • NIST Cybersecurity Framework ID.GV-3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Geographic Scope: Multi-state, Geographic Scope: Off-Shore (Outside U.S.)
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall account for any country specific regulations governing the use of cryptographic controls which may include the following: i. import and/or export of computer hardware and software for performing cryptographic functions; ii. import and/or export of computer hardware and software which is designed to have cryptographic functions added to it; iii. restrictions on the usage of encryption; iv. mandatory or discretionary methods of access by the countries to information encrypted by hardware or software to provide confidentiality of content.; and v. mechanisms for authentication to a cryptographic module that meets U.S. requirements for such authentication (e.g., validation under the Cryptographic Module Validation Program to confirm compliance with FIPS 140-2), if applicable. Legal advice shall be specific to either the country where the cryptographic controls are used, or the country to which such controls are imported or exported.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Control Standard Mapping:	• CMSRs 2013v2 IA-7 (HIGH) • CMSRs 2013v2 SC-13 (HIGH) • IRS Pub 1075 v2014 9.3.7.7 • IRS Pub 1075 v2014 9.3.16.9 • ISO/IEC 27002-2005 15.1.6 • ISO/IEC 27002-2013 A.18.1.5 • ISO 27799-2008 7.12.2.3 • MARS-E v1 IA-7 • MARS-E v1 SC-13 • MARS-E v1 SC-13(1) • NIST Cybersecurity Framework PR.AC-1 • NIST SP 800-53 R4 IA-7 • NIST SP 800-53 R4 SC-13

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	When cryptographic mechanisms are used, the organization employs, at a minimum, FIPS 140-2 compliant and NIST-validated cryptography to protect unclassified information.

Objective Name: 06.02 Compliance with Security Policies and Standards and Technical Compliance

Control Objective:	To ensure that the design, operation, use and management of information systems adheres to organizational security policies and standards.

Control Reference: 06.g Compliance with Security Policies and Standards

Control Specification:	Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	policies and standards. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Audit and Accountability Documentation and Records Policies and Procedures Requirements (Legal and Contractual) Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to Joint Commission Accreditation
Level 1 Implementation:	Reviews of the compliance of systems with security and privacy policies, standards and any other security and privacy requirements (HIPAA, legal, etc.) shall be supported by system and information owners. Compliance reviews shall be conducted by security, privacy and/or audit individuals and will incorporate reviews of documented evidence. Automated tools shall be used where possible, but manual processes are acceptable. Annual compliance assessments shall be conducted. If any non-compliance is found as a result of the review, managers shall: i. determine the causes of the non-compliance; ii. evaluate the need for actions to ensure that non-compliance do not recur; iii. determine and implement appropriate corrective action; and iv. review the corrective action taken. The results and recommendations of these reviews shall be documented and approved by management.
Level 1 Control Standard Mapping:	• COBIT 4.1 DS5.5 • COBIT 5 DSS05.07 • CSA IS-13 • HIPAA § 164.308(a)(1)(ii)(D) • HIPAA § 164.308(a)(2) • HIPAA § 164.308(a)(8) • ISO/IEC 27002-2005 15.2.1 • ISO/IEC 27002-2013 A.18.2.2

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• ISO 27799-2008 7.12.3 • JCAHO IM.02.01.03, EP 8 • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework ID.RA-6 • NIST Cybersecurity Framework DE.DP-1 • NIST Cybersecurity Framework DE.DP-4 • NIST SP 800-53 R4 AR-4 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The internal security organization shall regularly review the compliance of information processing as part of a formal risk assessment process. Automated compliance tools/scans shall be used where possible. The organization shall employ assessors or assessment teams to monitor the security controls in the information system on an ongoing basis as part of a continuous monitoring program. These teams will have a level of independence appropriate to the organization's continuous monitoring strategy. The organization shall develop a continuous monitoring strategy and implement a continuous monitoring program that includes: i. establishment of defined metrics to be monitored and defined frequencies for monitoring; ii. ongoing program assessments in accordance with its continuous monitoring strategy that includes, at a minimum: a. annual compliance assessments across the entire organization and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	b. third party independent compliance assessments performed bi-annually; iii. ongoing status monitoring IAW its continuous monitoring strategy; iv. correlation and analysis of security-related information generated by assessments and monitoring; v. response actions to address results of these analyses; and vi. reporting the security state of the information system to appropriate organizational officials monthly. The security organization shall maintain records of the compliance results (e.g., organization-defined metrics) in order to better track security trends within the organization, respond to the results of correlation and analysis, and to address longer term areas of concern.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CA-1 (HIGH) • CMSRs 2013v2 CA-7 (HIGH) • CMSRs 2013v2 CA-7(1) (HIGH) • IRS Pub 1075 v2014 9.3.4.1 • IRS Pub 1075 v2014 9.3.4.6 • IRS Pub 1075 v2014 9.4.2 (E.10) • MARS-E v1 CA-1 • MARS-E v1 CA-7 • MARS-E v1 CA-7(1) • NIST Cybersecurity Framework DE.CM-7 • NIST SP 800-53 R4 CA-1 • NIST SP 800-53 R4 CA-7 • NIST SP 800-53 R4 CA-7(1)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization employs assessors or assessment teams with CMS CISO defined level of independence to monitor the security controls in the

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	information system on an ongoing basis.

FTI Requirements

FTI Custodians:	Organizations must ensure that data warehousing meets minimum security requirements defined in the current revision of NIST SP 800-53 and address the methodology used to inform management, define accountability, and address known security vulnerabilities.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The use of independent security assessment agents or teams to monitor security controls is not required; however, if the organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis, this can be used to satisfy ST&E requirements.

Control Reference: 06.h Technical Compliance Checking

Control Specification:	Information systems shall be regularly checked for compliance with security implementation standards.
Factor Type:	Organizational
Topics:	Audit and Accountability Requirements (Legal and Contractual) Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The organization shall check the technical security configuration of systems. Checking shall be performed either manually, by an individual with experience with the systems, and/or with the assistance of automated software tools. These compliance checks shall be performed annually. If any non-compliance is found as a result of the review, the organization shall:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	i. determine the causes of the non-compliance; ii. evaluate the need for actions to ensure that non-compliance do not recur; iii. determine and implement appropriate corrective action; and iv. review the corrective action taken.
Level 1 Control Standard Mapping:	• COBIT 4.1 DS5.5 • COBIT 5 DSS05.07 • HIPAA § 164.308(a)(1)(ii)(D) • HIPAA § 164.308(a)(8) • ISO/IEC 27002-2005 15.2.2 • ISO/IEC 27002-2013 A.18.2.3 • ISO 27799-2008 7.12.3 • NIST Cybersecurity Framework ID.RA-1 • NIST Cybersecurity Framework ID.RA-6 • NIST Cybersecurity Framework PR.IP-12 • NIST Cybersecurity Framework DE.CM-8 • NIST Cybersecurity Framework RS.MI-3 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Technical compliance checking shall be performed by an experienced technical specialist with the assistance of industry standard automated tools, which generate a technical report for subsequent interpretation. Technical compliance checks shall be performed at least annually, and more frequently where needed based on risk as part of an official risk assessment process. Special attention shall be drawn to compliance for the purpose of technical

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	interoperability.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CA-2(2) (HIGH) • CMSRs 2013v2 CA-7 (HIGH) • CMSRs 2013v2 RA-5 (HIGH) • IRS Pub 1075 v2014 9.3.4.6 • IRS Pub 1075 v2014 9.3.14.3 • MARS-E v1 CA-7 • MARS-E v1 CA-7(2) • MARS-E v1 RA-5 • NIST SP 800-53 R4 CA-7 • NIST SP 800-53 R4 RA-5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization shall include as part of security control assessments, within every three hundred sixty-five (365) days, announced or unannounced in-depth system monitoring; vulnerability scanning; malicious user testing; insider threat assessment; and performance/load testing.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	Plans, schedules, and conducts automated or manual assessments on a continuous and unannounced basis, of all information systems and information systems that are processing data on behalf of or directly for including, but not limited to, in-depth monitoring of systems and networks, vulnerability and configuration scanning, and announced penetration testing to ensure compliance with all vulnerability mitigation procedures.

Objective Name: 06.03 Information System Audit Considerations

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Objective:	Ensure the integrity and effectiveness of the information systems audit process.

Control Reference: 06.i Information Systems Audit Controls

Control Specification:	Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to, to minimize the risk of disruptions to business processes.
Factor Type:	Organizational
Topics:	Audit and Accountability Documentation and Records Monitoring

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	At a minimum, an annual audit planning and scoping process shall exist and give consideration to risk, involvement of technical and business staff, other ongoing projects, and business impacts that may impact the effectiveness of the audit. If desired, a smaller quarterly process can be utilized to minimize impact to operations. The quarterly process shall ensure the entire organization is audited annually.
Level 1 Control Standard Mapping:	• HIPAA § 164.308(a)(1)(ii)(B) • HIPAA § 164.310(a)(2)(ii) • HIPAA § 164.312(b) • HIPAA § 164.316(a) • HIPAA § 164.316(b)(1) • HIPAA § 164.316(b)(2)(iii) • NIST Cybersecurity Framework DE.DP-2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall develop, disseminate, and review/update annually: i. a formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ii. formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. While planning and performing operational system audits, the following shall be addressed: i. audit requirements shall be agreed upon with appropriate management; ii. the scope of the checks shall be agreed and controlled; iii. the checks shall be limited to read-only access to software and data; iv. access other than read-only shall only be allowed for isolated copies of system files, which shall be erased when the audit is completed; v. IT resources for performing the checks shall be explicitly identified and made available; vi. requirements for special or additional processing shall be identified and agreed; vii. all access shall be monitored and logged to produce a reference trail; viii. all procedures, requirements and responsibilities shall be documented; ix. the person(s) carrying out the audit shall be independent of the activities audited; x. scheduling of the audits shall be performed during times of least impact to business operations, for example, not during other audits such as financial audits, end of major financial periods, deployments of major systems, etc.; and xi. audits shall be scheduled in advance to ensure availability of proper individuals and systems, and coordination of all business units.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Control Standard Mapping:	• CMSRs 2013v2 AU-1 (HIGH) • CMSRs 2013v2 PL-2 (HIGH) • CSA CO-01 • IRS Pub 1075 v2014 9.3.3.1 • IRS Pub 1075 v2014 9.3.12.2 • ISO/IEC 27002-2005 15.3.1 • ISO/IEC 27002-2013 A.12.7.1 • ISO 27799-2008 7.12.4 • MARS-E v1 AU-1 • MARS-E v1 PL-2 • NIST Cybersecurity Framework PR.PT-1 • NIST Cybersecurity Framework DE.DP-1 • NIST Cybersecurity Framework DE.DP-4 • NIST SP 800-53 R4 AU-1 • NIST SP 800-53 R4 PL-2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 06.j Protection of Information Systems Audit Tools

Control Specification:	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.
Factor Type:	Organizational
Topics:	Audit and Accountability Authorization User Access
Products and Services Guide:	06.j Protection of Information Systems Audit Tools

Level 1 Implementation Requirements

Level 1	Applicable to all organizations

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Organizational Factors:	
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.
Level 1 Control Standard Mapping:	• CSA IS-29

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance; Subject to CMS Minimum Security Requirements (High); Subject to MARS-E Requirements; Subject to FTI Compliance
Level 2 Implementation:	Level 1 plus: Information systems audit tools (e.g., software or data files) shall be separated from development and operational systems and not held in tape libraries or user areas. Access to these tools shall be documented and enforced per a formal procedure, restricted to authorized individuals only, and approved by designated system owners. Use of these tools shall only be authorized after receiving permission from system owners and as part of a documented assessment process. Specific controls identified within the access control section shall also be enforced for the audit tools. Audits of these controls shall be performed at least annually.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AU-9 (HIGH) • IRS Pub 1075 v2014 9.3.3.10 • ISO/IEC 27002-2005 15.3.2 • ISO 27799-2008 7.12.4 • MARS-E v1 AU-9 • NIST Cybersecurity Framework DE.DP-1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST SP 800-53 R4 AU-9

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Category: 07.0 - Asset Management

Objective Name: 07.01 Responsibility for Assets

Control Objective:	To ensure that management requires ownership and defined responsibilities for the protection of information assets.

Control Reference: 07.a Inventory of Assets

Control Specification:	All assets including information shall be clearly identified and an inventory of all assets drawn up and maintained. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Contingency Planning Documentation and Records IT Organization and Management Roles and Responsibilities Media and Assets Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The organization shall identify and inventory all assets including information (e.g., ePHI, PII) and document the importance of these assets. The asset inventories shall include all information necessary in order to recover from a disaster, including type or classification of the asset, format, location, backup information, license information, and a business value. The inventory shall not duplicate other inventories unnecessarily, but it shall be ensured that the content is aligned. The organization shall maintain an inventory of authorized wireless access points including a documented business justification, to support unauthorized

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	WAP identification (see 09.m) and response (see 11.c). Specific policies shall exist for maintaining records of organizational property (capital and non-capital) assigned to employees, contractors, or volunteers. Organization management shall be responsible for establishing procedures to issue and inventory property assigned to employees. Records of property assigned to employees shall be reviewed and updated annually. The record shall be used to document and ensure that all property is returned to the organization upon employee termination or transfer out of the organization or department. Organizations that assign organization owned property to contractors shall ensure that the procedures for assigning and monitoring the use of the property are included in the contract. If organization owned property is assigned to volunteer workers, there shall be a written agreement specifying how and when the property will be inventoried and how it shall be returned upon completion of the volunteer assignment. The organization shall create and document the process/procedure the organization intends to use for deleting data from hard-drives prior to property transfer, exchange, or disposal/surplus. The organization shall create and document the process/procedure the organization intends to use, transfer, exchange or dispose of an IT-related asset (according to the organization's established lifecycle).
Level 1 Control Standard Mapping:	• CSA FS-08 • HIPAA § 164.310(d)(1) • HIPAA § 164.310(d)(2)(iii) • NIST Cybersecurity Framework ID.AM-1 • NIST Cybersecurity Framework ID.AM-2 • NIST Cybersecurity Framework ID.AM-5 • NIST Cybersecurity Framework PR.DS-3 • PCI DSS v3 11.1.1 • PCI DSS v3 12.3.3 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	> 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: Ownership and information classification shall be agreed and documented for each of the assets. Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets shall be identified. The organization shall maintain inventory logs of all media and conduct media inventories at least annually.
Level 2 Control Standard Mapping:	• ISO/IEC 27002-2005 7.1.1 • ISO/IEC 27002-2013 A.8.1.1 • ISO 27799-2008 7.4.1 • NRS 603A.215.1 • PCI DSS v3 2.4 • PCI DSS v3 9.7.1 • PCI DSS v3 9.9 • PCI DSS v3 9.9.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: The organization shall create, document, and maintain a process and procedure to physically inventory and reconcile IT asset inventory information on hand for: i. capital Assets (Inventory must be conducted at least annually) ii. non-Capital Assets The asset inventory shall include:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

i. Unique identifier and/or serial number;
ii. Information system of which the component is a part;
iii. Type of information system component (e.g., server, desktop, application);
iv. Manufacturer/model information;
v. Operating system type and version/service pack Level;
vi. Presence of virtual machines;
vii. Application software version/license information;
viii. Physical location (e.g., building/room number);
ix. Logical location (e.g., IP address, position with the IS architecture);
x. Media access control (MAC) address;
xi. Ownership by position and role;
xii. Operational status;
xiii. Primary and secondary administrators; and
xiv. Primary user.

The organization shall:

i. employ automated mechanisms to scan the network no less than weekly to detect the presence of unauthorized components/devices (including hardware, firmware and software) into the information system; and
ii. disable network access by such components/devices and notify designated organizational officials.

The organization shall implement an IT Asset Lifecycle Program, monitor its effectiveness making changes as needed. The organization shall implement six stages for the lifecycle of an IT Asset. The following activities for each stage shall include:

i. planning – defining supporting processes, setting standards for configuration and retention, aligning purchase plans to business goals, collecting aggregate information on intended purchases, and negotiating volume discounts.
ii. procurement – requisitioning, approving requisitions, ordering, receiving, and validating orders
iii. deployment – tagging assets, entering asset information in a repository, configuring and installing assets including:
    a. disabling unnecessary or insecure services or protocols;
    b. limiting servers to one primary function; and
    c. defining system security parameters to prevent misuse
iv. management – inventory/counting, monitoring usage (some software), managing contracts for maintenance and support, and monitoring age and configuration.
v. support – adding and changing configurations, repairing devices, and relocating equipment and software.
vi. disposition – removing assets from service, deleting storage contents, disassembling components for reuse, surplusing equipment, terminating contracts, disposing of equipment, and removing asset from active inventory.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization provides each update of the inventory identifying assets with sensitive information (e.g., ePHI, PII) to the CIO or information security official on an organization-defined basis, but no less than annually, to support the establishment of information security requirements for all new or modified information systems containing this information.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 CM-8 (HIGH) • CMSRs 2013v2 CM-8(1) (HIGH) • CMSRs 2013v2 CM-8(2) (HIGH) • CMSRs 2013v2 CM-8(3) (HIGH) • CMSRs 2013v2 CM-8(4) (HIGH) • CMSRs 2013v2 CM-8(5) (HIGH) • CMSRs 2013v2 PM-5 (HIGH) • IRS Pub 1075 v2014 4.5 • IRS Pub 1075 v2014 9.3.5.8 • IRS Pub 1075 v2014 9.4.12 • IRS Pub 1075 v2014 9.4.18 • MARS-E v1 CM-8 • MARS-E v1 CM-8(1) • MARS-E v1 PM-5 • NIST SP 800-53 R4 CM-8 • NIST SP 800-53 R4 CM-8(1) • NIST SP 800-53 R4 CM-8(3) • NIST SP 800-53 R4 CM-8(5) • NIST SP 800-53 R4 PM-5 • NIST SP 800-53 R4 SE-1

CMS Contractor Requirements

CMS Contractors:	The organization shall employ automated mechanisms to help maintain an up-to-date, complete, accurate and readily available inventory of information system components. The organization verifies that all components within the authorization boundary of the information system are not duplicated in other information system inventories. In addition to the creation of the IT Asset Lifecycle Program, the organization shall identify an owner to manage all organization IT asset inventory and management related process and procedure documents. This owner shall ensure that the IT Asset Lifecycle Program shall: i. identify and document personnel with IT asset roles and responsibilities; ii. provide procurement training to personnel with IT asset roles and responsibilities;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	iii. provide procurement training material addressing the procedures and activities necessary to fulfill IT asset roles and responsibilities; iv. define the frequency of refresher training; and v. provide refresher IT asset training in accordance with organization defined frequency, at least on an annual basis.

PCI-DSS Requirements

PCI Data:	The organization shall maintain an inventory of system components that are in scope for PCI DSS. Lists of payment card devices shall be kept up-to-date and include the following: i. Make, model of device ii. Location of device (for example, the address of the site or facility where the device is located) iii. Device serial number or other method of unique identification. The inventory of system components and devices in scope for PCI DSS shall identify all personnel authorized to use the system components and devices.

Control Reference: 07.b Ownership of Assets

Control Specification:	All information and assets associated with information processing systems shall be owned by a designated part of the organization.
Factor Type:	Organizational
Topics:	IT Organization and Management Roles and Responsibilities Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance
Level 1 Implementation:	All information systems shall be documented including a method to accurately and readily determine the assigned owner of responsibility, contact information, and purpose (e.g., through labeling, coding, and/or inventory).
Level 1 Control Standard	• CSA DG-01 • CSA FS-08

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Mapping:	• HIPAA § 164.310(d)(1) • HIPAA § 164.310(d)(2)(iii) • NRS 603A.215.1 • PCI DSS v3 12.3.4 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA; Subject to CMS Minimum Security Requirements (High); Subject to MARS-E Requirements; Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The asset owner (e.g., individual responsible) shall be responsible for: i. ensuring that information and assets associated with information processing systems are appropriately classified; and ii. defining and periodically (at a minimum, annually) reviewing access restrictions and classifications, taking into account applicable access control policies. Responsibility may be allocated to: i. a business process; ii. a defined set of activities; iii. an application; or iv. a defined set of data. The organization shall create and document the process/procedures the organization intends to use to ensure that appropriate software licensing agreements for software used by organization employees are in place and that the organization is in compliance with those agreements. All information and assets associated with information processing systems shall be assigned responsibility to a designated part of the organization. All information shall have an information owner or owners (e.g., designated individuals responsible) established within the organization's lines of business. The information owner(s) shall be responsible to: i. create an initial information classification, including assigning

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	classification levels to all data; ii. approve decisions regarding controls, access privileges of users, and ongoing decisions regarding information management; iii. ensure the information will be regularly reviewed for value and updates to manage changes to risks due to new treats, vulnerabilities, or changes in the environment; iv. perform on an organization pre-defined time frame reclassification based upon business impact analysis, changing business priorities and/or new laws, regulations, and security standards; and v. follow organization's archive document retention rules regarding proper disposition of all information assets. When a person(s) designated as information owner no longer has the responsibility due to departure, transfer or reassignment, the organization shall appoint a new information owner(s) in a timely manner to ensure no lapse in accountability and responsibility for information assets.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CM-8 (HIGH) • IRS Pub 1075 v2014 9.4.2 (E.10) • ISO/IEC 27002-2005 7.1.2 • ISO/IEC 27002-2013 A.8.1.2 • ISO 27799-2008 7.4.1 • MARS-E v1 CM-8 • NIST Cybersecurity Framework ID.AM-6 • NIST Cybersecurity Framework ID.AM-5 • NIST Cybersecurity Framework PR.DS-3 • NIST SP 800-53 R4 CM-8

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

FTI Requirements

FTI Custodians:	All FTI shall have a management official, e.g., an accrediting authority, assigned as an owner to provide responsibility and accountability for its protection.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The agency shall configure control files and data sets to enable the FTI data owner to analyze and review both authorized and unauthorized accesses to a data warehouse.

Control Reference: 07.c Acceptable Use of Assets

Control Specification:	Rules for the acceptable use of information and assets associated with information processing systems shall be identified, documented, and implemented. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Awareness and Training Documentation and Records Media and Assets Personnel

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to State of Massachusetts Data Protection Act, Subject to Joint Commission Accreditation, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	The organization shall establish and make readily available to all information system users, a set of rules that describe their responsibilities and expected behavior with regards to information and information system usage. Employees, contractors and third party users using or having access to the organization's assets shall be aware of the limits existing for their use of organization's information and assets associated with information processing facilities, and resources. They shall be responsible for their use of any information processing resources, and of any such use carried out under their responsibility. Acceptable use shall address: i. rules for electronic mail and Internet usages; and ii. guidelines for the use of mobile devices, especially for the use outside the iii. premises of the organization. The organization shall include in the rules of behavior, explicit restrictions on the use of social media and networking sites, posting information on

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	commercial websites, and sharing information system account information.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PL-4 (HIGH) • CMSRs 2013v2 PL-4(1) (HIGH) • CSA IS-26 • IRS Pub 1075 v2014 9.3.12.3 • ISO/IEC 27002-2005 7.1.3 • ISO/IEC 27002-2013 A.8.1.3 • ISO 27799-2008 7.4.1 • JCAHO IM.02.01.03, EP 1 • MARS-E v1 PL-4 • NIST Cybersecurity Framework PR.DS-5 • NIST SP 800-53 R4 PL-4 • NIST SP 800-53 R4 PL-4(1) • NRS 603A.215.1 • PCI DSS v3 12.3 • PCI DSS v3 12.3.5 • (State of Mass.) 201 CMR 17.03(2)(c)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Objective Name: 07.02 Information Classification

Control Objective:	To ensure that information receives an appropriate and consistent level of protection.

Control Reference: 07.d Classification Guidelines

Control Specification:	Information shall be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.
Factor Type:	Organizational
Topics:	Audit and Accountability IT Organization and Management Roles and Responsibilities Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance
Level 1 Implementation:	Organizations processing protected health information shall uniformly classify such data as confidential, which means that there are limitations to its disclosure within the organization and externally.
Level 1 Control Standard Mapping:	• HIPAA § 164.308(a)(1)(ii)(A) • HIPAA § 164.308(a)(1)(ii)(B) • NIST Cybersecurity Framework ID.AM-5 • NIST Cybersecurity Framework PR.DS-5 • NIST SP 800-53 R4 RA-2 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	> 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to Joint Commission Accreditation, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall categorize (classify) records by type (e.g., accounting records, database records, transaction logs, audit logs and operational procedures) with details of storage media and document the results. Classifications and associated protective controls for information shall take account of: i. business needs for sharing or restricting information; ii. the business impacts associated with such needs; and iii. the aggregation effect (see 9.p). Classification guidelines shall include conventions for initial classification and reclassification over time in accordance with the access control policy. It shall be the responsibility of the asset owner (see 7.b) to: i. define the classification of an asset; ii. periodically review the classification; iii. ensure it is kept up to date; and iv. ensure it is at the appropriate level. Consideration shall be given to the number of classification categories and the benefits to be gained from their use. Overly complex schemes can become cumbersome and uneconomic to use or prove impractical. The level of protection shall be assessed by analyzing confidentiality, integrity and availability and any other requirements for the information considered. Organizations shall identify, record, and control inventory items that have a high risk of loss such as computer and electronic equipment and hand tools and instruments. Personal property meeting the definition of capital assets shall be capitalized, tagged with an organization identification tag and property control number, listed on the capital asset property inventory, and physically inventoried at least annually. Discrepancies shall be investigated. Documentation that a physical inventory has been taken, for all locations, shall be retained in the organization's central accounting office. The organization shall create and document process and procedure to affix an organization identification tag to:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	i. newly purchased IT-related assets (Tagging required prior to deployment in the computing environment); ii. existing non-capital assets (Tagging required within 1 year); and iii. existing capital assets (Tagging required within 1 year). Care shall be taken in interpreting classification labels on documents from other organizations, which may have different definitions for the same or similarly named labels. The organization shall document security categorizations (including supporting rationale) in the security plan for the information system.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 RA-2 (HIGH) • CSA DG-02 • IRS Pub 1075 v2014 9.4.2 (E.10) • ISO/IEC 27002-2005 7.2.1 • ISO/IEC 27002-2013 A.8.2.1 • ISO 27799-2008 7.4.2.1 • JCAHO IM.02.01.03, EP 5 • MARS-E v1 RA-2 • NIST Cybersecurity Framework ID.RA-4 • NIST Cybersecurity Framework ID.RA-5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	Level 2 plus: Organizations shall establish a classification schema to differentiate between various levels of sensitivity and value. Information assets shall be classified according to their level of sensitivity as follows: • Level 1: Low-sensitive information. Information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of employees, clients, and partners. This includes information regularly made available to the public via electronic, verbal or hard

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	copy. • Level 2: Sensitive information that may not to be protected from public disclosure but if made easily and readily available. The organization shall follow its disclosure policies and procedures before providing this information to external parties. • Level 3: Sensitive information intending for limiting business use that can be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of employees, clients, or partners. • Level 4: Information that is deemed extremely sensitive and is intended for use by named individuals only. This information is typically exempt from public disclosure. Users of health information systems shall be notified and made aware when the data they are accessing contains personal health information.
Level 3 Control Standard Mapping:	None

FTI Requirements

FTI Custodians:	Access controls in a data warehouse are classified in general as follows: i. General users ii. Limited access users iii. Unlimited access users. FTI shall always fall into the limited access user's category.

Control Reference: 07.e Information Labeling and Handling

Control Specification:	An appropriate set of procedures for information labeling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organization.
Factor Type:	Organizational
Topics:	Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory	Subject to State of Massachusetts Data Protection Act

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 Implementation:	Organizations shall physically and/or electronically label and handle sensitive information commensurate with the risk of the information or document. Care shall be given to ensure patient information subject to special handling, e.g., HIV test results and mental health and substance abuse-related records, is identified and appropriate labeling and handling requirements are expressly defined and implemented consistent with applicable federal and state legislative and regulatory requirements and industry guidelines. The labeling shall reflect the classification according to the rules in the information classification policy. Items to include are printed reports, screen displays, recorded media (e.g., tapes, disks, CDs, electronic messages, and file transfers). The organization may exempt specific types of media or hardware components, as specified, in writing, by the CIO or his/her designated representative, from marking as long as the exempted items remain within a secure environment.
Level 1 Control Standard Mapping:	• CSA DG-03 • HIPAA § 164.310(b) • HIPAA § 164.310(c) • HIPAA § 164.310(d)(1) • NIST Cybersecurity Framework PR.DS-5 • NIST Cybersecurity Framework PR.PT-2 • (State of Mass.) 201 CMR 17.03(2)(g) • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(4)(A)(ii) • 1 TAC § 390.2(a)(4)(A)(vi) • 1 TAC § 390.2(a)(4)(A)(vii) • 1 TAC § 390.2(a)(4)(B)(iv)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Compliance
Level 2 Implementation:	Level 1 plus:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Procedures for information labeling shall cover information assets in physical and electronic formats, supported by automated tools. Output from systems containing information that is classified as being sensitive or critical shall carry an appropriate classification label (in the output). For each classification level, handling procedures including the secure processing, storage, transmission, declassification, and destruction shall be defined. This shall also include the procedures for chain of custody and logging of any security relevant event. Agreements with other organizations that include information sharing shall include procedures to identify the classification of that information and to interpret the classification labels from other organizations.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 MP-3 (HIGH) • IRS Pub 1075 v2014 9.3.10.3 • IRS Pub 1075 v2014 9.4.3 • IRS Pub 1075 v2014 9.4.4 • ISO/IEC 27002-2005 7.2.2 • ISO/IEC 27002-2013 A.8.2.2 • MARS-E v1 MP-3 • NIST SP 800-53 R4 MP-3 • NRS 603A.215.1 • PCI DSS v3 9.6.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	Level 2 plus: Information belonging to different classification levels shall be logically or physically separated. Whenever possible information assets classified as "Critical" shall be stored in a separate, secure area. All information systems processing covered information (e.g., PHI) shall inform users of the confidentiality of covered information accessible from the system (e.g., at start-up or log-in).

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Control Standard Mapping:	• ISO 27799-2008 7.4.2.2

FTI Requirements

FTI Custodians:	The agency must label removable media and information system output containing FT to indicate the distribution limitations and handling caveats (note IRS Notice 129-A or Notice 129-B are available for this purpose). Properly label emails that contain FTI (e.g., email subject contains "FTI") to ensure that the recipient is aware that the message content contains FTI. The agency includes a cover sheet on fax transmissions that explicitly provides guidance to the recipient, which includes: i. A notification of the sensitivity of the data and the need for protection; and ii. ii. A notice to unintended recipients to telephone the sender—collect, if necessary—to report the disclosure and confirm destruction of the information.

Texas Covered Entities

Texas Covered Entities:	Freestanding emergency medical facilities shall implement the Health and Human Services Executive Commissioner's minimum standards for the contents, maintenance, and release of medical records and shall designate an individual to be in charge of the creation, maintenance and disposal of medical records per TAC § 131.53, including the confidentiality, security and safe storage of medical records throughout the record's lifecycle.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Category: 08.0 - Physical and Environmental Security

Objective Name: 08.01 Secure Areas

Control Objective:	To prevent unauthorized physical access, damage, and interference to the organization's premises and information.

Control Reference: 08.a Physical Security Perimeter

Control Specification:	Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information assets.
Factor Type:	Organizational
Topics:	Authorization Physical and Facility Security Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Computers that store or process covered information shall not be located in areas that are unattended and have unrestricted access by the public. These computers shall be located in rooms with doors and windows that shall be locked when unattended and external protection shall be considered for windows, particularly at ground level (public, sensitive and restricted areas). Perimeters of a building or site containing information assets shall be physically sound; there shall be no gaps in the perimeter or areas where a break-in could easily occur. The external walls of the site shall be of solid construction and all external doors shall be protected against unauthorized access with control mechanisms (e.g., bars, alarms, locks etc.).
Level 1 Control Standard	• CSA FS-03 • HIPAA § 164.310(a)(1)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Mapping:	• HIPAA § 164.310(a)(2)(iii) • HIPAA § 164.310(b) • HIPAA § 164.310(c) • NIST Cybersecurity Framework PR.AC-2 • NIST Cybersecurity Framework DE.CM-2 • NIST Cybersecurity Framework DE.CM-7 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: Security perimeters, such as any boundaries where security controls are in place to protect assets from unauthorized access, shall be clearly defined, and the siting and strength of each of the perimeters shall depend on the security requirements of the assets within the perimeter (public, sensitive and restricted areas). A manned reception area or other means to control physical access to the site or building shall be in place. Access to sites and buildings shall be restricted to authorized personnel only (sensitive and restricted areas). Different levels of scrutiny shall be applied to public areas in which non-employees are expected, such as, exam rooms, hallways, nurse stations, and communications closet, data center. Physical barriers shall, where applicable, be built to prevent unauthorized physical access and environmental contamination (sensitive and restricted areas). Any repairs or modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks) shall be documented and retained in accordance with the organization's retention policy.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	All fire doors on a security perimeter shall be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance to suitable regional, national, and international standards. They shall operate in accordance with local fire code in a fail safe manner.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 MA-2 (HIGH) • CMSRs 2013v2 SC-24 (HIGH) • IRS Pub 1075 v2014 9.3.9.2 • MARS-E v1 MA-2 • NIST Cybersecurity Framework DE.DP-2 • NRS 603A.215.1 • PCI DSS v3 9.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: Information assets and facilities managed by the organization shall be physically separated from those managed by third parties. Two (2) barriers to access covered information under normal security shall be required: i. secured perimeter/locked container; ii. locked perimeter/secured interior; or iii. locked perimeter/security container. Covered information shall be containerized in areas where other than authorized employees may have access afterhours.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 PE-3 (HIGH) • IRS Pub 1075 v2014 4.2 • IRS Pub 1075 v2014 4.3 • IRS Pub 1075 v2014 4.5 • IRS Pub 1075 v2014 9.3.11.3

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• IRS Pub 1075 v2014 9.4.11 • IRS Pub 1075 v2014 9.4.15 • IRS Pub 1075 v2014 9.4.18 • ISO/IEC 27002-2005 9.1.1 • ISO/IEC 27002-2013 A.11.1.1 • ISO 27799-2008 7.6.1.1 • MARS-E v1 PE-3 • NIST SP 800-53 R4 PE-3

FTI Requirements

FTI Custodians:	Minimum protection standards require two physical barriers between FTI and an individual not authorized to access FTI. The perimeter is enclosed by slab-to-slab walls constructed of durable materials and supplemented by periodic inspection. Any lesser-type partition must be supplemented by electronic intrusion detection and fire detection systems. All doors entering the space must be locked in accordance with Locking Systems for Secured Areas. In the case of a fence/gate, the fence must have intrusion detection devices or be continually guarded, and the gate must be either guarded or locked with intrusion alarms. A security room is a room that has been constructed to resist forced entry. The entire room must be enclosed by slab-to-slab walls constructed of approved materials (e.g., masonry brick, concrete) and supplemented by periodic inspection, and entrance must be limited to specifically authorized personnel. Door hinge pins must be non-removable or installed on the inside of the room. FTI must be containerized in areas where other than authorized employees or authorized contractors may have access afterhours. A security guard, custodial services worker or landlord may have access to a locked building or a locked room if FTI is in a locked container. If FTI is in a locked room, but not in a locked container, the guard, janitor or landlord may have a key to the building but not to the room. During business hours, if authorized personnel serve as the second barrier between FTI and unauthorized individuals, the authorized personnel must wear an identification badge or credential clearly displayed, preferably work above the waist.

Control Reference: 08.b Physical Entry Controls

Control Specification:	Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	*Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Authentication Authorization Documentation and Records Monitoring Physical and Facility Security Third Parties and Contractors User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	At a minimum, the organization: i. develops, approves and maintains a list of individuals with authorized access to the facility where the information system resides; ii. issues authorization credentials for facility access; and iii. reviews the access list and authorization credentials periodically but no less than quarterly, iv. removes individuals from the facility access list when access is no longer required. For facilities where the information system resides, the organization shall enforce physical access authorizations at defined entry/exit points to the facility where the information system resides, maintain physical access audit logs, and provide security safeguards the organization determines are necessary for areas officially designated as publicly accessible. Except those areas officially designated as publicly accessible, the organization shall maintain visitor access logs for facilities where information systems reside for at least two years and review visitor records periodically but no less than monthly. Visitor records shall contain: i. name and organization of the person visiting; ii. signature of the visitor; iii. form of identification; iv. date of access; v. time of entry and departure;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	vi. purpose of visit; and vii. name and organization of person visited. Access to areas where sensitive information (e.g., covered information, payment card data) is processed or stored shall be controlled and restricted to authorized persons only. All visitors shall be escorted and supervised (their activities monitored) unless their access has been previously approved. Third party support service personnel shall be granted restricted access to secure areas or covered information processing facilities only when required. This access shall be authorized and monitored.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PE-2 (HIGH) • CMSRs 2013v2 PE-3 (HIGH) • CMSRs 2013v2 PE-8 (HIGH) • CSA FS-02 • CSA FS-04 • HIPAA § 164.310(a)(1) • HIPAA § 164.310(a)(2)(iii) • HIPAA § 164.310(b) • HIPAA § 164.310(c) • IRS Pub 1075 v2014 4.3.1 • IRS Pub 1075 v2014 9.3.11.2 • IRS Pub 1075 v2014 9.3.11.3 • IRS Pub 1075 v2014 9.3.11.7 • MARS-E v1 PE-2 • MARS-E v1 PE-3 • MARS-E v1 PE-7 • MARS-E v1 PE-7(1) • MARS-E v1 PE-8 • NIST Cybersecurity Framework PR.AC-2 • NIST Cybersecurity Framework DE.CM-2 • NIST Cybersecurity Framework DE.CM-7 • NIST SP 800-53 R4 PE-2 • NIST SP 800-53 R4 PE-3 • NIST SP 800-53 R4 PE-8 • PCI DSS v3 9.4 • PCI DSS v3 9.4.1 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year,

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: A visitor log shall be required including: i. the date and time of entry and departure; ii. the visitor's name; iii. the organization represented; and iv. the employee authorizing physical access. The log shall be reviewed no less than monthly and upon occurrence of organization-defined security events, and retained for at least three months in accordance with the organization's retention policy. Visitors shall only be granted access for specific and authorized purposes and shall be issued with instructions on the security requirements of the area and on emergency procedures. Authentication controls (e.g., access control card plus PIN) shall be used to authorize and validate all access. Access must be authorized and based on individual job function. An audit trail of all access shall be securely maintained. The organization shall ensure onsite personnel and visitors can be easily distinguished. All employees, contractors and third party users and all visitors shall be required to wear some form of visible identification and shall immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification. Visitors shall be given a badge or access device that identifies them as non-employees, and they shall be required to surrender the badge or device before leaving the facility or upon expiration. The organization shall ensure onsite personnel and visitor identification (e.g., badges) are revoked or terminated when expired or when access is no longer authorized, and all physical access mechanisms, such as keys, access cards and combinations, are returned disabled or changed. Identification should also be updated when access requirements change to ensure their status can be easily distinguished. Access rights to secure areas shall be regularly reviewed, at a minimum every 90 days, and updated and revoked when necessary. A restricted area, security room, or locked room is used to control access to

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	areas containing covered information. These areas will be controlled accordingly.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 PE-6 (HIGH) • IRS Pub 1075 v2014 4.3.2 • IRS Pub 1075 v2014 9.3.11.6 • ISO/IEC 27002-2005 9.1.2 • ISO/IEC 27002-2013 A.11.1.2 • ISO 27799-2008 7.6.1.2 • MARS-E v1 PE-6 • NIST Cybersecurity Framework RS.CO-3 • NIST SP 800-53 R4 PE-6 • NRS 603A.215.1 • PCI DSS v3 9.1 • PCI DSS v3 9.2 • PCI DSS v3 9.3 • PCI DSS v3 9.4 • PCI DSS v3 9.4.2 • PCI DSS v3 9.4.3 • PCI DSS v3 9.4.4

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: Doors to internal secure areas shall lock automatically, implement a door delay alarm, and be equipped with electronic locks (e.g., keypad, card swipe). The organization shall inventory physical access devices within every ninety (90) days. Combinations and keys for organization-defined high-risk entry/exit points shall be changed within every three hundred and sixty-five (365) days and when keys are lost, combinations are compromised. Intruder detection systems shall be installed to national, regional or

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	international standards and regularly tested, at a minimum annually, to cover all external doors and accessible windows. Unoccupied areas shall be alarmed at all times. Cover shall also be provided for other areas (e.g., computer room or communications rooms) specifically sensitive and restricted areas. The organization shall monitor and investigate notifications from physical intrusion alarms and surveillance equipment.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 PE-3(1) (HIGH) • CMSRs 2013v2 PE-6(1) (HIGH) • CMSRs 2013v2 PE-8(1) (HIGH) • IRS Pub 1075 v2014 4.3 • IRS Pub 1075 v2014 4.3.2 • IRS Pub 1075 v2014 9.3.11.6 • MARS-E v1 PE-6(1) • NIST Cybersecurity Framework RS.AN-1 • NIST Cybersecurity Framework DE.DP-2 • NIST Cybersecurity Framework DE.DP-3 • NIST SP 800-53 R4 PE-6(1)

CMS Contractor Requirements

CMS Contractors:	The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at defined physical spaces (defined in the applicable security plan) containing a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers, etc.). The organization shall employ automated mechanisms to facilitate the maintenance and review of access records.

FTI Requirements

FTI Custodians:	A visitor access log containing specific data elements will be used to authenticate and authorize visitor's access to any facility where FTI resides, either electronically or in paper, at the location where the outside (2nd) barrier is breached. The organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at spaces where FTI is received, processed, stored, or transmitted. Unauthorized access to areas containing FTI during duty and non-duty hours must be denied. This can be done utilizing a combination of methods: secured or locked perimeter, secured area or containerization. The physical security and control of computers and electronic media must be addressed. Computer operations must be in a secure area with restricted

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	access. A restricted area visitor log will be maintained at a designated entrance to the restricted area and all visitors (persons not assigned to the area) entering the area shall be directed to the designated entrance. The entry control monitor should verify the identity of visitors by comparing the name and signature entered into the register with some type of photo identification card. Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited. Whenever cleaning and maintenance personnel are working in restricted areas containing FTI, the cleaning and maintenance activities must be performed in the presence of an authorized employee.

PCI-DSS Requirements

PCI Data:	The organization shall ensure visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained. Visitor logs shall include the name of the onsite personnel (workforce member) authorizing physical access.

Control Reference: 08.c Securing Offices, Rooms, and Facilities

Control Specification:	Physical security for offices, rooms, and facilities shall be designed and applied.
Factor Type:	Organizational
Topics:	Physical and Facility Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Account shall be taken of relevant health and safety regulations and standards when securing facilities.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Control Standard Mapping:	• HIPAA § 164.310(a)(1) • HIPAA § 164.310(a)(2)(iii) • HIPAA § 164.310(b) • HIPAA § 164.310(c) • NIST Cybersecurity Framework DE.DP-2 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Critical facilities shall be sited to avoid access by the public. For particularly sensitive and restricted facilities (e.g., data centers and communication closets) buildings shall be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities. Directories and internal telephone books identifying locations of covered information processing facilities shall not be readily accessible by the public. Video cameras or other access control mechanisms shall be implemented and secured to monitor individual physical access to sensitive areas. These devices shall be protected from tampering or disabling of the device. The results of the mechanisms shall be reviewed regularly and correlated with other entries and access control information (e.g., audit trails, sign in sheets, authorization levels, maintenance logs). The information from cameras or other access control mechanisms shall be stored for at least three months in accordance with the organizations retention policy. Automated mechanisms shall be used to recognize potential intrusions and initiate designated response actions.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 PE-3 (HIGH) • COBIT 4.1 DS5.7 • COBIT 5 DSS05.05

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• CSA FS-01 • IRS Pub 1075 v2014 9.3.11.3 • ISO/IEC 27002-2005 9.1.3 • ISO/IEC 27002-2013 A.11.1.3 • ISO 27799-2008 7.6.1.2 • MARS-E v1 PE-3 • NIST Cybersecurity Framework PR.AC-2 • NIST Cybersecurity Framework DE.CM-2 • NIST Cybersecurity Framework DE.CM-3 • NIST Cybersecurity Framework DE.CM-7 • NIST SP 800-53 R4 PE-3 • NRS 603A.215.1 • PCI DSS v3 9.1.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 08.d Protecting Against External and Environmental Threats

Control Specification:	Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Awareness and Training Physical and Facility Security Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational	Applicable to all organizations

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The organization shall develop, disseminate, and review/update annually: i. formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ii. formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. The following controls shall be implemented to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster: i. appropriate fire extinguishers shall be located throughout the facility, and shall be no more than 50 feet away from critical electrical components; and ii. fire detectors (e.g., smoke or heat activated) shall be installed on and in the ceilings and floors. Fire authorities shall be automatically notified when a fire alarm is activated.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PE-1 (HIGH) • CSA RS-06 • HIPAA § 164.310(a)(1) • HIPAA § 164.310(a)(2)(ii) • HIPAA § 164.310(a)(2)(iii) • IRS Pub 1075 v2014 9.3.11.1 • ISO/IEC 27002-2005 9.1.4 • ISO/IEC 27002-2013 A.11.1.4 • ISO 27799-2008 7.6.1.2 • MARS-E v1 PE-1 • NIST Cybersecurity Framework PR.IP-5 • NIST SP 800-53 R4 PE-1 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2	BioTech Organizations: > $100,000 Spend on Research and Development Per

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Organizational Factors:	Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: Any security threats presented by neighboring premises shall be identified (e.g., a fire in a neighboring building, water leaking from the roof or in floors below ground level or an explosion in the street). Fire prevention training shall be included in the regular training programs provided to the organization personnel. Appropriate fire suppression systems (e.g., sprinklers, gas) shall be implemented throughout the building and within secure areas containing information processing devices. For facilities not staffed continuously, these suppression systems shall be automated. The building's HVAC system shall be configured to automatically shut down upon fire detection.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 PE-13(3) (HIGH) • CSA RS-05 • MARS-E v1 PE-13(3) • NIST SP 800-53 R4 PE-13(3)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	Requirements
Level 3 Implementation:	Level 2 plus: Water detectors shall be located in the dropped ceilings and raised floors to detect leaks or possible flooding. The organization shall protect the information systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel. Fire suppression and detection devices/systems are implemented and maintained that are supported by an independent energy source.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 PE-13 (HIGH) • CMSRs 2013v2 PE-13(1) (HIGH) • CMSRs 2013v2 PE-13(2) (HIGH) • CMSRs 2013v2 PE-15 (HIGH) • CMSRs 2013v2 PE-15(1) (HIGH) • IRS Pub 1075 v2014 4.3 • MARS-E v1 PE-13 • MARS-E v1 PE-13(1) • MARS-E v1 PE-13(2) • MARS-E v1 PE-15 • NIST SP 800-53 R4 PE-13 • NIST SP 800-53 R4 PE-15

CMS Contractor Requirements

CMS Contractors:	The organization employs automated mechanisms to detect the presence of water in the vicinity of the information system and alerts defined personnel or roles (defined in the applicable security plan). Fire suppression devices/systems shall activate automatically and automatically notify the organization and emergency responders in the event of a fire.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	Fire suppression devices/systems shall activate automatically and automatically notify the organization and emergency responders in the event of a fire.

Control Reference: 08.e Working in Secure Areas

Control Specification:	Physical protection and guidelines for working in secure areas shall be designed and applied.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factor Type:	Organizational
Topics:	Personnel Physical and Facility Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FTI Requirements
Level 1 Implementation:	The arrangements for working in secure areas shall include controls for the employees, contractors, and third party users working in the secure area, as well as other third party activities taking place there. Personnel shall only be aware of the existence of, or activities within, a secure area on a need to know basis. Unsupervised working in secure areas shall be avoided both for safety reasons and to prevent opportunities for malicious activities. Vacant secure areas shall be physically locked and periodically checked. Photographic, video, audio or other recording equipment such as cameras in mobile devices, shall not be allowed unless otherwise authorized.
Level 1 Control Standard Mapping:	• HIPAA § 164.310(a)(2)(iii) • HIPAA § 164.310(c) • IRS Pub 1075 v2014 4.5 • ISO/IEC 27002-2005 9.1.5 • ISO/IEC 27002-2013 A.11.1.5 • ISO 27799-2008 7.6.1.2 • NIST Cybersecurity Framework PR.AC-2 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

FTI Requirements

FTI Custodians:	All computers, electronic media, and removable media containing FTI, must be kept in a secured area under the immediate protection and control of an authorized employee or locked up. When not in use, the media must be promptly returned to a proper storage area/container.

Control Reference: 08.f Public Access, Delivery, and Loading Areas

Control Specification:	Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.
Factor Type:	Organizational
Topics:	Media and Assets Physical and Facility Security User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	Access to a delivery and loading area from outside of the building shall be restricted to identified and authorized personnel. The delivery and loading area shall be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building. The external doors of a delivery and loading area shall be secured when the internal doors are opened. Incoming material shall be registered in accordance with asset management procedures on entry to the site. Incoming and outgoing shipments shall be physically segregated, where possible.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PE-16 (HIGH) • CSA FS-05 • IRS Pub 1075 v2014 4.3.1 • IRS Pub 1075 v2014 9.3.11.8 • MARS-E v1 PE-16 • NIST SP 800-53 R4 PE-16

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: Incoming material shall be inspected for potential threats before this material is moved from the delivery and loading area to the point of use.
Level 2 Control Standard Mapping:	• ISO/IEC 27002-2005 9.1.6 • ISO/IEC 27002-2013 A.11.1.6 • ISO 27799-2008 7.6.1.3

Level 3 Implementation Requirements

Level 3	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Organizational Factors:	
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Objective Name: 08.02 Equipment Security

Control Objective:	To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

Control Reference: 08.g Equipment Siting and Protection

Control Specification:	Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
Factor Type:	Organizational
Topics:	Media and Assets Physical and Facility Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to CMS Minimum Security Requirements (High), Subject to MARS-E Requirements
Level 1 Implementation:	Guidelines for eating, drinking, and smoking in proximity to information assets shall be established. Lightning protection shall be applied to all buildings, and lightning protection filters (e.g., surge protectors) shall be fitted to all incoming power and communications lines. Information assets handling covered information shall be positioned and the viewing angle restricted to reduce the risk of information being viewed by

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	unauthorized persons during their use, and storage devices secured to avoid unauthorized access. Device locks shall be distributed and implemented for equipment containing covered information. Types of locks include, but are not limited to, slot locks, port controls peripheral switch controls and cable traps. The organization shall restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines. The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy. Controls shall be implemented to minimize the risk of potential physical threats including theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism. The organization shall position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. The following controls shall be implemented to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster: i. Hazardous or combustible materials shall be stored at a safe distance from a secure area; ii. bulk supplies such as stationery shall not be stored within a secure area; and iii. fallback equipment and back-up media shall be stored at a safe distance to avoid damage from disaster affecting the main site.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PE-1 (HIGH) • CMSRs 2013v2 PE-18 (HIGH) • HIPAA § 164.310(a)(1) • HIPAA § 164.310(a)(2)(ii) • HIPAA § 164.310(a)(2)(iii) • HIPAA § 164.310(c) • IRS Pub 1075 v2014 4.3 • IRS Pub 1075 v2014 9.3.11.1 • IRS Pub 1075 v2014 9.3.11.10 • MARS-E v1 PE-1 • MARS-E v1 PE-18 • NIST Cybersecurity Framework PR.IP-5 • NIST SP 800-53 R4 PE-1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NRS 603A.215.1 • PCI DSS v3 9.1.3 • PCI DSS v3 9.9 • PCI DSS v3 9.9.2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Equipment shall be sited to minimize unnecessary access into work areas. Environmental conditions, such as temperature and humidity, shall be monitored for conditions which could adversely affect the operation of information assets. Items requiring special protection shall be isolated to reduce the general level of protection required. The use of special protection methods, such as keyboard membranes, shall be implemented for equipment in industrial environments.
Level 2 Control Standard Mapping:	• CSA RS-06 • IRS Pub 1075 v2014 9.4.3 • IRS Pub 1075 v2014 9.4.9 • ISO/IEC 27002-2005 9.2.1 • ISO/IEC 27002-2013 A.11.2.1 • ISO 27799-2008 7.6.2.1

Level 3 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

FTI Requirements

FTI Custodians:	Multifunction Devices (MFDs) are locked with a mechanism to prevent physical access to the hard disk. Place fax machines in a secured area.

PCI-DSS Requirements

PCI Data:	The organization shall periodically inspect payment card device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).

Control Reference: 08.h Supporting Utilities

Control Specification:	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.
Factor Type:	Organizational
Topics:	Contingency Planning Maintenance Monitoring Physical and Facility Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Regulatory Factors:	None
Level 1 Implementation:	All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning shall be adequate for the systems they are supporting. Support utilities shall be regularly inspected and tested to ensure their proper functioning and to reduce any risk from their malfunction or failure. A suitable electrical supply shall be provided that conforms to the equipment manufacturer's specifications. An uninterruptable power supply (UPS) to support orderly close down shall be required for equipment supporting critical business operations. Power contingency plans shall cover the action to be taken on failure of the UPS. UPS equipment and generators shall be regularly checked to ensure they have adequate capacity and are tested in accordance with the manufacturer's recommendations. The water supply shall be stable and adequate to supply air conditioning, humidification equipment and fire suppression systems, where used. Malfunctions in the water supply system may damage equipment or prevent fire suppression from acting effectively.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PE-11 (HIGH) • CMSRs 2013v2 PE-11(1) (HIGH) • CSA RS-07 • CSA RS-08 • ISO 27799-2008 7.6.2.2 • MARS-E v1 PE-11 • NIST Cybersecurity Framework ID.BE-4 • NIST Cybersecurity Framework PR.IP-5 • NIST SP 800-53 R4 PE-11

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance; Subject to CMS Minimum Security Requirements (High); Subject to MARS-E Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Implementation:	Level 1 plus: The organization maintains temperature and humidity levels in facilities where critical information processing systems reside within acceptable vendor-recommended levels and monitors these levels at an organization-defined frequency. Organizations shall evaluate the level of alert and follow prescribed guidelines for that alert level, alert component management of possible loss of service and/or media, and, if necessary, report damage and provide remedial action. Implement contingency plan. Emergency lighting shall be provided in case of main power failure that covers emergency exists and evacuation routes within the facility. Emergency power off switches shall be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. These devices shall be protected from accidental activation. A master power switch or emergency cut-off switch is implemented and maintained, prominently marked and protected by a cover, for data center, servers, and mainframe rooms. An alarm system to detect malfunctions in the supporting utilities shall be evaluated and installed if required. Only authorized maintenance personnel are permitted to access infrastructure assets, including power generators, HVAC systems, cabling, and wiring closets.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 PE-9 (HIGH) • CMSRs 2013v2 PE-10 (HIGH) • CMSRs 2013v2 PE-12 (HIGH) • CMSRs 2013v2 PE-14 (HIGH) • MARS-E v1 PE-9 • MARS-E v1 PE-10 • MARS-E v1 PE-12 • MARS-E v1 PE-14 • NIST Cybersecurity Framework PR.AC-2 • NIST SP 800-53 R4 PE-9 • NIST SP 800-53 R4 PE-10 • NIST SP 800-53 R4 PE-12 • NIST SP 800-53 R4 PE-14

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	
Level 3 Implementation:	Level 2 plus: Voice services shall be adequate to meet local legal requirements for emergency communications.
Level 3 Control Standard Mapping:	• ISO/IEC 27002-2005 9.2.2 • ISO/IEC 27002-2013 A.11.2.2

CMS Contractor Requirements

CMS Contractors:	The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

Provider Requirements

Providers	Level 1 Providers: A back-up generator shall be considered if processing is required to continue in case of a prolonged power failure. An adequate supply of fuel shall be available to ensure that the generator, if used, can perform for a prolonged period. Level 2 Providers: A back-up generator shall be implemented and an adequate supply of fuel shall be available to ensure that the generator can perform for a prolonged period. Generators shall be regularly checked to ensure they have adequate capacity and are tested in accordance with the manufacturer's recommendations. Level 3 Providers: Multiple power sources or a separate power substation shall be used. Telecommunications equipment shall be connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services. The organization shall develop telecommunications service agreements that contain priority of service (Telecommunications Service Priority) provisions.

Control Reference: 08.i Cabling Security

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Specification:	Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.
Factor Type:	Organizational
Topics:	Media and Assets Physical and Facility Security Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The organization shall protect power equipment and power cabling for the information system from damage and destruction. Access to patch panels and cable rooms shall be controlled. A documented patch list shall be used to reduce the possibility of errors. Clearly identifiable cable and equipment markings shall be used to minimize handling errors, such as accidental patching of wrong network cables.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PE-9 (HIGH) • HIPAA § 164.310(a)(1) • HIPAA § 164.310(c) • MARS-E v1 PE-9 • NIST SP 800-53 R4 PE-9 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Power and telecommunications lines into information processing facilities shall be underground, where possible, or subject to adequate alternative protection. Network cabling shall be protected from unauthorized interception or damage, for example by using a conduit or by avoiding routes through public areas. Power cables shall be segregated from communications cables to prevent interference (only applicable where copper telecommunications cables are used). Armored conduit and locked rooms or boxes at inspection and termination points shall be installed. Alternative routings and/or transmission media providing appropriate security shall be used. Electromagnetic shielding shall be used to protect the cables. The organization controls physical access to information system distribution and transmission lines within organizational facilities by disabling any physical ports (e.g., wiring closets, patch panels, etc.) not in use. The organization shall implement physical and/or logical controls to restrict access to publicly accessible network jacks.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 PE-4 (HIGH) • CSA RS-08 • IRS Pub 1075 v2014 4.5 • IRS Pub 1075 v2014 9.3.11.4 • IRS Pub 1075 v2014 9.3.16.6 • ISO/IEC 27002-2005 9.2.3 • ISO/IEC 27002-2013 A.11.2.3 • ISO 27799-2008 7.6.2.2 • MARS-E v1 PE-4 • NIST Cybersecurity Framework PR.AC-2 • NIST SP 800-53 R4 PE-4 • NRS 603A.215.1 • PCI DSS v3 9.1.2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	Level 2 plus: Technical sweeps and physical inspections shall be initiated for unauthorized devices being attached to the cables.
Level 3 Control Standard Mapping:	None

FTI Requirements

FTI Contractors:	If encryption is not used to protect the transmission of FTI, the agency must ensure that all network infrastructure, access points, wiring, conduits, and cabling are within the control of authorized agency personnel.

Control Reference: 08.j Equipment Maintenance

Control Specification:	Equipment shall be correctly maintained to ensure its continued availability and integrity. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Documentation and Records Maintenance Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Implementation:	The organization shall develop, disseminate, and review/update annually: i. a formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ii. formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. Equipment shall be maintained in accordance with the supplier's recommended service intervals and specifications. Only authorized maintenance personnel shall carry out repairs and service equipment. Appropriate controls shall be implemented when equipment is scheduled for maintenance (e.g., authorization levels) taking into account whether this maintenance is performed by personnel on site or external to the organization. The organization: i. Establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; ii. Ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and iii. Designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. The organization monitors and controls nonlocal maintenance and diagnostic activities; and prohibits nonlocal system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative. If nonlocal maintenance and diagnostic actives are authorized, the organization: i. Allows the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system; ii. Employs strong identification and authentication techniques in the establishment of nonlocal maintenance and diagnostic sessions; iii. Maintains records for nonlocal maintenance and diagnostic activities; and iv. Terminates all sessions and network connections when nonlocal maintenance is completed. v. The organization obtains maintenance support and/or spare parts for defined key information system components (defined in the applicable security plan) within the applicable Recovery Time Objective (RTO) specified in the contingency plan. All requirements imposed by insurance policies shall be complied with.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 MA-1 (HIGH) • CMSRs 2013v2 MA-4 (HIGH) • CMSRs 2013v2 MA-4(1) (HIGH)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• CMSRs 2013v2 MA-4(3) (HIGH) • CMSRs 2013v2 MA-5 (HIGH) • CMSRs 2013v2 MA-5(1) (HIGH) • CMSRs 2013v2 MA-6 (HIGH) • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.310(a)(2)(iv) • IRS Pub 1075 v2014 9.3.9.1 • IRS Pub 1075 v2014 9.3.9.4 • IRS Pub 1075 v2014 9.3.9.5 • ISO 27799-2008 7.6.2.2 • MARS-E v1 MA-1 • MARS-E v1 MA-4 • MARS-E v1 MA-4(1) • MARS-E v1 MA-5 • MARS-E v1 MA-6 • NIST Cybersecurity Framework PR.MA-1 • NIST Cybersecurity Framework PR.MA-2 • NIST SP 800-53 R4 MA-1 • NIST SP 800-53 R4 MA-4 • NIST SP 800-53 R4 MA-5 • NIST SP 800-53 R4 MA-6 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: Covered information shall be cleared from the equipment, or the maintenance personnel shall be sufficiently cleared prior to all maintenance. Records shall be kept of all suspected or actual faults and all preventive and corrective

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	maintenance including: i. date and time of maintenance; ii. name of individual performing maintenance; iii. name of escort; iv. a description of maintenance performed; and v. a list of equipment removed or replaced. The organization shall check all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 MA-2 (HIGH) • CMSRs 2013v2 MA-2(2) (HIGH) • CSA OP-04 • IRS Pub 1075 v2014 9.3.9.2 • ISO/IEC 27002-2005 9.2.4 • ISO/IEC 27002-2013 A.11.2.4 • MARS-E v1 MA-2 • MARS-E v1 MA-2(1) • NIST Cybersecurity Framework PR.DS-1 • NIST SP 800-53 R4 MA-2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: The organization shall approve, control and monitor the use of information system maintenance tools (e.g., hardware and software brought into the organization for diagnostic/repair actions). All maintenance tools carried into the facility by maintenance personnel shall be inspected for improper or unauthorized modifications. All media containing diagnostic and test programs shall be checked for malicious code prior to the media being used in the information system.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization documents the requirements (e.g., policies and procedures) for the establishment and use of nonlocal maintenance and diagnostic connections in the security plan for the information system.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 MA-3 (HIGH) • CMSRs 2013v2 MA-3(1) (HIGH) • CMSRs 2013v2 MA-3(2) (HIGH) • CMSRs 2013v2 MA-3(3) (HIGH) • CMSRs 2013v2 MA-4(2) (HIGH) • IRS Pub 1075 v2014 9.3.9.3 • IRS Pub 1075 v2014 9.3.9.4 • MARS-E v1 MA-3 • MARS-E v1 MA-3(1) • MARS-E v1 MA-3(2) • MARS-E v1 MA-4(2) • NIST SP 800-53 R4 MA-3 • NIST SP 800-53 R4 MA-3(1) • NIST SP 800-53 R4 MA-3(2) • NIST SP 800-53 R4 MA-4(2)

CMS Contractor Requirements

CMS Contractors:	The organization: i. Implements procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements: a. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; b. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and ii. Develops and implements alternate security safeguards in the event an information system component cannot be sanitized, removed, or disconnected from the system. If password-based authentication is used during remote maintenance, change the passwords following each remote maintenance service. The organization shall audit non-local maintenance and diagnostic sessions

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	using available auditable events and shall review the records of the sessions. The organization shall: i. require that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or ii. remove the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to sensitive information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system. Automated mechanisms are implemented to schedule, conduct, and document maintenance and repairs as required, producing up-to-date, accurate, complete and available records of all maintenance and repair actions, needed, in process and completed. The equipment shall be appropriately sanitized before release; if the equipment cannot be sanitized, the equipment shall remain within control of the organization, be destroyed, or obtain an exemption from the CMS CIO or his/her designated representative explicitly authorizing removal of the equipment from the facility. The organization requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organization information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.

Control Reference: 08.k Security of Equipment Off-Premises

Control Specification:	Security shall be applied to off-site equipment taking into account the different risks of working outside the organization's premises.
Factor Type:	Organizational
Topics:	Authorization IT Organization and Management Roles and Responsibilities Media and Assets Physical and Facility Security

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Compliance
Level 1 Implementation:	Regardless of ownership, the use of any information processing equipment outside the organization's premises shall be authorized by management. This shall include equipment used by remote workers, even where such use is permanent (e.g., a core feature of the employee's role, such as for ambulance personnel or therapists.). Equipment and media taken off the premises shall not be left unattended in public places. Portable computers shall be carried as hand luggage and disguised where possible when travelling. Manufacturers' instructions for protecting equipment shall be observed at all times (e.g., protection against exposure to strong electromagnetic fields). Home-working controls shall be applied, including lockable filing cabinets, clear desk policy, and access controls for computers and secure communication with the office. Adequate insurance coverage shall be in place to protect equipment off-site. Security risks (e.g., of damage, theft or eavesdropping) may vary considerably between locations and shall be taken into account in determining the most appropriate controls.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 R4 MP-5 (HIGH) • CMSRs 2013v2R4 PE-17 (HIGH) • CSA FS-07 • HIPAA § 164.310(a)(2)(i) • HIPAA § 164.310(d)(1) • HIPAA § 164.310(d)(2)(iii) • HIPAA § 164.312(c)(1) • IRS Pub 1075 v2014 9.3.10.5 • IRS Pub 1075 v2014 9.3.11.9 • ISO/IEC 27002-2005 9.2.5 • ISO/IEC 27002-2013 A.11.2.6 • ISO 27799-2008 7.6.2.3 • MARS-E v1 MP-5 • MARS-E v1 PE-17

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST Cybersecurity Framework PR.DS-3 • NIST SP 800-53 R4 MP-5 • NIST SP 800-53 R4 PE-17 • NRS 603A.215.1 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 08.l Secure Disposal or Re-Use of Equipment

Control Specification:	All items of equipment containing storage media shall be checked to ensure that any covered information and licensed software has been removed or securely overwritten prior to disposal. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Data Loss Prevention Media and Assets

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Compliance, Subject to the State of Nevada Security of Personal Information Requirements, Subject to Joint Commission Accreditation
Level 1 Implementation:	Surplus equipment is stored securely while not in use, and disposed of or sanitized when no longer required. Devices containing covered information shall be physically destroyed or the information shall be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function. The following are appropriate techniques to securely remove information: i. disk wiping ii. degaussing The following are appropriate techniques to securely destroy electronic and hard copy media: i. shredding disk platters ii. disintegration iii. grinding surfaces iv. incineration v. pulverization vi. melting See NIST SP800-88 Guidelines for Media Sanitization for more information on implementing media sanitization and destruction techniques. The organization shall render information unusable, unreadable, or indecipherable on system media, both digital and non-digital, prior to disposal or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies. The organization destroys media containing sensitive information that cannot be sanitized.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 MP-6 (HIGH) • CSA DG-05 • Guidance to render PHI unusable, unreadable, or indecipherable (2)(i) • Guidance to render PHI unusable, unreadable, or indecipherable (2)(ii)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• HIPAA § 164.310(d)(1) • HIPAA § 164.310(d)(2)(i) • HIPAA § 164.310(d)(2)(ii) • IRS Pub 1075 v2014 8.2 • IRS Pub 1075 v2014 9.3.10.6 • ISO/IEC 27002-2005 9.2.6 • ISO/IEC 27002-2013 A.11.2.7 • ISO 27799-2008 7.6.2.4 • JCAHO IM.02.01.03, EP 7 • MARS-E v1 MP-6 • NIST Cybersecurity Framework PR.DS-3 • NIST Cybersecurity Framework PR.IP-6 • NIST SP 800-53 R4 MP-6 • NIST SP 800-53 R4 DM-2 • NRS 603A.200.1 • NRS 603A.200.2.b.1 • NRS 603A.200.2.b.2 • NRS 603A.215.1 • PCI DSS v3 9.8.1 • PCI DSS v3 9.8.2 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 3 Implementation:	No additional requirements

Control Reference: 08.m Removal of Property

Control Specification:	Equipment, information or software shall not be taken off-site without prior authorization.
Factor Type:	Organizational
Topics:	Authorization Documentation and Records Media and Assets Personnel Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to Joint Commission Accreditation, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	Equipment, information or software shall not be taken off-site without prior authorization. Employees, contractors and third party users who have authority to permit off-site removal of assets shall be clearly identified. Time limits for equipment removal shall be set and returns checked for compliance. Where necessary and appropriate, equipment shall be recorded as being removed off-site and recorded when returned.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PE-16 (HIGH) • CSA FS-06 • IRS Pub 1075 v2014 4.3.1 • IRS Pub 1075 v2014 9.3.11.8 • ISO/IEC 27002-2005 9.2.7 • ISO/IEC 27002-2013 A.11.2.5 • ISO 27799-2008 7.6.2.5 • JCAHO IM.02.01.03, EP 4 • MARS-E v1 PE-16 • NIST Cybersecurity Framework PR.DS-3 • NIST SP 800-53 R4 PE-16

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Category: 09.0 - Communications and Operations Management

Objective Name: 09.01 Documented Operating Procedures

Control Objective:	To ensure that operating procedures are documented, maintained and made available to all users who need them.

Control Reference: 09.a Documented Operations Procedures

Control Specification:	Operating procedures shall be documented, maintained, and made available to all users who need them.
Factor Type:	System
Topics:	Cryptography Documentation and Records Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Compliance
Level 1 Implementation:	Documented procedures shall be prepared for system activities associated with information and communication assets, including computer start-up and close-down procedures, backup of data, equipment maintenance, media handling, electronic communications, computer room and mail handling management, and safety. The operating procedures shall specify the detailed instructions for the execution of each job including: i. processing and handling of information; ii. the backup of data; iii. scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times; iv. instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	use of system utilities; v. support contacts in the event of unexpected operational or technical difficulties; vi. special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs; vii. system restart and recovery in the event of system failure; and viii. the management of audit-trail and system log information. Operating procedures, and the documented procedures for system activities, shall be treated as formal documents and changes authorized by management.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 MA-1 (HIGH) • CSA OP-01 • CSA OP-02 • HIPAA § 164.310(a)(2)(iv) • IRS Pub 1075 v2014 9.3.9.1 • IRS Pub 1075 v2014 9.4.2 (E.10) • ISO/IEC 27002-2005 10.1.1 • ISO/IEC 27002-2013 A.12.1.1 • ISO 27799-2008 7.7.1.1 • MARS-E v1 MA-1 • NIST SP 800-53 R4 MA-1 • NRS 603A.215.1 • PCI DSS v3 1.5 • PCI DSS v3 2.5 • PCI DSS v3 3.7 • PCI DSS v3 4.3 • PCI DSS v3 5.4 • PCI DSS v3 6.7 • PCI DSS v3 7.3 • PCI DSS v3 8.8 • PCI DSS v3 9.10 • PCI DSS v3 10.8 • PCI DSS v3 11.6 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

FTI Requirements

FTI Custodians:	If data warehousing documentation is integrated with other security documents, these documents shall have a section dedicated to the data warehouse(s) to define controls specific to that environment. The organization shall ensure these documents: i. describe how "legacy system data" will be brought into the data warehouse and how the legacy data that is FTI will be cleansed for the extraction, transformation and loading (ETL) process; and ii. any unique issues related to data warehousing.

PCI-DSS Requirements

PCI Data:	The organization shall ensure operational procedures are documented, communicated (known to all parties) and in use for the following: i. managing firewalls, ii. managing vendor defaults and other security parameters, iii. protecting stored cardholder data, iv. encrypting transmissions of cardholder data, v. protecting systems against malware, vi. developing and maintaining secure systems and applications, vii. restricting access to cardholder data, viii. identification and authentication, ix. restricting physical access to cardholder data, x. monitoring access to network resources and cardholder data, and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	xi. security monitoring and testing.

Control Reference: 09.b Change Management

Control Specification:	Changes to information assets and systems shall be controlled and archived.
Factor Type:	System
Topics:	IT Organization and Management Roles and Responsibilities Media and Assets

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Changes to information assets, including systems, networks and network services, shall be controlled and archived.
Level 1 Control Standard Mapping:	None

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Number of Transactions Per Day: > 6,750, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Changes shall be managed strictly and consistently. Formal management responsibilities and procedures shall be in place to ensure satisfactory control of all changes to equipment, software or procedures, including: i. the identification and recording of significant changes;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	ii. the planning and testing of changes; iii. the assessment of the potential impacts, including security impacts, of such changes; iv. the formal approval for proposed changes; and v. the communication of change details to all relevant persons. Fallback procedures shall be defined and implemented, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CM-3 (HIGH) • CMSRs 2013v2 CM-4 (HIGH) • CMSRs 2013v2 CM-5 (HIGH) • IRS Pub 1075 v2014 9.3.5.3 • IRS Pub 1075 v2014 9.3.5.4 • IRS Pub 1075 v2014 9.3.5.5 • ISO/IEC 27002-2005 10.1.2 • ISO/IEC 27001:2013 8.1 • ISO/IEC 27002-2013 A.12.1.2 • ISO 27799-2008 7.7.1.2 • MARS-E v1 CM-3 • MARS-E v1 CM-4 • MARS-E v1 CM-5 • NIST Cybersecurity Framework PR.IP-3 • NIST SP 800-53 R4 CM-3 • NIST SP 800-53 R4 CM-4 • NIST SP 800-53 R4 CM-5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 09.c Segregation of Duties

Control Specification:	Separation of duties shall be enforced to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	assets. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Authorization IT Organization and Management Roles and Responsibilities Monitoring

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Small organizations may find segregation of duties difficult to achieve, but the principle shall be applied as far as is possible and practicable. Whenever it is difficult to segregate controls such as monitoring of activities, audit trails, management supervision or a system of dual control (e.g., two individuals with separate responsibilities needing to work together to accomplish a task) shall be required. Security audit activities shall always remain independent.
Level 1 Standard Control Mapping:	• HIPAA § 164.308(a)(3)(i) • HIPAA § 164.308(a)(4)(i) • HIPAA § 164.308(a)(4)(ii)(A) • HIPAA § 164.312(a)(1) • NIST Cybersecurity Framework PR.AC-4 • NIST Cybersecurity Framework PR.DS-5 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 2 Regulatory Factors:	Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. No single person shall be able to access, modify or use assets without authorization or detection. The initiation of an event shall be separated from its authorization to reduce the possibility of collusion. The organization shall identify duties that require separation and define information system access authorizations to support separation of duties. Job descriptions shall reflect accurately the assigned duties and responsibilities that support separation of duties. Incompatible duties shall be segregated across multiple users to minimize the opportunity for misuse or fraud. In cases where conflicting duties must be assigned to a single user, activity logging and log reviews by an independent party shall be required.
Level 2 Control Standard Mapping:	• COBIT 4.1 DS5.7 • COBIT 5 DSS05.05 • CSA IS-15 • ISO/IEC 27002-2005 10.1.3 • ISO/IEC 27002-2013 A.6.1.2 • ISO 27799-2008 7.7.1.3 • NIST SP 800-53 R4 AC-5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Pharmaceutical Companies: > 70,000,000 Prescriptions Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to PCI Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: The organization shall:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	i. ensure that audit functions are not performed by security personnel responsible for administering access control; ii. maintain a limited group of administrators with access based upon the users' roles and responsibilities; iii. ensure that mission critical functions and information system support functions are divided among separate individuals; iv. ensure that information system testing functions (i.e., user acceptance, quality assurance, information security) and production functions are divided among separate individuals or groups; v. ensure that an independent entity, not the Business Owner, System Developer(s) / Maintainer(s), or System Administrator(s) responsible for the information system, conducts information security testing of the information system; and vi. ensure that quality assurance and code reviews of custom-developed applications, scripts, libraries, and extensions are conducted by an independent entity, not the code developers.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 AC-5 (HIGH) • IRS Pub 1075 v2014 9.3.1.5 • IRS Pub 1075 v2014 9.4.5 • MARS-E v1 AC-5 • NRS 603A.215.1 • PCI DSS v3 6.4.2

FTI Requirements

FTI Custodians:	To use an Integrated Voice Response (IVR) system that provides FTI over the telephone to a customer, the agency must ensure independent security testing is conducted on the IVR system prior to implementation.

Control Reference: 09.d Separation of Development, Test, and Operational Environments

Control Specification:	Development, test, and operational environments shall be separated and controlled to reduce the risks of unauthorized access or changes to the operational system.
Factor Type:	System
Topics:	IT Organization and Management Roles and Responsibilities Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The organization shall minimize any testing on production systems. When testing must be performed, a test plan shall be developed that documents all changes to the system and the procedures for undoing any changes made to the system (e.g., removing test accounts).
Level 1 Control Standard Mapping:	None

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Number of Transactions Per Day: > 6,750, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to CMS Minimum Security Requirements (High), Subject to MARS-E Requirements; Subject to FTI Compliance
Level 2 Implementation:	Level 1 plus: The level of separation between operational, test, and development environments shall be identified and controls shall be implemented to prevent operational issues, including: i. along with removing accounts, a review of all custom code preceding the release to production or to customers must be completed in order to identify any possible coding vulnerability, to include at least the following: a. code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices; b. code reviews ensure code is developed according to secure coding guidelines; c. appropriate corrections are implemented prior to release; and d. code-review results are reviewed and approved by management prior to release; ii. test data and accounts shall be removed completely before the application is placed into a production state. iii. organizations shall remove all custom application accounts, user IDs, and passwords before applications go from development to

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	production or are released to customers iv. rules for the transfer of software from development to operational status shall be defined and documented; v. development and operational software shall run on different systems or computer processors and in different domains or directories; vi. compilers, editors, and other development tools or system utilities shall not be accessible from operational systems when not required; vii. the test system environment shall emulate the operational system environment as closely as possible; viii. users shall use different user profiles for operational and test systems, and menus shall display appropriate identification messages to reduce the risk of error; and ix. covered information shall not be copied into the test system environment.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CM-2 (HIGH) • CSA SA-06 • IRS Pub 1075 v2014 9.3.5.2 • IRS Pub 1075 v2014 9.4.2 (E.10) • ISO/IEC 27002-2005 10.1.4 • ISO/IEC 27002-2013 A.12.1.4 • ISO 27799-2008 7.7.1.4 • MARS-E v1 CM-2 • NIST Cybersecurity Framework PR.DS-7 • NIST SP 800-53 R4 CM-2 • NRS 603A.215.1 • PCI DSS v3 6.3.1 • PCI DSS v3 6.3.2 • PCI DSS v3 6.4.1 • PCI DSS v3 6.4.3 • PCI DSS v3 6.4.4

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

CMS Contractors:	All systems supporting development and pre-production testing are connected to an isolated network separated from production systems. Network traffic into and out of the development and pre-production testing environment is only permitted to facilitate system testing, and is restricted by source and destination access control lists (ACLs) as well as ports and protocols.

FTI Requirements

FTI Custodians:	Whenever FTI is located on both production and test environments, these environments are to be segregated, especially in the development stages of the data warehouse.

Objective Name: 09.02 Control Third Party Service Delivery

Control Objective:	To ensure that third party service providers maintain security requirements and levels of service as part of their service delivery agreements.

Control Reference: 09.e Service Delivery

Control Specification:	It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated and maintained by the third party. *Required for HITRUST Certification 2015
Factor Type:	System
Topics:	Monitoring Requirements (Legal and Contractual) Services and Acquisitions Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Third Party Support (Vendor Access or Maintenance): Yes
Level 1 Regulatory Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Implementation:	In an agreed service arrangement, service delivery by a third party (e.g., a certification authority for the provision of cryptographic services) shall include: i. service definitions; ii. delivery levels; iii. security controls, including third-party personnel security, information classification, transmission, and authorization; and iv. aspects of service management, including monitoring, auditing, and change management; and v. issues of liability, reliability of services and response times for the provision of services.
Level 1 Control Standard Mapping:	• CSA CO-03 • HIPAA § 164.308(b)(1) • HIPAA § 164.308(b)(3) • HIPAA § 164.314(a)(1) • HIPAA § 164.314(a)(2)(i) • HIPAA § 164.314(a)(2)(ii) • ISO 27799-2008 7.7.2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Geographic Scope: Multi-state, Geographic Scope: Off-Shore (Outside U.S.) , Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Number of Transactions Per Day: > 6,750, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to FTC Red Flags Rule Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall develop, disseminate, and review/update annually a list of current service providers. In the case of outsourcing arrangements, the organization shall plan the necessary transitions (of information, information processing systems, and anything else that needs to be moved), and shall ensure that security is maintained throughout the transition period. The service provider shall protect the company's data with reasonable controls (e.g., policies and procedures) designed to detect, prevent, and mitigate risk.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization shall define and document oversight (e.g., governmental, organizational) and user roles and responsibilities with regard to external information system services. The organization shall ensure that the third party maintains sufficient service capabilities together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.
Level 2 Control Standard Mapping:	• 16 CFR Part §681.2(e)(4) • 16 CFR Part §681 Appendix A VI(c) • CMSRs 2013v2 SA-9 (HIGH) • IRS Pub 1075 v2014 9.3.15.7 • ISO/IEC 27002-2005 10.2.1 • ISO/IEC 27001:2013 8.1 • MARS-E v1 SA-9 • NIST Cybersecurity Framework ID.AM-4 • NIST Cybersecurity Framework PR.AT-3 • NIST Cybersecurity Framework DE.CM-6 • NIST SP 800-53 R4 SA-9 • NRS 603A.215.1 • PCI DSS v3 2.6 • PCI DSS v3 12.8 • PCI DSS v3 12.8.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

FTI Requirements

FTI Custodians:	The organization restricts the location of information systems that receive, process, store, or transmit FTI to areas within the United States territories, embassies, or military installations. FTI may not be accessed by agency employees, agents, representatives or contractors located "off-shore," outside of the United States or its territories. FTI may not be received,

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	stored, processed or disposed via information technology systems located off-shore.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The organization prohibits service providers from outsourcing any system function outside the U.S. or its territories.

Control Reference: 09.f Monitoring and Review of Third Party Services

Control Specification:	The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly to govern and maintain compliance with the service delivery agreements. *Required for HITRUST Certification 2015
Factor Type:	System
Topics:	Audit and Accountability Documentation and Records Incident Response Requirements (Legal and Contractual) Services and Acquisitions Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Third Party Support (Vendor Access or Maintenance): Yes
Level 1 Regulatory Factors:	None
Level 1 Implementation:	A periodic review of service-level agreements (SLAs) shall be conducted at least annually and compared against the monitoring records.
Level 1 Control Standard Mapping:	• CSA CO-03 • HIPAA § 164.308(b)(1) • HIPAA § 164.308(b)(3) • HIPAA § 164.314(a)(1) • HIPAA § 164.314(a)(2)(i) • HIPAA § 164.314(a)(2)(ii) • ISO 27799-2008 7.7.2 • 1 TAC § 390.2(a)(1)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Geographic Scope: Multi-state, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Number of Transactions Per Day: > 6,750, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to FTC Red Flags Rule Compliance; Requirements (High)Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization monitors security control compliance by external service providers on an ongoing basis. Monitoring shall involve a service management relationship and process between the organization and the third party. Service performance levels shall be monitored to check adherence to the agreements. Service reports produced by the third party shall be reviewed and regular progress meetings shall be arranged as required by the agreements. Third party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered shall be reviewed. Information about information security incidents shall be provided to the incident response team. This information shall be reviewed by the third party that experienced the incident and the organization which the third party provides services to as required by the agreements and any supporting guidelines and procedures. Any identified problems shall be resolved and reviewed by the organization as noted above. The organization shall monitor the network service features and service levels to detect abnormalities and violations. The organization shall periodically audit the network services to ensure that network service providers implement the required security features and meet the requirements agreed with management, including with new and existing regulations.
Level 2 Control Standard Mapping:	• 16 CFR Part §681.1 (e)(4) • 16 CFR Part §681 Appendix A VI(c) • CMSRs 2013v2 SA-9 (HIGH) • IRS Pub 1075 v2014 5.3 • IRS Pub 1075 v2014 9.3.15.7 • ISO/IEC 27002-2005 10.2.2 • ISO/IEC 27001:2013 8.1 • ISO/IEC 27002-2013 A.15.2.1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• MARS-E v1 SA-9 • NIST Cybersecurity Framework PR.AT-3 • NIST Cybersecurity Framework DE.CM-6 • NIST SP 800-53 R4 SA-9 • PCI DSS v3 12.8 • PCI DSS v3 12.8.4 • 1 TAC § 390.2(a)(3)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	Geographic Scope: Off-Shore (Outside U.S.) , Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 5,500, Number of Transactions Per Day: > 85,000, Number of Interfaces to Other Systems: > 75
Level 3 Regulatory Factors:	Subject to PCI Compliance
Level 3 Implementation:	Level 2 plus: The organization shall maintain sufficient overall control and visibility into all security aspects for covered and critical information or information processing systems accessed, processed or managed by a third party. The organization shall ensure they retain visibility into security activities such as change management, identification of vulnerabilities, and information security incident reporting and response through a clearly defined reporting process, format and structure.
Level 3 Control Standard Mapping:	• NRS 603A.215.1 • PCI DSS v3 2.6

CMS Requirements

CMS Contractors:	The organization employs defined processes, methods and techniques (defined in the applicable security plan) to monitor security control compliance by external service providers on an ongoing basis.

Control Reference: 09.g Managing Changes to Third Party Services

Control Specification:	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	*Required for HITRUST Certification 2015
Factor Type:	System
Topics:	Risk Management and Assessments Services and Acquisitions Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Third Party Support (Vendor Access or Maintenance): Yes
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The organization shall ensure that third party organization's use appropriate change management procedures for any changes to a third party service or organizational system (see 9.a and 10.k).
Level 1 Control Standard Mapping:	• ISO 27799-2008 7.7.2 • NIST Cybersecurity Framework ID.BE-1 • NIST Cybersecurity Framework PR.AT-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Geographic Scope: Multi-state, Geographic Scope: Off-Shore (Outside U.S.), Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Number of Transactions Per Day: > 6,750, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to FTC Red Flags Rule Compliance
Level 2 Implementation:	Level 1 plus: Change management on a third party service shall include: i. the assessment and explicit recording of the potential impacts, including security impacts, of such changes; ii. evaluating and implementing changes made by the organization for: a. enhancements to the current services offered; b. development of any new applications and systems; c. modifications or updates of the organization's policies and procedures; and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	d. new controls to resolve information security incidents and to improve security; iii. evaluating and implementing changes in third party services for: a. changes and enhancement to networks; b. use of new technologies; c. adoption of new products or newer versions/releases; d. new development tools and environments; e. changes to physical location of service facilities; and f. change of vendors.
Level 2 Control Standard Mapping:	• 16 CFR Part §681.1 (e)(4) • 16 CFR Part §681 Appendix A VI(c) • ISO/IEC 27002-2005 10.2.3 • ISO/IEC 27001:2013 8.1 • ISO/IEC 27002-2013 A.15.2.2 • 1 TAC § 390.2(a)(3)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Objective Name: 09.03 System Planning and Acceptance

Control Objective:	To ensure that systems meet the businesses current and projected needs to minimize failures.

Control Reference: 09.h Capacity Management

Control Specification:	The availability of adequate capacity and resources shall be planned, prepared, and managed to deliver the required system performance. Projections of future capacity requirements shall be made to mitigate the risk of system overload.
Factor Type:	System
Topics:	IT Organization and Management Roles and Responsibilities Monitoring

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Planning

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The use of information and information system resources shall be monitored, and projections made of future capacity requirements to ensure adequate systems performance. Organizations shall allocate sufficient storage capacity to reduce the likelihood of exceeding capacity and reduce the impact on network infrastructure, e.g., bandwidth.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AU-4 (HIGH) • HIPAA § 164.312(b) • IRS Pub 1075 v2014 9.3.3.5 • ISO/IEC 27002:2005 10.3.1 • ISO/IEC 27002-2013 A.12.1.3 • MARS-E v1 AU-4 • NIST Cybersecurity Framework PR.DS-4 • NIST Cybersecurity Framework PR.PT-1 • NIST SP 800-53 R4 AU-4 • 1 TAC §390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Geographic Scope: Multi-state, Geographic Scope: Off-Shore (Outside U.S.), Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Number of Transactions Per Day: > 6,750, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to FISMA Compliance; Requirements (High)Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Capacity and monitoring procedures shall include:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	i. the identification of capacity requirements for each new and ongoing system/service; ii. the projection of future capacity requirements, taking into account current use, audit record storage requirements, projected trends, and anticipated changes in business requirements; and iii. the system monitoring and tuning to ensure and improve the availability and effectiveness of current systems. The information system shall take the following additional actions in response to an audit storage capacity issue: i. shutdown the information system, ii. stop generating audit records, or iii. overwrite the oldest records, in the case that storage media is unavailable. The organization shall protect against or limit the effects of the types of denial of service attacks defined in NIST SP 800-63 Rev. 1, Computer Security Incident Handling Guide, and the following Websites: i. SANS Organization www.sans.org/dosstep; ii. SANS Organization's Roadmap to Defeating DDoS www.sans.org/dosstep/roadmap.php; and iii. NIST CVE List National Vulnerability Database: http://nvd.nist.gov/home.cfm.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AU-5 (HIGH) • CMSRs 2013v2 SC-5 (HIGH) • CSA OP-03 • IRS Pub 1075 v2014 9.3.16.4 • ISO 27799-2008 7.7.3.1 • MARS-E v1 AU-5 • MARS-E v1 SC-5 • NIST SP 800-53 R4 AU-5 • NIST SP 800-53 R4 SC-5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

FTI Requirements

FTI Custodians:	The agency must allocate audit record storage capacity to retain audit records for the required audit retention period of seven years.

Control Reference: 09.i System Acceptance

Control Specification:	Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance to maintain security.
Factor Type:	System
Topics:	Awareness and Training Documentation and Records IT Organization and Management Roles and Responsibilities

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Managers shall ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested. New information systems, upgrades, and new versions shall only be migrated into production after obtaining formal acceptance from management.
Level 1 Control Standard Mapping:	• CSA RM-01

Level 2 Implementation Requirements

Level 2 Organizational Factors:	Geographic Scope: Multi-state, Geographic Scope: Off-Shore (Outside U.S.), Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Number of Transactions Per Day: > 6,750, Number of Interfaces to Other Systems: > 25
Level 2	Subject to FISMA Compliance; Subject to the CMS Minimum Security

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Regulatory Factors:	Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization requires the developer of the information system, system component, or information system service to: i. Create and implement a security assessment plan; ii. Perform unit, integration, system and regression testing/evaluation in accordance with organization-defined requirements for depth and coverage; iii. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; iv. Implement a verifiable flaw remediation process; and v. Correct flaws identified during security testing/evaluation. The following actions shall be carried out prior to formal acceptance being provided: i. an agreed set of security controls are in place; ii. consultation with affected persons, or representatives of affected groups, at all phases of the process; iii. preparation and testing of routine operating procedures to defined standards; iv. effective manual procedures; v. evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end; vi. evidence that an analysis has been carried out to the effect the new system has on the overall security of the organization; vii. training in the operation or use of new systems; viii. error recovery and restart procedures, and contingency plans; ix. ease of use (as this affects user performance and avoids human error); and x. training in the new operation(s). Organizations shall ensure that the IT systems employed contain application functionality that enforces the approval of processes by different role holders. The impact of the installation of any new system shall be thoroughly analyzed and tested with the coverage of the extreme operational conditions of the current systems.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 SA-11 (HIGH) • CSA RM-03 • IRS Pub 1075 v2014 9.3.15.9 • IRS Pub 1075 v2014 9.4.15 • ISO/IEC 27002-2005 10.3.2 • ISO/IEC 27002-2013 A.14.2.9 • ISO 27799-2008 7.7.3.2 • MARS-E v1 SA-11

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST SP 800-53 R4 SA-11

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization requires the developer of the information system, system component, or information system service to: i. Create and implement a security assessment plan in accordance with, but not limited to, current CMS procedures; ii. Perform unit; integration; system; regression testing/evaluation in accordance with the CMS eXpedited Life Cycle (XLC); iii. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; iv. Implement a verifiable flaw remediation process; and v. Correct flaws identified during security testing/evaluation. If the security control assessment results are used in support of the security authorization process for the information system, the organization ensures that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results. The organization uses hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.

FTI Requirements

FTI Custodians:	The agency must submit a request to the IRS Office of Safeguards for authority to use live data for testing, providing a detailed explanation of the safeguards in place to protect the FTI over the Internet to a customer.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	To use a VoIP network that provides FTI to a customer, the agency must ensure security testing is conducted on the VoIP system prior to implementation with FTI.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	If the security control assessment results are used in support of the security authorization process for the information system, the organization ensures that no security relevant modifications of the information systems have been made subsequent to the assessment and after selective verification of the results. The organization uses hypothetical data when executing test scripts or in a test environment that is configured to comply with the security controls as if it is a production environment.

Objective Name: 09.04 Protection Against Malicious and Mobile Code

Control Objective:	Ensure that integrity of information and software is protected from malicious or unauthorized code.

Control Reference: 09.j Controls Against Malicious Code

Control Specification:	Detection, prevention, and recovery controls shall be implemented to protect against malicious code, and appropriate user awareness procedures on malicious code shall be provided. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Awareness and Training Contingency Planning Policies and Procedures Viruses and Malware

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory	Subject to State of Massachusetts Data Protection Act

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 Implementation:	Protection against malicious code shall be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls. Formal policies shall be required and technologies implemented for the timely installation and upgrade of the protective measures, including the installation of anti-virus or anti-spyware software, and for the regular updating of it, including virus definitions, automatically whenever updates are available. Periodic reviews/scans shall be required of installed software and the data content of systems to identify and, where possible, remove any unauthorized software. Procedures shall be defined for response to identification of malicious code or unauthorized software. Checking anti-virus or anti-spy software shall generate audit logs of checks performed. The checks carried out by the malicious code detection and repair software to scan computers and media shall include: i. checking any files on electronic or optical media, and files received over networks, for malicious code before use; ii. checking electronic mail attachments and downloads for malicious code before use; this check shall be carried out at different places (e.g., at electronic mail servers, desk top computers and when entering the network of the organization); and iii. checking web traffic, such as HTML, JavaScript, and HTTP, for malicious code. Formal policies shall be required prohibiting the use or installation of unauthorized software, including a prohibition of obtaining data and software from external networks. User awareness and training on these policies and methods shall be provided for all users on a regular basis.
Level 1 Control Standard Mapping:	• COBIT 4.1 DS5.9 • COBIT 5 DSS05.01 • CSA IS-21 • HIPAA § 164.308(a)(5)(ii)(B) • ISO 27799-2008 7.7.4.1 • NIST Cybersecurity Framework DE.CM-4 • NRS 603A.215.1 • PCI DSS v3 5.1 • PCI DSS v3 5.1.1 • PCI DSS v3 5.2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• (State of Mass.) 201 CMR 17.04(7) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Critical system file scans are performed during system boot and every 12 hours. Malicious code is blocked and quarantined and an alert sent to administrators in response to malicious code detection. The organization shall address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Malicious code protection mechanisms shall be centrally managed. For systems considered to be not commonly affected by malicious software, the organization shall perform periodic assessments to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software. The organization shall: i. employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; ii. implement spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages transported by email, email attachments, Web accesses, or other common means; iii. automatically update malicious code and spam protection mechanisms (including signature definitions) when new releases are available in accordance with the organization's configuration management policy and procedures; iv. configure malicious code protection mechanisms to perform periodic scans of the information system according to organization guidelines

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	and real-time scans of files from external sources at either endpoints or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and block malicious code, quarantine malicious code, or send alerts to administrator in response to malicious code detection; and v. addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. Malicious code and spam protection mechanisms shall be centrally managed. User functionality (including user interface services [e.g., web services]) shall be separated from information system management (e.g., database management systems) functionality. The information system must implement safeguards to protect its memory from unauthorized code execution.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CM-11 (HIGH) • CMSRs 2013v2 SC-2 (HIGH) • CMSRs 2013v2 SI-3 (HIGH) • CMSRs 2013v2 SI-3(1) (HIGH) • CMSRs 2013v2 SI-3(2) (HIGH) • CMSRs 2013v2 SI-8 (HIGH) • CMSRs 2013v2 SI-8(1) (HIGH) • CMSRs 2013v2 SI-8(2) (HIGH) • IRS Pub 1075 v2014 9.3.5.11 • IRS Pub 1075 v2014 9.3.16.2 • IRS Pub 1075 v2014 9.3.17.3 • IRS Pub 1075 v2014 9.3.17.6 • IRS Pub 1075 v2014 9.3.17.10 • IRS Pub 1075 v2014 9.4.3 • IRS Pub 1075 v2014 9.4.13 • ISO/IEC 27002-2005 10.4.1 • ISO/IEC 27002-2013 A.12.2.1 • MARS-E v1 SA-7 • MARS-E v1 SC-2 • MARS-E v1 SI-3 • MARS-E v1 SI-3(1) • MARS-E v1 SI-3(2) • MARS-E v1 SI-3(3) • MARS-E v1 SI-8 • MARS-E v1 SI-8(1) • NIST SP 800-53 R4 CM-11 • NIST SP 800-53 R4 SC-2 • NIST SP 800-53 R4 SI-3 • NIST SP 800-53 R4 SI-3(1)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST SP 800-53 R4 SI-3(2) • NIST SP 800-53 R4 SI-8 • NIST SP 800-53 R4 SI-8(1) • NIST SP 800-53 R4 SI-8(2) • NIST SP 800-53 R4 SI-16 • PCI DSS v3 5.1.2 • PCI DSS v3 5.3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	Desktop malicious code scanning software is configured to perform critical system file scans every twelve (12) hours.

FTI Requirements

FTI Custodians:	The agency must: i. Establish policies governing the installation of software by users; ii. Enforce software installation policies through automated methods; and iii. Monitor policy compliance on a continual basis. Implement malware protection at one or more points within the email delivery process to protect against viruses, worms, and other forms of malware. The agency must configure virtualized desktops to provide the functionalities only required for operations—non-essential functionality or components must be removed or prohibited.

Health Insurance Exchange Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Health Insurance Exchanges:	Desktop malicious code scanning software is configured to perform critical system file scans every twenty-four (24) hours.

Control Reference: 09.k Controls Against Mobile Code

Control Specification:	Mobile code shall be authorized before its installation and use, and the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy. All unauthorized mobile code shall be prevented from executing.
Factor Type:	Organizational
Topics:	Authorization Cryptography Policies and Procedures Viruses and Malware

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Automated controls (e.g., browser settings) shall be in place to authorize and restrict the use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, and Flash animations). A formal policy shall be in place for mobile code protection and to ensure protective measures including anti-virus and anti-spyware are in place and regularly updated.
Level 1 Control Standard Mapping:	• CSA SA-15 • HIPAA § 164.308(a)(5)(ii)(B) • NIST Cybersecurity Framework DE.CM-5 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall formally address controls (e.g., policies and procedures) for blocking any use and receipt (e.g., downloading and execution) of mobile code s. The following actions shall be carried out to protect against mobile code performing unauthorized actions: i. ensuring a logically isolated environment is established for executing mobile code; ii. activating technical measures as available on a specific system to ensure mobile code is managed; and iii. control the resources with access to mobile code. Rules for the migration of software from development to operational status shall be defined and documented by the organization hosting the affected application(s), including that development, test, and operational systems be separated (physically or virtually) to reduce the risks of unauthorized access or changes to the operational system.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 SC-2 (HIGH) • CMSRs 2013v2 SC-3 (HIGH) • CMSRs 2013v2 SC-3(1) (HIGH) • CMSRs 2013v2 SC-3(2) (HIGH) • CMSRs 2013v2 SC-3(3) (HIGH) • CMSRs 2013v2 SC-3(4) (HIGH) • CMSRs 2013v2 SC-3(5) (HIGH) • CMSRs 2013v2 SC-18 (HIGH) • IRS Pub 1075 v2014 9.3.16.2 • IRS Pub 1075 v2014 9.3.16.12 • ISO/IEC 27002-2005 10.4.2 • ISO/IEC 27002-2013 A.12.2.1 • ISO 27799-2008 7.7.4.2 • MARS-E v1 SC-2 • MARS-E v1 SC-18 • NIST SP 800-53 R4 SC-2 • NIST SP 800-53 R4 SC-3 • NIST SP 800-53 R4 SC-18

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The information system shall implement underlying hardware separation mechanisms to facilitate security function isolation. Security functions enforcing access and information flow control shall be isolated from both non-security functions and from other security functions. An information system isolation boundary shall be implemented to minimize the number of non-security functions included within the boundary containing security functions. Security functions shall be implemented as largely independent modules that avoid unnecessary interactions between modules. Security functions shall be implemented as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

Objective Name: 09.05 Information Back-Up

Control Objective:	Ensure the maintenance, integrity, and availability of organizational information.

Control Reference: 09.l Back-up

Control Specification:	Back-up copies of information and software shall be taken and tested regularly.
Factor Type:	Organizational

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Topics:	Cryptography Documentation and Records Physical and Facility Security Policies and Procedures Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to Joint Commission Accreditation
Level 1 Implementation:	Back-up copies of information and software shall be made, and tested at appropriate intervals, in accordance with an agreed-upon back-up policy. A formal definition of the level of back-up required for each system shall be defined and documented including the scope of data to be imaged, frequency of imaging, and duration of retention. This shall be based on the contractual, legal, regulatory and business requirements. Complete restoration procedures shall be defined and documented for each system. The back-ups shall be stored in a physically secure remote location, at a sufficient distance to make them reasonably immune from damage to data at the primary site. Physical and environmental controls shall be in place for the back-up copies. Regular testing of back-up media and restoration procedures shall be performed. Inventory records for the back-up copies, including content and current location shall be maintained. When the back-up service is delivered by the third party, the service level agreement shall include the detailed protections to control confidentiality, integrity, and availability of the back-up information.
Level 1 Control Standard Mapping:	• CSA DG-04 • HIPAA § 164.308(a)(7)(ii)(A) • HIPAA § 164.308(a)(7)(ii)(B) • HIPAA § 164.310(d)(2)(iv) • HIPAA § 164.312(c)(1) • JCAHO IM.01.01.03, EP 4 • NIST Cybersecurity Framework PR.IP-4

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST SP 800-53 R4 CP-9 • NRS 603A.215.1 • PCI DSS v3 9.5.1 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: Automated tools shall track all back-ups. The integrity and security of the back-up copies shall be maintained to ensure future availability in accordance with the agreed backup policy. Any potential accessibility problems with the back-up copies shall be identified and mitigated in the event of an area-wide disaster. Covered information shall be backed-up in an encrypted format to guarantee confidentiality.
Level 2 Control Standard Mapping:	• ISO/IEC 27002-2005 10.5.1 • ISO/IEC 27002-2013 A.12.3.1 • ISO 27799-2008 7.7.5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Pharmaceutical Companies: > 70,000,000 Prescriptions Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: The organization shall perform full backups weekly to separate media. Incremental or differential backups shall be performed daily to separate media. Three (3) generations of backups (full plus all related incremental or differential backups) shall be stored off-site. Off-site and on-site backups shall be logged with name, date, time and action. The organization shall ensure a current, retrievable copy of covered information is available before movement of servers. The organization shall test backup information following each backup to verify media reliability and information integrity.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 CP-9 (HIGH) • CMSRs 2013v2 CP-9(1) (HIGH) • CMSRs 2013v2 CP-9(3) (HIGH) • CMSRs 2013v2 CP-9(5) (HIGH) • IRS Pub 1075 v2014 4.2 • IRS Pub 1075 v2014 4.4 • IRS Pub 1075 v2014 4.5 • IRS Pub 1075 v2014 9.3.6.7 • IRS Pub 1075 v2014 9.3.10.3 • IRS Pub 1075 v2014 9.4.11 • IRS Pub 1075 v2014 9.4.14 • IRS Pub 1075 v2014 9.4.18 • MARS-E v1 CP-9 • MARS-E v1 CP-9(1) • NIST SP 800-53 R4 CP-9(1)

CMS Requirements

CMS Contractors:	Backups shall include: i. copies of user-level and system-level information (including system state information); ii. copies of the operating system and other critical information system software; and iii. the information system inventory (including hardware, software, and firmware components).

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization transfers information system backup information to the alternate storage site at defined time periods (defined in the applicable security plan) and transfer rates (defined in the applicable security plan) consistent with the recovery time and recovery point objectives.

FTI Requirements

FTI Custodians:	Back-up tapes must be labeled as containing FTI, must be logged, must be transported securely using two barriers and a transmittal, and must be inventoried on a semi-annual basis. The organization protects the confidentiality of backup information at storage locations pursuant to IRC 6013. Backups (virtual machine snapshot) must be properly secured and must be stored in a logical location where the backup is only accessible to those with a need-to-know.

Objective Name: 09.06 Network Security Management

Control Objective:	Ensure the protection of information in networks and protection of the supporting network infrastructure.

Control Reference: 09.m Network Controls

Control Specification:	Networks shall be managed and controlled in order to protect the organization from threats and to maintain security for the systems and applications using the network, including information in transit. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Authentication Communications and Transmissions Cryptography Data Loss Prevention Monitoring Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Network managers shall implement controls to ensure the security of information in networks, and the protection of connected services from unauthorized access. Controls shall be implemented to ensure the availability of network services and information services using the network. Responsibilities and procedures shall be established for the management of equipment on the network, including equipment in user areas. When configuring wireless access points and devices, the organization shall change the following: i. vendor default encryption keys. ii. encryption keys anytime anyone with knowledge of the keys leaves the company or changes positions iii. default SNMP community strings on wireless devices iv. default passwords/passphrases on access points v. other security-related wireless vendor defaults, if applicable. A current network diagram (for example, one that shows how covered information flows over the network) shall exist, documenting all connections to systems storing, processing or transmitting covered information, including any wireless networks. Review and update the network diagram as based on the changes in the environment and no less than every 6 months. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols can be continued targets of malicious individuals who exploit these vulnerabilities to gain privileged access to covered information environments. The organization monitors for all authorized and unauthorized wireless access to the information system and prohibits installation of wireless access points (WAP) unless explicitly authorized, in writing, by the CIO or his/her designated representative. If wireless access is explicitly approved, wireless access points and devices shall have appropriate (e.g., FIPS-approved) encryption enabled for authentication and transmission. WAPs shall be placed in secure areas.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-18 (HIGH) • CSA SA-10 • HIPAA § 164.312(a)(2)(i) • HIPAA § 164.312(c)(1) • HIPAA § 164.312(c)(2) • HIPAA § 164.312(d) • HIPAA § 164.312(e)(1)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• HIPAA § 164.312(e)(2)(i) • HIPAA § 164.312(e)(2)(ii) • IRS Pub 1075 v2014 9.3.1.13 • MARS-E v1 AC-18 • NIST Cybersecurity Framework ID.AM-3 • NIST Cybersecurity Framework PR.DS-5 • NIST Cybersecurity Framework DE.AE-1 • NIST Cybersecurity Framework DE.CM-1 • NIST SP 800-53 R4 AC-18 • PCI DSS v3 1.1 • PCI DSS v3 1.1.2 • PCI DSS v3 1.1.3 • PCI DSS v3 1.1.4 • PCI DSS v3 1.1.5 • PCI DSS v3 2.1.1 • PCI DSS v3 4.1.1 • PCI DSS v3 11.1 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: The organization shall uniquely identify and authenticate network devices that require authentication mechanisms before establishing a connection that, at a minimum, use shared information (i.e., MAC or IP address) and access control lists to control remote network access. To identify and authenticate devices on local and/or wide area networks, the information system shall use either:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

i. shared known information solutions (Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses); or
ii. an organizational authentication solution (IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication).

The required strength of the device authentication mechanism shall be determined by the security categorization of the information system.
A formal process shall be established for approving and testing all network connections and changes to the firewall and router configurations. The organization shall build a firewall configuration that restricts connections between un-trusted networks and any system components in the covered information environment (Note: An "un-trusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.) Any changes to the firewall configuration shall be updated in the network diagram.

The firewall configuration shall:
i. restrict inbound and outbound traffic to that which is necessary for the covered information systems environment;
ii. secure and synchronize router configuration files;
iii. require firewalls between any wireless networks and the covered information systems environment; and
iv. configure these firewalls to deny or control any traffic from a wireless environment into the covered data environment.

The organization shall ensure information systems protect the confidentiality and integrity of transmitted information, including during preparation for transmission and during reception. The organization requires information systems to use FIPS-validated cryptographic mechanisms during transmission to prevent unauthorized disclosure of information and detect changes to information unless otherwise protected by organization-defined alternative physical measures.

Usage restrictions and implementation guidance shall be defined and documented for VoIP, including the authorization and monitoring of the service.

Perform quarterly scans for unauthorized wireless access points and take appropriate action if any access points are discovered.

The organization shall:
i. authorize connections from the information system to other information systems outside of the organization through the use of interconnection security agreements or other formal agreement; and
ii. document for each connection, the interface characteristics, security requirements, and the nature of the information communicated, and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	iii. employ a deny all, permit by exception policy for allowing connections from the information system to other information systems outside of the organization.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 IA-3 (HIGH) • CMSRs 2013v2 SC-7 (HIGH) • CMSRs 2013v2 SC-8 (HIGH) • CMSRs 2013v2 SC-8(1) (HIGH) • CMSRs 2013v2 SC-8(2) (HIGH) • CMSRs 2013v2 SC-19 (HIGH) • CMSRs 2013v2 SC-20 (HIGH) • CSA SA-08 • IRS Pub 1075 v2014 9.3.7.3 • IRS Pub 1075 v2014 9.3.16.5 • IRS Pub 1075 v2014 9.3.16.6 • IRS Pub 1075 v2014 9.3.16.13 • IRS Pub 1075 v2014 9.4.15 • MARS-E v1 IA-3 • MARS-E v1 SC-7 • MARS-E v1 SC-8 • MARS-E v1 SC-8(1) • MARS-E v1 SC-9 • MARS-E v1 SC-9(1) • MARS-E v1 SC-19 • MARS-E v1 SC-20 • MARS-E v1 SC-20(1) • NIST Cybersecurity Framework PR.AC-1 • NIST Cybersecurity Framework PR.AC-5 • NIST Cybersecurity Framework PR.DS-2 • NIST SP 800-53 R4 IA-3 • NIST SP 800-53 R4 SC-7 • NIST SP 800-53 R4 SC-8 • NIST SP 800-53 R4 SC-8(1) • NIST SP 800-53 R4 SC-8(2) • NIST SP 800-53 R4 SC-19 • NIST SP 800-53 R4 SC-20 • PCI DSS v3 1.1.1 • PCI DSS v3 1.2 • PCI DSS v3 1.2.1 • PCI DSS v3 1.2.2 • PCI DSS v3 1.2.3 • Phase 1 CORE 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.1

Level 3 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: An analysis shall be conducted to determine the impact the loss of network service availability will have upon critical business functions. Technical controls shall be implemented to safeguard the confidentiality and integrity of covered information passing over the organization's network and to/from public networks. Technical tools and solutions shall be implemented and used to identify the vulnerabilities and mitigate the threats, including intrusion detection system (IDS), and vulnerability scanning. The organization shall employ tools and techniques, such as an IDS, to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system. These tools shall be implemented at the perimeter of the organization's environment and at key points within the environment, including IDS deployed on the wireless side of the firewall. These tools shall be updated on a regular basis, including the engines, the baselines and signatures. Management processes shall be implemented to ensure coordination of and consistency in the elements of the network infrastructure. The organization shall establish firewall and router configuration standards for the current network with all connections to covered information, including any wireless networks. A description shall be documented of groups, roles, and responsibilities for the logical management of network components. Documentation and business justification shall be provided for the use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. The firewall and router rule sets shall be reviewed at least every six months. Wireless access points shall be shut down when not in use (e.g., nights, weekends). MAC address authentication and static IP addresses shall be utilized. Access points shall be placed in secure areas. File sharing shall

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	be disabled on all wireless clients. The organization shall build a firewall configuration to restrict inbound and outbound traffic to that which is necessary for the covered data environment (e.g., information flooding types of denial of service attacks). The router configuration files shall be secured and synchronized. Access to all proxies shall be denied, except for those hosts, ports, and services that are explicitly required. The organization shall utilize firewalls from at least two (2) different vendors at the various levels within the network to reduce the possibility of compromising the entire network. The organization shall prohibit direct public access between the Internet and any system component in the covered data environment. This shall be achieved by performing the following: i. establishing DMZ to limit inbound and outbound traffic to only protocols that are necessary for the covered data environment; ii. limiting inbound Internet traffic to IP addresses within the DMZ; iii. not allowing any direct routes inbound or outbound for traffic between the Internet and the covered data environment; iv. not allowing internal addresses to pass from the Internet into the DMZ; v. restricting outbound traffic from the covered data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ; vi. implementing stateful inspection, also known as dynamic packet filtering (that is, only "established" connections are allowed into the network); vii. placing all database(s), servers and other system components storing or processing covered information in an internal network zone, segregated from the DMZ; and viii. methods including but not limited to Network Address Translation (NAT), placing system components behind a proxy server, and/or removing or filtering route advertisements. To eliminate single points of failure and to enhance redundancy, there shall be at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. These servers shall be located on different subnets and geographically separated. Authoritative DNS servers shall be segregated into internal and external roles. The DNS server with the internal role shall provide name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role shall only provide name/address resolution information pertaining to external information technology resources.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 AC-18(1) (HIGH) • CMSRs 2013v2 AC-18(4) (HIGH) • CMSRs 2013v2 AC-18(5) (HIGH)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• CMSRs 2012v1.5 SC-7(18) (HIGH) • CMSRs 2013v2 SC-21 (HIGH) • CMSRs 2013v2 SC-22 (HIGH) • COBIT 4.1 DS5.10 • COBIT 5 DSS05.02 • IRS Pub 1075 v2014 9.3.1.13 • IRS Pub 1075 v2014 9.4.2 (E.10) • IRS Pub 1075 v2014 9.4.10 • IRS Pub 1075 v2014 9.4.11 • IRS Pub 1075 v2014 9.4.14 • IRS Pub 1075 v2014 9.4.17 • ISO/IEC 27002-2005 10.6.1 • ISO/IEC 27002-2005 12.5.4 • ISO/IEC 27002-2013 A.13.1.1 • MARS-E v1 AC-18(1) • MARS-E v1 SC-7(6) • MARS-E v1 SC-22 • NIST SP 800-53 R4 AC-18(1) • NIST SP 800-53 R4 SC-21 • NIST SP 800-53 R4 SC-22 • NRS 603A.215.1 • PCI DSS v3 1.1.6 • PCI DSS v3 1.1.7 • PCI DSS v3 1.3 • PCI DSS v3 1.3.1 • PCI DSS v3 1.3.2 • PCI DSS v3 1.3.3 • PCI DSS v3 1.3.4 • PCI DSS v3 1.3.5 • PCI DSS v3 1.3.6 • PCI DSS v3 1.3.7 • PCI DSS v3 1.3.8 • PCI DSS v3 11.4

CMS Contractor Requirements

CMS Contractors:	The information system shall fail securely in the event of an operational failure of a boundary protection device. The organization identifies and explicitly authorizes users allowed to independently configure wireless networking capabilities. The organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization shall prohibit the use of Voice over Internet Protocol (VoIP) technologies, unless explicitly authorized, in writing, by the CMS CIO or his/her designated representative. If VoIP is authorized, the organization shall ensure VoIP equipment used to transmit or discuss sensitive information is protected with FIPS 140-2 encryption standards.

Federal Requirements

Federal Agencies and Contractors:	The information system shall provide: i. additional data origin integrity artifacts (e.g., digital signatures, cryptographic keys) along with authoritative data (e.g., DNS resource records) in response queries to obtain origin authentication and integrity verification assurances; and ii. the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. The information system requests and performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. A resolving or caching domain name system (DNS) server and authoritative DNS servers are examples of systems that perform this function.

FTI Requirements

FTI Custodians:	Intrusion-detection software shall be installed and maintained to monitor networks for any unauthorized attempt to access tax data in a data warehousing environment. The agency shall identify and analyze how FTI in a data warehouse is used and how FTI is queried or targeted by end users. Parts of the system containing FTI shall be mapped to follow the flow of the query from a client through the authentication server to the release of the query from the database server. To use a VoIP network that provides FTI to a customer, VoIP phones must be logically protected. FTI must be encrypted while in transit within a SAN environment. SAN management traffic must also be encrypted for SAN components. To use a virtual environment that receives, processes, stores, or transmits FTI, FTI data transmitted via hypervisor management communication systems on untrusted networks must be encrypted using FIPS-approved methods provided by either the virtualization solution or third-party solution, such as a VPN that encapsulates the management traffic.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	To use a VoIP network that provides FTI to a customer, the VoIP traffic must be encrypted using a NIST-approved method operating in a NIST-approved mode when FTI is in transit across the network (either Internet or state agency's network). To access FTI from a Web browser, the agency must encrypt FTI transmissions within the agency's internal network using a cryptographic module that is FIPS 140-2 validated.

PCI-DSS Requirements

PCI Data:	The organization shall ensure network diagrams identify all cardholder data connections and data flows. Using intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network, monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.

Control Reference: 09.n Security of Network Services

Control Specification:	Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Documentation and Records Monitoring Requirements (Legal and Contractual) Services and Acquisitions Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 Implementation:	The ability of the network service provider to manage agreed services in a secure way shall be determined and regularly monitored, and the right to audit shall be agreed by management. The security arrangements necessary for particular services including security features, service levels, and management requirements, shall be identified and documented.
Level 1 Control Standard Mapping:	• CSA IS-31 • HIPAA § 164.308(b)(1) • HIPAA § 164.308(b)(3) • HIPAA § 164.314(a)(1) • HIPAA § 164.314(a)(2)(ii) • ISO/IEC 27002-2005 10.6.2 • ISO/IEC 27002-2013 A.13.1.2 • ISO 27799-2008 7.7.6.2 • NIST Cybersecurity Framework ID.AM-6 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance; Requirements (High)Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall: i. authorize connections from the information system to other information systems outside of the organization through the use of interconnection security agreements or other formal agreement; ii. centrally document for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and iii. reviews and updates the interconnection security agreements on an ongoing basis verifying enforcement of security requirements.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization employs, and documents in a formal agreement or other document (e.g., an applicable security plan), either i) allow-all, deny-by-exception, or, ii) deny-all, permit-by-exception (preferred), policy for allowing specific information systems (defined in the applicable agreement, security plan, etc.) to connect to external information systems. The organization requires external/outsourced service providers to identify the specific functions, ports, and protocols used in the provision of such external/outsourced services. The contract with the external/outsourced service provider shall include the specification that the service provider is responsible for the protection of covered information shared in the contract.
Level 2 Control Standard Mapping:	• 16 CFR Part §681.1 (e)(4) • CMSRs 2013v2 CA-3 (HIGH) • CMSRs 2013v2 CA-3(5) (HIGH) • CMSRs 2013v2 SA-9 (HIGH) • CMSRs 2013v2 SA-9(2) (HIGH) • IRS Pub 1075 v2014 9.3.4.3 • IRS Pub 1075 v2014 9.3.15.7 • MARS-E v1 CA-3 • MARS-E v1 SA-9 • NIST Cybersecurity Framework ID.AM-3 • NIST Cybersecurity Framework ID.AM-4 • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework DE.AE-1 • NIST Cybersecurity Framework PR.AT-3 • NIST Cybersecurity Framework PR.PT-4 • NIST Cybersecurity Framework DE.CM-6 • NIST Cybersecurity Framework DE.CM-7 • NIST SP 800-53 R4 CA-3 • NIST SP 800-53 R4 CA-3(5) • NIST SP 800-53 R4 SA-9 • NIST SP 800-53 R4 SA-9(2) • NIST SP 800-53 R4 SC-8(1)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Regulatory Factors:	
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization shall record each system interconnection in the security plan for the system that is connected to the remote location. The Interconnection Security Agreement or data sharing agreement is updated following significant changes to the system, organizations, or the nature of the electronic sharing of information that could impact the validity of the agreement.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The organization shall record each system interconnection in the System Security Plan (SSP) and Information Security (IS) Risk Assessment (RA) for the system that is connected to the remote location.

Objective Name: 09.07 Media Handling

Control Objective:	Prevent unauthorized disclosure, modification, removal or destruction of information assets, or interruptions to business activities

Control Reference: 09.o Management of Removable Media

Control Specification:	Formal procedures shall be documented and implemented for the management of removable media. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Authorization Cryptography Documentation and Records Media and Assets Physical and Facility Security Policies and Procedures

Level 1 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The organization shall formally establish and enforce controls (e.g., policies and procedures) for the management of removable media and laptops including: i. restrictions on the type(s) of media, and usages thereof to maintain security; ii. registration of certain type(s) of media including laptops. Media containing covered information shall be physically stored and its data encrypted in accordance with the organization's data protection and privacy policy on the use of cryptographic controls (see 06.d) until the media are destroyed or sanitized (see 09.p) and commensurate with the confidentiality and integrity requirements for its data classification level.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 MP-1 (HIGH) • CMSRs 2013v2 MP-4 (HIGH) • CSA IS-32 • Guidance to render PHI unusable, unreadable, or indecipherable (1)(i) • HIPAA § 164.310(c) • HIPAA § 164.310(d)(1) • HIPAA § 164.310(d)(2)(iii) • HIPAA § 164.310(d)(2)(iv) • HIPAA § 164.312(c)(1) • IRS Pub 1075 v2014 9.3.10.1 • IRS Pub 1075 v2014 9.3.10.4 • ISO 27799-2008 7.7.7.1 • MARS-E v1 MP-1 • MARS-E v1 MP-4 • NIST Cybersecurity Framework PR.PT-2 • NIST SP 800-53 R4 MP-1 • NIST SP 800-53 R4 MP-4 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.03(2)(c) • (State of Mass.) 201 CMR 17.04(5) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to State of Massachusetts Data Protection Act, Subject to MARS-E Requirements
Level 2 Implementation:	Level 1 plus: Redundancy of storage shall be established in light of the risks to the removable media, including where storage retention requirements exceed the rated life of the media. Organizations shall identify digital and non-digital media requiring restricted use and the specific safeguards necessary to restrict use. The organization: i. protects and controls digital and non-digital media containing sensitive information during transport outside of controlled areas using cryptography and tamper evident packaging and a. if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or b. if shipped, trackable with receipt by commercial carrier; ii. maintains accountability for information system media during transport outside of controlled areas; iii. documents activities associated with the transport of information system media; and iv. restricts the activities associated with transport of such media to authorized personnel.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 MP-5 (HIGH) • CMSRs 2013v2 MP-5(3) (HIGH) • CMSRs 2013v2 MP-5(4) (HIGH) • CMSRs 2013v2 MP-7 (HIGH) • IRS Pub 1075 v2014 9.3.10.5 • ISO/IEC 27002-2005 10.7.1 • ISO/IEC 27002-2013 A.8.3.1 • MARS-E v1 MP-5 • MARS-E v1 MP-5(2) • MARS-E v1 MP-5(4) • NIST SP 800-53 R4 MP-5

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST SP 800-53 R4 MP-5(4) • NIST SP 800-53 R4 MP-7 • NRS 603A.215.1 • PCI DSS v3 9.6.3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Pharmaceutical Companies: > 70,000,000 Prescriptions Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: Organizations shall restrict the use of writable, removable media and personally-owned, removable media in organizational systems.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 MP-6(3) (HIGH) • CMSRs 2013v2 MP-7(1) (HIGH) • NIST SP 800-53 R4 MP-7(1)

CMS Requirements

CMS Contractors:	The organization physically controls and securely stores digital and non-digital media defined within NIST SP 800-88, Guidelines for Media Sanitization, within controlled areas using physical security safeguards prescribed for the highest system security level of the information ever recorded on it. The organization evaluates employing an approved method of cryptography (see SC-13) to protect PII at rest, consistent with NIST SP 800-66 guidance and, if PII is recorded on magnetic media with other data, it should be protected as if it were entirely personally identifiable information. The organization employs an identified custodian through the transport of CMS information system media. Portable, removable storage devices shall be sanitized prior to connecting

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	such devices to the information system under the following circumstances: i. initial use after purchase; ii. when obtained from an unknown source; iii. when the organization loses a positive chain of custody; and iv. when the device was connected to a lower assurance system based on its security categorization (e.g., a publically accessible kiosk).

Control Reference: 09.p Disposal of Media

Control Specification:	Media shall be disposed of securely and safely when no longer required, using formal procedures that are documented. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Media and Assets Policies and Procedures Services and Acquisitions Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to Joint Commission Accreditation
Level 1 Implementation:	The organization shall destroy media when it is no longer needed for business or legal reasons. Formal procedures for the secure disposal of media shall minimize the risk of information leakage to unauthorized persons. The procedures for the secure disposal of media containing information shall be commensurate with the sensitivity of that information. The following items shall be addressed: i. the use of generally-accepted secure disposal or erasure methods (see 08.l) for use by another application within the organization, for media that contains (or might contain) covered information; and ii. the identification of information that qualifies as covered, or a policy shall be developed that all information shall be considered covered in the absence of unequivocal evidence to the contrary. It may be easier to arrange for all media items to be collected and disposed

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	of securely, rather than attempting to separate out the items containing covered information. If collection and disposal services offered by other organizations are used, care shall be taken in selecting a suitable contractor with adequate controls and experience.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 MP-6 (HIGH) • CSA DG-05 • Guidance to render PHI unusable, unreadable, or indecipherable (2)(i) • Guidance to render PHI unusable, unreadable, or indecipeherable (2)(i) • HIPAA § 164.310(d)(1) • HIPAA § 164.310(d)(2)(i) • HIPAA § 164.310(d)(2)(ii) • IRS Pub 1075 v2014 8.2 • IRS Pub 1075 v2014 9.3.10.6 • IRS Pub 1075 v2014 9.4.2 (E.10) • IRS Pub 1075 v2014 9.4.9 • IRS Pub 1075 v2014 9.4.18 • ISO 27799-2008 7.7.7.2 • JCAHO IM.02.01.03, EP 3 • MARS-E v1 MP-6 • NIST Cybersecurity Framework PR.DS-3 • NIST Cybersecurity Framework PR.DS-5 • NIST Cybersecurity Framework PR.IP-6 • NIST SP 800-53 R4 MP-6 • NIST SP 800-53 R4 DM-2 • NRS 603A.215.1 • PCI DSS v3 9.8 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Implementation:	Level 1 plus: Procedures shall be implemented to prevent the aggregation effect, which may cause a large quantity of non-covered information to become covered for accumulating media for disposal.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 MP-6(1) (HIGH) • CMSRs 2013v2 MP-6(2) (HIGH) • IRS Pub 1075 v2014 9.4.7 • ISO/IEC 27002-2005 10.7.2 • ISO/IEC 27002-2013 A.8.3.2 • MARS-E v1 MP-6(5) • MARS-E v1 MP-6(6)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contactor Requirements

CMS Contractors:	The organization reviews, approves, tracks, documents (logs), and verifies media sanitization and disposal actions. The organization tests sanitization equipment and procedures within every three hundred and sixty-five (365) days to verify that the intended sanitization is being achieved.

FTI Requirements

FTI Custodians:	The agency shall cleanse FTI at the staging area of a data warehouse and document how it cleanses the FTI when it is extracted, transformed, and loaded (i.e., in the ETL process). In addition, the agency shall describe the process of object reuse once FTI is replaced from data sets. All FTI must be removed from media in the data warehouse by a random overwrite software program.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	If the media will be reused by the agency for the same purpose of storing FTI and will not be leaving organization control, then clearing is a sufficient method of sanitization. If the media will be reused and repurposed for a non-FTI function or will be leaving organization control (i.e., media being exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the agency), then purging should be selected as the sanitization method. If the media will not be reused at all, then destroying is the method for media sanitization. The following media sanitization requirements are applicable for media used in a "pre-production" or "test" environments. i. The technique for clearing, purging, and destroying media depends on the type of media being sanitized. ii. A representative sampling of media must be tested after sanitization has been completed. iii. Media sanitization should be witnessed or verified by an agency employee. Disposal of all Multifunction Device (MFD) hardware (e.g., hard disks) and WLAN components follows the organization's standard media sanitization and disposal procedure requirements. FTI furnished to the user and any paper material generated therefrom, such as extra copies, photo impressions, computer printouts, carbon paper, notes, stenographic notes, and work papers must be destroyed by burning, mulching, pulping, shredding, or disintegrating. FTI must never be disclosed to an agency's agents or contractors during disposal unless authorized by the Internal Revenue Code. Agencies must review and approve media to be sanitized to ensure compliance with records-retention policies. Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken. Agencies verify that the sanitization of the media was effective prior to disposal.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The organization reviews, approves, tracks, documents (logs), and verifies media sanitization and disposal actions. The organization tests sanitization equipment and procedures within every three hundred and sixty-five (365) days to verify that the intended

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	sanitization is being achieved. Electronic media containing FTI must not be made available for reuse by other offices or released for destruction without first being subject to electromagnetic erasing. If reuse is not intended, the electronic media should be destroyed. Whenever physical media leaves the physical or systemic control of the agency for maintenance, exchange or other servicing, any FTI on it must be cleared completely by overwriting all data tracks a minimum of three times. Paper FTI may be burned, cross-cut shredded to 5/16" wide or small strips or pulped.

Control Reference: 09.q Information Handling Procedures

Control Specification:	Procedures for the handling and storage of information shall be established to protect this information from unauthorized disclosure or misuse. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Cryptography Data Loss Prevention Documentation and Records Media and Assets Monitoring User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to State of Massachusetts Data Protection Act, Subject to FTI Requirements
Level 1 Implementation:	Procedures for handling, processing, communication and storage of information (including information media awaiting disposal) shall be established to protect data from unauthorized disclosure or misuse including: i. physical and technical access restrictions commensurate with the data classification level; ii. handling and labeling of all media according to its indicated classification (sensitivity) level; iii. periodic review (at a minimum annually) of distribution and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	authorized recipient lists; and iv. monitoring the status and location of media containing unencrypted covered information.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 MP-2 (HIGH) • CMSRs 2013v2 SI-12 (HIGH) • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.310(b) • HIPAA § 164.310(c) • HIPAA § 164.310(d)(1) • HIPAA § 164.312(c)(1) • IRS Pub 1075 v2014 9.3.10.2 • IRS Pub 1075 v2014 9.3.10.3 • IRS Pub 1075 v2014 9.3.17.9 • ISO 27799-2008 7.7.7.3 • MARS-E v1 MP-2 • MARS-E v1 SI-12 • NIST Cybersecurity Framework PR.DS-3 • NIST Cybersecurity Framework PR.PT-2 • NIST SP 800-53 R4 MP-2 • NIST SP 800-53 R4 SI-12 • PCI DSS v3 9.5 • (State of Mass.) 201 CMR 17.03(2)(c) • (State of Mass.) 201 CMR 17.03(2)(g) • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(4)(A)(ii)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: The organization shall maintain inventories of media to maintain strict control over storage and accessibility. Management shall approve any and all media that is moved from a secured area, especially when media is

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	distributed to individuals. Maintenance of formal records of data transfers, including logging and an audit trail shall be maintained.
Level 2 Control Standard Mapping:	• IRS Pub 1075 v2014 4.5 • IRS Pub 1075 v2014 9.3.10.2 • ISO/IEC 27002-2005 10.7.3 • ISO/IEC 27002-2013 A.8.2.3 • NRS 603A.215.1 • PCI DSS v3 3.2 • PCI DSS v3 3.2.1 • PCI DSS v3 3.2.2 • PCI DSS v3 3.2.3 • PCI DSS v3 3.3 • PCI DSS v3 9.6 • PCI DSS v3 9.6.3 • PCI DSS v3 9.7

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Pharmaceutical Companies: > 70,000,000 Prescriptions Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements
Level 3 Implementation:	Level 2 plus: Inventory and disposition records for information system media shall be maintained to ensure control and accountability of the organization's information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach. The media records shall, at a minimum, contain: i. the name of media recipient; ii. the signature of media recipient; iii. the date/time media received; iv. the media control number and contents; v. the movement or routing information; and vi. if disposed of, the date, time, and method of destruction.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The information system implements cryptographic mechanisms to protect the confidentiality and integrity of sensitive (non-public) information stored on digital media during transport outside of controlled areas.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 MP-CMS-1 (HIGH) • MARS-E v1 MP-CMS-1

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted. Inventory and disposition records for information system media shall be maintained to ensure control and accountability of CMS information. The media related records shall contain sufficient information to reconstruct the data in the event of a breach.

PCI-DSS Requirements

PCI Data:	The system shall not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, the system shall render all data unrecoverable upon completion of the authorization process. The system shall not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data. The system shall not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-no-present transactions. The system shall not store the personal identification number (PIN) or the encrypted PIN block. The system shall mask the PAN when displaced (the first six and last our digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN. (Note this requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 09.r Security of System Documentation

Control Specification:	System documentation shall be protected against unauthorized access.
Factor Type:	Organizational
Topics:	Authorization Documentation and Records User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	The organization: i. Obtains administrator documentation for the information system, system component, or information system service that describes: a. Secure configuration, installation, and operation of the system, component, or service; b. Effective use and maintenance of security functions/mechanisms; and c. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; ii. Obtains user documentation for the information system, system component, or information system service that describes: a. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; b. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and c. User responsibilities in maintaining the security of the system, component, or service. Organizations shall document attempts to obtain information system documentation when such documentation is either unavailable or non-existent. The organization shall protect system documentation in accordance with the organization's risk management strategy, e.g., by access controls (see 1.0),

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	and distribute documentation to organization-defined personnel with the need for such documentation. The access list for system documentation shall be kept to a minimum and authorized by the application owner.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 SA-5 (HIGH) • CSA OP-02 • IRS Pub 1075 v2014 9.3.15.5 • ISO/IEC 27002-2005 10.7.4 • ISO 27799-2008 7.7.7.4 • MARS-E v1 SA-5 • NIST Cybersecurity Framework ID.RA-1 • NIST SP 800-53 R4 SA-5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Objective Name: 09.08 Exchange of Information

Control Objective:	Ensure the exchange of information within an organization and with any external entity is secured and protected, and carried out in compliance with

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	relevant legislation and exchange agreements.

Control Reference: 09.s Information Exchange Policies and Procedures

Control Specification:	Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication mediums. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Awareness and Training Communications and Transmissions Cryptography Personnel Policies and Procedures Third Parties and Contractors Viruses and Malware

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance
Level 1 Implementation:	The organization shall ensure that communications protection requirements, including the security of exchanges of information, is the subject of policy development (see also 04.a and 04.b) and compliance audits (see 06.g) consistent with relevant legislation. When using electronic communication applications or systems for information exchange, the following items shall be addressed: i. policies or guidelines shall be defined outlining acceptable use of electronic communication applications or systems; ii. the use of anti-malware for the detection of and protection against malicious code that may be transmitted through the use of electronic communications; iii. procedures shall be implemented for the use of wireless communications including an appropriate level of encryption (see 09.m); iv. employee, contractor and any other user's responsibilities shall be defined to not compromise the organization (e.g., through

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.);

v. the required use of cryptographic techniques to protect the confidentiality, integrity and authenticity of covered information;

vi. the retention and disposal guidelines shall be defined for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations; and

vii. controls and restrictions shall be implemented associated with the forwarding of communications (e.g., automatic forwarding of electronic mail to external mail addresses).

The organization shall establish terms and conditions, consistent with any trust relationship established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

i. access the information system from external information systems; and

ii. process, store or transit organization-controlled information using external information systems.

Personnel shall be appropriately educated and periodically reminded of the following:

i. not to leave covered or critical information on printing systems (e.g., copiers, printers, and facsimile machines) as these may be accessed by unauthorized personnel;

ii. that they should take necessary precautions, including not to reveal covered information to avoid being overheard or intercepted when making a phone call by:
    a. people in their immediate vicinity particularly when using mobile phones;
    b. wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers; or
    c. people at the recipient's end;

iii. not leaving messages containing sensitive information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialing;

iv. the problems of using facsimile machines, namely:
    a. unauthorized access to built-in message stores to retrieve messages;
    b. deliberate or accidental programming of machines to send messages to specific numbers; and
    c. sending documents and messages to the wrong number either by misdialing or using the wrong stored number;

v. not to register demographic data, such as the e-mail address or other personal information, in any software to avoid collection for unauthorized use; and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	vi. that modern facsimile machines and photocopiers have page caches and store pages in case of a paper or transmission fault, which will be printed once the fault is cleared. Cryptography shall be used to protect the confidentiality and integrity of remote access sessions to the internal network and to external systems. Formal procedures shall be defined to encrypt data in transit including use of strong cryptography protocols to safeguard covered information during transmission over open public networks. Valid encryption processes include: i. transport Layer Security (TLS) 1.0 ii. secure Sockets Layer (SSL) 3.1 iii. IPSec VPNs: a. gateway-To-Gateway Architecture b. host-To-Gateway Architecture c. host-To-Host Architecture iv. SSL VPNs: a. SSL Portal VPN b. SSL Tunnel VPN See NIST SP800-52 Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementation and NIST SP800-77 Guide to IPsec VPNs for more information on implementing encryption technologies for information transmissions. Examples of open, public network include: i. the Internet; ii. wireless technologies; iii. Global System for Mobile communications (GSM); and iv. General Packet Radio Service (GPRS).
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AC-17 (HIGH) • CMSRs 2013v2 AC-17(2) (HIGH) • CMSRs 2013v2 AC-20 (HIGH) • CMSRs 2013v2 SC-1 (HIGH) • CSA SA-03 • HIPAA § 164.310(b) • ISO/IEC 27002-2005 10.8.1 • IRS Pub 1075 v2014 4.7.3 • IRS Pub 1075 v2014 9.3.1.12 • IRS Pub 1075 v2014 9.3.1.15 • IRS Pub 1075 v2014 9.3.16.1 • ISO/IEC 27002-2013 A.13.2.1 • ISO 27799-2008 7.7.8.1 • JCAHO IM.02.01.03, EP 1 • MARS-E v1 AC-17

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• MARS-E v1 AC-20 • MARS-E v1 SC-1 • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework PR.AC-3 • NIST SP 800-53 R4 AC-17 • NIST SP 800-53 R4 AC-17(2) • NIST SP 800-53 R4 AC-20 • NIST SP 800-53 R4 SC-1 • PCI DSS v3 4.1 • PCI DSS v3 4.1.1 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to State of Massachusetts Data Protection Act, Subject to the State of Nevada Security of Personal Information Requirements, Subject to Joint Commission Accreditation, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall permit authorized individuals to use an external information system to access the information system or to process, store or transmit organization-controlled information only when then organization: i. verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or ii. retains approved information connection or processing agreements with the organizational entity hosting the external information system (see 09.t). The organization shall limit the use of organization-controlled portable storage media by authorized individuals on external information systems. Terms and conditions shall be established for authorized individuals to: i. to access the information system from an external information system shall be established; and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	ii. to process, store and/or transmit organization-controlled information using an external information system. The information system shall: i. prohibit remote activation of collaborative computing devices; and ii. provide an explicit indication of use to users physically present at the devices.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-20(1) (HIGH) • CMSRs 2013v2 AC-20(2) (HIGH) • CMSRs 2013v2 SC-15 (HIGH) • CMSRs 2013v2 SC-15(1) (HIGH) • COBIT 4.1 DS5.11 • COBIT 5 DSS05.02 • CSA IS-18 • Guidance to render PHI unusable, unreadable, or indecipherable (1)(ii) • IRS Pub 1075 v2014 9.3.16.10 • IRS Pub 1075 v2014 9.4.9 • JCAHO IM.02.01.03, EP 5 • NIST SP 800-53 R4 AC-20(1) • MARS-E v1 SC-15 • MARS-E v1 SC-15(1) • NIST SP 800-53 R4 AC-20(2) • NIST SP 800-53 R4 SC-15 • NRS 603A.215.1 • NRS 603A.215.2.a • Phase 1 CORE 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.1 • (State of Mass.) 201 CMR 17.04(3)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

CMS Contractors:	The organization shall prohibit the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process CMS sensitive information, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If external information systems are authorized, the organization shall establish strict terms and conditions for their use. The terms and conditions shall address, at a minimum: i. the types of applications that can be accessed from external information systems; ii. the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; iii. how other users of the external information system will be prevented from accessing federal information; iv. the use of virtual private networking (VPN) and firewall technologies; v. the use of and protection against the vulnerabilities of wireless technologies; vi. the maintenance of adequate physical security controls; vii. the use of virus and spyware protection software; and viii. how often the security capabilities of installed software are to be updated. The organization shall prohibit running collaborative computing mechanisms, unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the authorization shall specifically identify allowed mechanisms, allowed purpose, and the information system upon which the mechanisms can be used.

FTI Requirements

FTI Custodians:	Unless approved by the Office of Safeguards, the agency must prohibit: i. Access to FTI from external information systems; ii. Use of agency-controlled portable storage devices (e.g., flash drives, external hard drives) containing FTI on external information systems; and iii. Use of non-agency-owned information systems; system components; or devices to process, store, or transmit FTI. Any non-agency-owned information system usage requires the agency to notify the Office of Safeguards 45 days prior to implementation. All FTI data in transit to and from a Multifunctional Device (MFD) should be encrypted when moving across a WAN and within the LAN.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The organization prohibits the use of external information systems, including but not limited to, Internet kiosks, personal desktop computers, laptops, tablet personal computers, personal digital assistant (PDA) devices, cellular telephones, facsimile machines, and equipment available in hotels or airports to store, access, transmit, or process sensitive information (such as FTI or Privacy Act protected information), unless explicitly authorized, in writing, by the CIO or his/her designated representative. If authorized, the organization establishes strict terms and conditions for their use. The terms and conditions shall address, at a minimum: i. the types of applications that can be accessed from external information systems; ii. the maximum FIPS 199 security category of information that can be processed, stored, and transmitted; iii. how other users of the external information system will be prevented from accessing federal information; iv. the use of virtual private networking (VPN) and firewall technologies; v. the use of and protection against the vulnerabilities of wireless technologies; vi. the maintenance of adequate physical security controls; vii. the use of virus and spyware protection software; and viii. how often the security capabilities of installed software are to be updated.

Control Reference: 09.t Exchange Agreements

Control Specification:	Agreements shall be established and implemented for the exchange of information and software between the organization and external parties.
Factor Type:	Organizational
Topics:	Communications and Transmissions Data Loss Prevention IT Organization and Management Roles and Responsibilities Media and Assets Requirements (Legal and Contractual) Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 Regulatory Factors:	Subject to the State of Nevada Security of Personal Information Requirements
Level 1 Implementation:	Exchange agreements shall specify the minimum set of controls on responsibility, procedures, technical standards and solutions. The exchange agreements shall also specify organization policies including: i. classification policy for the sensitivity of the business information; ii. management responsibilities for controlling and notifying transmission, dispatch, and receipt; iii. procedures for notifying sender of transmission, dispatch, and receipt; iv. procedures to ensure traceability and non-repudiation; v. minimum technical standards for packaging and transmission; vi. courier identification standards; vii. responsibilities and liabilities in the event of information security incidents, such as loss of data; viii. use of an agreed labeling system for covered or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected; ix. ownership and responsibilities for data protection, copyright, software license compliance and similar considerations; x. technical standards for recording and reading information and software; xi. any special controls that may be required to protect covered items, including cryptographic keys; and xii. escrow agreements. Policies, procedures, and standards shall be established and maintained to protect information and physical media in transit, and shall be referenced in such exchange agreements.
Level 1 Control Standard Mapping:	• COBIT 4.1 DS5.11 • COBIT 5 DSS05.02 • CSA LG-02 • ISO/IEC 27002-2005 10.8.2 • ISO/IEC 27002-2013 A.13.2.2 • ISO 27799-2008 7.7.8.1 • NIST Cybersecurity Framework PR.AT-3 • NRS 603A.210.2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3

Level 2 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 09.u Physical Media in Transit

Control Specification:	Media containing information shall be protected against unauthorized access, misuse or corruption during transportation beyond the organization's physical boundaries.
Factor Type:	Organizational
Topics:	Communications and Transmissions Cryptography Media and Assets Policies and Procedures Services and Acquisitions

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 Regulatory Factors:	Subject to PCI Compliance
Level 1 Implementation:	The following procedures shall be established to protect information media being transported between sites: i. reliable transport or couriers shall be used that can be tracked; ii. a list of authorized couriers shall be agreed with management; iii. procedures to check the identification of couriers shall be developed; and iv. packaging shall be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications (e.g., for software) for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields. Controls shall be adopted to protect covered information from unauthorized disclosure or modification, including at least one of the following: i. use of locked containers; ii. delivery by hand; iii. tamper-evident packaging (which reveals any attempt to gain access); or iv. splitting of the consignment into more than one delivery and dispatch by different routes.
Level 1 Control Standard Mapping:	• CSA IS-32 • HIPAA § 164.310(d)(1) • HIPAA § 164.310(d)(2)(iii) • HIPAA § 164.312(c)(1) • ISO/IEC 27002-2005 10.8.3 • ISO/IEC 27002-2013 A.8.3.3 • ISO 27799-2008 7.7.8.2 • NIST Cybersecurity Framework PR.DS-2 • NIST Cybersecurity Framework PR.PT-2 • NRS 603A.215.1 • PCI DSS v3 9.6.2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: >

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the State of Nevada Security of Personal Information Requirements, Subject to Joint Commission Accreditation, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Media shall be encrypted when being moved off site. Media shall be encrypted on-site unless physical security can be guaranteed. The information system implements cryptographic mechanisms to protect the confidentiality and integrity of sensitive (non-public) information stored on digital media during transport outside of control areas.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 MP-5 (HIGH) • CMSRs 2013v2 MP-5(3) (HIGH) • CMSRs 2013v2 MP-5(4) (HIGH) • COBIT 4.1 DS5.11 • COBIT 5 DSS05.02 • IRS Pub 1075 v2014 4.3.1 • IRS Pub 1075 v2014 4.4 • IRS Pub 1075 v2014 9.3.10.6 • IRS Pub 1075 v2014 9.3.11.8 • JCAHO IM.02.01.03, EP 5 • MARS-E v1 MP-5 • MARS-E v1 MP-5(4) • MARS-E v1 PE-16 • NIST SP 800-53 R4 MP-5 • NIST SP 800-53 R4 MP-5(4) • NRS 603A.215.2.a

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization shall: i. protect and control digital and non-digital media containing CMS sensitive information during transport outside of controlled areas using cryptography and tamper-evident packaging and a. if hand carried, using securable container (e.g., locked briefcase) via authorized personnel, or b. if shipped, trackable with receipt by commercial carrier; ii. maintain accountability for information system media during transport outside of controlled areas; and iii. restrict the activities associated with transport of such media to authorized personnel. The organization shall employ an identified custodian throughout the transport of information system media outside of controlled areas. Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

FTI Requirements

FTI Custodians:	All transportation or shipments of FTI (including electronic media or microfilm) must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. All FTI transported through the mail or courier/messenger service must be double-sealed; that is one envelope within another envelope. The inner envelope should be marked confidential with some indication that only the designed official or delegate is authorized to open it.

Control Reference: 09.v Electronic Messaging

Control Specification:	Information involved in electronic messaging shall be appropriately protected.
Factor Type:	Organizational
Topics:	Authentication Authorization Communications and Transmissions

Level 1 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	Legal considerations, including requirements for electronic signatures, shall be addressed. Approval shall be obtained prior to using external public services, including instant messaging or file sharing. Stronger levels of authentication controlling access from publicly accessible networks shall be implemented. Stronger controls, such as electronic signatures, shall be implemented to protect certain electronic messages (e.g., clinical information). The electronic messages shall be protected throughout the duration of its end-to-end transport path. Cryptographic mechanisms shall be employed to protect message integrity and confidentiality unless protected by alternative measures, e.g., physical controls. The organization shall never send unencrypted sensitive information (e.g., covered information, PANs, FTI) by end-user messaging technologies (e.g., e-mail, instant messaging, and chat).
Level 1 Control Standard Mapping:	• CMSRs 2013v2 SC-8 (HIGH) • CMSRs 2013v2 SC-8(1) (HIGH) • CMSRs 2013v2 SC-8(2) (HIGH) • CMSRs 2013v2 SC-CMS-1 (HIGH) • COBIT 4.1 DS5.11 • COBIT 5 DSS05.02 • HIPAA § 164.312(c)(1) • HIPAA § 164.312(c)(2) • HIPAA § 164.312(e)(1) • HIPAA § 164.312(e)(2)(i) • HIPAA § 164.312(e)(2)(ii) • IRS Pub 1075 v2014 9.3.16.6 • IRS Pub 1075 v2014 9.4.3 • IRS Pub 1075 v2014 9.4.4 • ISO/IEC 27002-2005 10.8.4 • ISO/IEC 27002-2013 A.13.2.3 • ISO 27799-2008 7.7.8.3 • MARS-E v1 SC-8 • MARS-E v1 SC-8(1) • MARS-E v1 SC-9 • MARS-E v1 SC-9(1)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• MARS-E v1 SC-ACA-1 • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework PR.DS-2 • NIST Cybersecurity Framework PR.DS-5 • NIST SP 800-53 R4 SC-8 • NIST SP 800-53 R4 SC-8(1) • PCI DSS v3 4.2 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

FTI Requirements

FTI Custodians:	If FTI is allowed to be included within emails or email attachments, the agency must only transmit FTI to an authorized recipient. Encrypt email transmissions that contain FTI using a FIPS 140-2 validated mechanism.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	If FTI is allowed to be included within fax communications, the agency must only transmit FTI to an authorized recipient and must adhere to the following requirements: i. Have a trusted staff member at both the sending and receiving fax machines; and ii. ii. Accurately maintain broadcast lists and other preset numbers of frequent recipients of FTI.

Control Reference: 09.w Interconnected Business Information Systems

Control Specification:	Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.
Factor Type:	Organizational
Topics:	Communications and Transmissions Physical and Facility Security Policies and Procedures User Access Network Security

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Security and business implications shall be addressed for interconnecting business information assets including: i. policy and appropriate controls to manage information sharing; ii. excluding categories of sensitive business information and classified documents if the system does not provide an appropriate level of protection; iii. categories of personnel, contractors or business partners allowed to use the system and the locations from which it may be accessed; iv. restricting selected systems and facilities to specific categories of user; and v. identifying the status of users (e.g., employees of the organization or contractors in directories for the benefit of other users).
Level 1 Control Standard	• HIPAA § 164.308(b)(1) • HIPAA § 164.308(b)(3)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Mapping:	• HIPAA § 164.314(a)(2)(ii) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: The organization: i. Authorizes and approves connections of defined internal information system components or classes of components (defined in the applicable security plan) to the information system; and ii. Documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated along with their security and business implications. Security and business implications shall be addressed for interconnecting business information assets including: i. known vulnerabilities in the administrative and accounting systems where information is shared between different parts of the organization; ii. restricting access to diary information relating to selected individuals (e.g., personnel working on sensitive projects); and iii. vulnerabilities of information in business communication systems (e.g., recording phone calls or conference calls, confidentiality of calls, storage of facsimiles, opening mail, distribution of mail). Interconnected business information systems shall be linked to other requirements and controls, including: i. the separation of operational systems from interconnected system; ii. the retention and back-up of information held on the system; and iii. the fallback requirements and arrangements. A baseline shall be established for basic security hygiene in interconnected

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	systems. A firewall physical and logical configuration shall be established that restricts connections between untrusted networks and systems storing, processing or transmitting covered information.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CA-9 (HIGH) • COBIT 4.1 DS5.10 • COBIT 4.1 DS5.11 • COBIT 5 DSS05.02 • ISO/IEC 27002-2005 10.8.5 • ISO 27799-2008 7.7.8.4 • NIST Cybersecurity Framework PR.AC-5 • NIST Cybersecurity Framework PR.IP-1 • NIST Cybersecurity Framework DE.AE-1 • NIST SP 800-53 R4 CA-9 • NRS 603A.215.1 • PCI DSS v3 1.2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Objective Name: 09.09 Electronic Commerce Services

Control Objective:	Ensure the security of electronic commerce services, and their secure use.

Control Reference: 09.x Electronic Commerce Services

Control Specification:	Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure or modification.
Factor Type:	Organizational
Topics:	Authorization Cryptography Data Loss Prevention

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Requirements (Legal and Contractual) Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The confidentiality and integrity for electronic commerce shall be maintained by ensuring the following: i. the level of confidence each party requires in each other's claimed identity (e.g., through authentication); ii. authorization processes associated with who may set prices, issue or sign key trading documents; iii. ensuring that trading partners are fully informed of their authorizations; iv. determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents, and the non-repudiation of contracts (e.g., associated with tendering and contract processes); v. the level of trust required in the integrity of advertised price lists; vi. the confidentiality of any covered data or information; vii. the confidentiality and integrity of any order transactions, payment information, delivery address details, and confirmation of receipts; viii. the degree of verification appropriate to check payment information supplied by a customer; ix. selecting the most appropriate settlement form of payment to guard against fraud; x. the level of protection required to maintain the confidentiality and integrity of order information; xi. avoidance of loss or duplication of transaction information; xii. liability associated with any fraudulent transactions; and xiii. insurance requirements.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AU-10 (HIGH) • CSA IS-28 • HIPAA § 164.312(c)(1) • HIPAA § 164.312(c)(2) • HIPAA § 164.312(e)(1) • HIPAA § 164.312(e)(2)(i) • HIPAA § 164.312(e)(2)(ii)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• ISO 27799-2008 7.7.9.1 • MARS-E v1 AU-10 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: A documented agreement shall be committed and maintained for electronic commerce arrangements between trading partners on the agreed terms of trading, including details of authorization. Other agreements with information service and value added network providers shall also be required. Attacks of the host(s) used for electronic commerce shall be addressed to provide resilient service(s). The security implications of any network interconnection required for the implementation of electronic commerce services shall be identified and addressed. Cryptographic controls shall be used to enhance security, taking into account compliance with legal requirements.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 SC-8 (HIGH) • CMSRs 2013v2 SC-8(1) (HIGH) • CMSRs 2013v2 SC-8(2) (HIGH) • IRS Pub 1075 v2014 9.3.16.6 • ISO/IEC 27002-2005 10.9.1 • ISO/IEC 27002-2013 A.14.1.2 • MARS-E v1 SC-8 • MARS-E v1 SC-8(1) • MARS-E v1 SC-9 • MARS-E v1 SC-9(1) • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework PR.DS-1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST Cybersecurity Framework PR.DS-2 • NIST Cybersecurity Framework PR.DS-5 • NIST SP 800-53 R4 SC-8 • NIST SP 800-53 R4 SC-8(1)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The information system shall protect against an individual (or process acting on behalf of an individual) from falsely denying having performed a particular action.

Control Reference: 09.y On-Line Transactions

Control Specification:	Information involved in on-line transactions shall be protected to prevent incomplete transmission, miss-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.
Factor Type:	Organizational
Topics:	Authentication Communications and Transmissions Cryptography

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Regulatory Factors:	
Level 1 Implementation:	Data involved in electronic commerce and online transactions shall be checked to determine if it contains covered information. Security shall be maintained through all aspects of the transaction, ensuring that: i. user credentials of all parties are valid and verified; ii. the transaction remains confidential; and iii. privacy associated with all parties involved is retained. Protocols used to communicate between all involved parties shall be secured using cryptographic techniques (e.g., SSL).
Level 1 Control Standard Mapping:	• CSA IS-28 • ISO 27799-2008 7.7.9.1 • NIST Cybersecurity Framework PR.DS-1 • NIST Cybersecurity Framework PR.DS-2 • NIST Cybersecurity Framework PR.DS-5

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FTI Compliance
Level 2 Implementation:	Level 1 plus: The use of electronic signatures by each of the parties involved in the transaction shall be required. The organization shall ensure the storage of the transaction details are located outside of any publicly accessible environments (e.g., on a storage platform existing on the organization's intranet) and not retained and exposed on a storage medium directly accessible from the Internet. Where a trusted authority is used (e.g., for the purposes of issuing and maintaining digital signatures and/or digital certificates) security shall be integrated and embedded throughout the entire end-to-end

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	certificate/signature management process. Communications path between all involved parties shall be encrypted. The protocols used for communications shall be enhanced to address any new vulnerability, and the updated versions shall be adopted as soon as possible.
Level 2 Control Standard Mapping:	• ISO/IEC 27002-2005 10.9.2 • ISO/IEC 27002-2013 A.14.1.3 • IRS Pub 1075 v2014 9.4.2 (E.10) • Phase 1 CORE 153: Eligibility and Benefits Connectivity Rule v1.1.0 Subsection 5.1

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

FTI Requirements

FTI Custodians:	All Internet transmissions in a data warehouse are to be encrypted with the use of HTTPS protocol and secure sockets layer encryption based on a certificate that contains a key no less than 128 bits in length, or FIPS 140-2 compliant, whichever is stronger. All sessions shall be encrypted and provide end-to-end encryption (i.e., from workstation to point of data), as data is at its highest risk during the ETL stages when it enters the warehouse. Web server(s) that receive online transactions in a data warehouse shall be configured in a "demilitarized zone" to receive external transmissions but still have some measure of protection against unauthorized intrusion (e.g., by an IDS/IPS). Application server(s) and database server(s) supporting a data warehouse shall be configured behind the firewalls for optimal security against unauthorized intrusion. Only authenticated applications and users shall be allowed access to these servers. Transaction data shall be "swept" from the Web server(s) at frequent intervals, consistent with good system performance, and removed to a

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	secured server behind the firewalls to minimize the risk that these transactions could be destroyed or altered by intrusion.

Control Reference: 09.z Publicly Available Information

Control Specification:	The integrity of information being made available on a publicly available system shall be protected to prevent unauthorized modification.
Factor Type:	Organizational
Topics:	Authorization

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	There shall be a formal approval process before information is made publicly available. In addition, all input provided from the outside to the system shall be verified and approved. The source (authorship) of publicly available information shall be stated. The organization ensures that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications.
Level 1 Control Standard Mapping:	• NIST Cybersecurity Framework PR.AC-4 • NIST Cybersecurity Framework PR.DS-6

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to CMS Minimum Security Requirements (High), Subject to FTI Compliance
Level 2 Implementation:	Level 1 plus: The organization shall: i. designate individuals authorized to post information onto a publicly accessible information system; ii. train authorized individuals to ensure that publicly accessible information does not contain nonpublic information; iii. review the proposed content of information prior to posting onto the publically accessible information system prior to posting to ensure non-public information is not included; iv. review the content on the publicly accessible information systems for nonpublic information bi-weekly; and v. remove nonpublic information from the publicly accessible information systems, if discovered. The publicly accessible system shall be tested against weaknesses and failures prior to information being made available. Installation checklist and vulnerability testing shall be implemented to ensure security baselines and configuration baselines are met or exceeded. Electronic publishing systems, especially those that permit feedback and direct entering of information, shall be carefully controlled so that: i. information is obtained in compliance with any data protection legislation; ii. information input to, and processed by, the publishing system will be processed completely and accurately in a timely manner; iii. covered information will be protected during collection, processing, and storage; and iv. access to the publishing system does not allow unintended access to networks to which the system is connected. Publicly available health information (as distinct from personal health information) shall be archived.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-22 (HIGH) • CMSRs 2013v2 SC-CMS-2 (HIGH) • IRS Pub 1075 v2014 9.3.1.17 • ISO 27799-2008 7.7.9.2 • ISO/IEC 27001-2005 A10.9.3 • ISO/IEC 27001:2013 14.1.2 • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework PR.IP-1 • NIST Cybersecurity Framework DE.CM-6 • NIST SP 800-53 R4 AC-22

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to MARS-E Requirements
Level 3 Implementation:	Level 2 plus: Software, data, and other information requiring a high level of integrity being made available on a publicly available system shall be protected by appropriate mechanisms, including digital signatures. The signatures themselves provide a convenient point for either access or denial of service attack, and require extra protection. Digital Signatures shall be protected on a secure fault-tolerant system (e.g., increased capacity and bandwidth, service redundancy) with protected access and with full auditing.
Level 3 Control Standard Mapping:	• ISO/IEC 27002-2005 10.9.3 • ISO/IEC 27002-2013 A.14.1.2 • MARS-E v1 SC-14

CMS Contractor Requirements

CMS Contractors:	Web sites are operated within the restrictions addressed in OMB directives M-10-22 "Guidance for Online Use of Web Measurement and Customization Technologies" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications" and applicable CMS and DHHS directives and instruction. The organization shall monitor the CMS and DHHS security programs to determine if there are any modified directives and instruction.

FTI Requirements

FTI Custodians:	The agency must: i. Designate individuals authorized to post information onto a publicly accessible information system;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	ii. Train authorized individuals to ensure that publicly accessible information does not contain FTI; iii. Review the proposed content of information prior to posting onto the publicly accessible information system to ensure that FTI is not included; and iv. iv. Review the content on the publicly accessible information system for FTI, at a minimum, quarterly and remove such information, if discovered.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The organization ensures that network access controls, operating system file permissions, and application configurations protect the integrity of information stored, processed, and transmitted by publicly accessible systems, as well as the integrity of publicly accessible applications. If e-authentication is required and implemented in conjunction with or related to public access protections, refer to ARS Appendix D: E-authentication Standard.

Objective Name: 09.10 Monitoring

Control Objective:	Ensure information security events are monitored and recorded to detect unauthorized information processing activities in compliance with all relevant legal requirements.

Control Reference: 09.aa Audit Logging

Control Specification:	Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring. *Required for HITRUST Certification 2015
Factor Type:	System
Topics:	Audit and Accountability Documentation and Records Incident Response User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Information systems processing covered information shall create a secure audit record each time a user accesses, creates, updates, or archives covered information via the system. The audit logs shall include: i. a unique user identifier; ii. a unique data subject (e.g., the patient) identifier; iii. the function performed by the user (e.g., log-in, record creation, access, update, etc.); and iv. the time and date that the function was performed. Logs for operators or administrators shall also include: i. the type of event that occurred (e.g., success or failure); ii. the time at which an event occurred; iii. information about the event (e.g., files handled) or failure (e.g., error occurred and corrective action taken); iv. the account(s) and administrator(s) or operator(s) involved; and v. the process(es) involved. Retention for audit logs shall be specified by the organization and retained accordingly.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AU-8 (HIGH) • CSA SA-14 • HIPAA § 164.308(a)(5)(ii)(C) • HIPAA § 164.312(b) • IRS Pub 1075 v2014 9.3.3.11 • NIST Cybersecurity Framework PR.PT-1 • NIST Cybersecurity Framework DE.CM-1 • NIST Cybersecurity Framework DE.CM-3 • NIST SP 800-53 R4 AU-3 • NIST SP 800-53 R4 AU-8 • NIST SP 800-53 R4 AU-11 • NIST SP 800-53 R4 AR-4 • MARS-E v1 AU-8 • PCI DSS v3 10.1 • PCI DSS v3 10.2.1 • PCI DSS v3 10.3.1 • PCI DSS v3 10.3.2 • PCI DSS v3 10.3.3 • PCI DSS v3 10.3.6 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Number of Transactions Per Day: > 6,750, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: Messaging systems used to transmit messages containing covered information shall keep a log of message transmissions, such a log shall contain the time, date, origin and destination of the message, but not its content. The organization shall carefully assess and determine the retention period for these audit logs, with particular reference to professional standards and legal obligations, in order to enable investigations to be carried out when necessary and to provide evidence of misuse where necessary. Audit logs shall include, but are not limited to: i. dates, times, and details of key events (e.g., log-on and log-off); ii. records of successful and rejected system access attempts; iii. records of successful and rejected data and other resource access attempts; iv. changes to system configuration and procedures for managing configuration changes; v. use of privileges; vi. use of system utilities and applications; vii. files accessed and the kind of access; viii. network addresses and protocols; ix. alarms raised by the access control system; and x. activation and de-activation of protection systems, including anti-virus systems and intrusion detection systems, and identification and authentication mechanisms. xi. creation and deletion of system level objects. The organization shall provide a rationale for why the auditable events are deemed adequate to support after the fact investigations of security incidents and which events require auditing on a continuous basis in response to specific situations. The listing of auditable events shall be

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	reviewed and updated within every three hundred sixty-five (365) days. Information systems' audit logging systems shall be operational at all times while the information system being audited is available for use. Where necessary for highly sensitive logs, separation of duties and split key access shall be employed. Audit records shall be retained for ninety (90) days, and old records archived for one (1) year to provide support for after-the-fact investigations of security incidents and to meet regulatory and the organization's retention requirements.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AC-6(9) • CMSRs 2013v2 AU-2(3) (HIGH) • CMSRs 2013v2 AU-11 (HIGH) • IRS Pub 1075 v2014 9.3.1.6 • IRS Pub 1075 v2014 9.3.3.3 • ISO/IEC 27002-2005 10.10.1 • ISO/IEC 27002-2013 A.12.4.1 • ISO 27799-2008 7.7.10.2 • MARS-E v1 AU-2 • MARS-E v1 AU-2(4) • MARS-E v1 AU-11 • NIST Cybersecurity Framework DE.CM-7 • NIST SP 800-53 R4 AC-6(9) • NIST SP 800-53 R4 AU-2 • NIST SP 800-53 R4 AU-2(3) • PCI DSS v3 10.2 • PCI DSS v3 10.2.4 • PCI DSS v3 10.2.7 • PCI DSS v3 10.3 • PCI DSS v3 10.3.4 • PCI DSS v3 10.3.5 • PCI DSS v3 10.7 • PCI DSS v3 A.1.3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 5,500, Number of Transactions Per Day: > 85,000, Number of Interfaces to Other Systems: > 75
Level 3 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3	Level 2 plus:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Implementation:	i. server alerts and error messages; ii. user log-on and log-off (successful or unsuccessful); iii. all system administration activities; iv. modification of privileges and access; v. Start up and shut down; vi. application modifications; vii. application alerts and error messages; viii. configuration changes; ix. account creation, modification, or deletion; x. file creation and deletion; xi. read access to sensitive information; xii. modification to sensitive information; and xiii. printing sensitive information. The information system also generates audit records containing the following additional, more detailed information: i. Filename accessed; ii. Program or command used to initiate the event; and iii. Source and destination addresses. Disclosures of covered information shall be recorded. Information type, date, time, receiving party, and releasing party shall be logged. The organization shall verify every ninety (90) days for each extract that the data is erased or its use is still required. Account creation, modification, disabling, enabling and removal actions shall be automatically logged and audited providing notification, as required, to appropriate individuals.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 AC-2(4) (HIGH) • CMSRs 2013v2 AU-2 (HIGH) • CMSRs 2013v2 AU-2(4) (HIGH) • CMSRs 2013v2 AU-3 (HIGH) • CMSRs 2013v2 AU-3(1) (HIGH) • CMSRs 2013v2 AU-3(2) (HIGH) • CMSRs 2013v2 AU-12 (HIGH) • CMSRs 2013v2 AU-12(1) (HIGH) • CMSRs 2012v2 AU-12(3) (HIGH) • IRS Pub 1075 v2014 9.3.3.4 • IRS Pub 1075 v2014 9.3.3.12 • IRS Pub 1075 v2014 9.4.3 • IRS Pub 1075 v2014 9.4.9 • IRS Pub 1075 v2014 9.4.11 • IRS Pub 1075 v2014 9.4.13 • IRS Pub 1075 v2014 9.4.18 • MARS-E v1 AC-2(4) • MARS-E v1 AU-3

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• MARS-E v1 AU-12 • MARS-E v1 AU-12(1) • NIST SP 800-53 R4 AC-2(4) • NIST SP 800-53 R4 AU-3(1) • NIST SP 800-53 R4 AU-12 • NRS 603A.215.1 • PCI DSS v3 10.2.5 • PCI DSS v3 10.2.6 • 1 TAC § 390.2(a)(4)(A)(xi)

CMS Contractor Requirements:

Health Insurance Exchanges:	The organization shall audit inspection reports, including a record of corrective actions, shall be retained by the organization for a minimum of three (3) years from the date the inspection was completed. Audit records shall be compiled from multiple components throughout the system into a system-wide (logical or physical) audit trail that is time-correlated to within +/- five (5) minutes. The organization shall centrally manage the content of audit records generated by individual components throughout the information system. A real time alert shall be provided when the audit record log is full or there is an authentication or encryption logging failure. The information system provides the capability for defined individuals or roles (defined in the applicable security plan) to change the auditing to be performed on defined information system components (defined in the applicable security plan) based on defined selectable event criteria (defined in the applicable security plan) within minutes.

FTI Requirements

FTI Custodians:	The organization shall provide an audit record generation capability and audit the following events, at a minimum: i. Log onto system; ii. Log off of system; iii. Change of password; iv. All system administrator commands, while logged on as system v. administrator; vi. Switching accounts or running privileged actions from another account, vii. (e.g., Linux/Unix SU or Windows RUNAS); viii. Creation or modification of super-user groups; ix. Subset of security administrator commands, while logged on in the security x. administrator role;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

xi. Subset of system administrator commands, while logged on in the user role;
xii. Clearing of the audit log file;
xiii. Startup and shutdown of audit functions;
xiv. Use of identification and authentication mechanisms (e.g., user ID and
xv. password);
xvi. Change of file or user permissions or privileges (e.g., use of suid/guid, chown, su);
xvii. Remote access outside of the corporate network communication channels (e.g., modems, dedicated VPN) and all dial-in access to the system;
xviii. Changes made to an application or database by a batch file;
xix. Application-critical record changes;
xx. Changes to database or application records, where the application has been bypassed to produce the change (via a file or other database utility);
xxi. All system and data interactions concerning FTI; and
xxii. Additional platform-specific events, as defined in SCSEMs located on the Office of Safeguards website.

The organization shall audit records for the following events in addition to those specified:

i. all successful and unsuccessful authorization attempts;
ii. all changes to logical access control authorities (e.g., rights, permissions);
iii. all system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services;
iv. the audit trail shall capture the enabling or disabling of audit report generation services; and
v. the audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

The organization shall also:

i. allow designated agency officials to select which auditable events are to be audited by specific components of the information system;
ii. coordinate the security audit function with other agency entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;
iii. provide a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
iv. review and update the audited events at a minimum, annually.

Audit logs must enable tracking activities taking place on the system. Pub 1075, Exhibit 9, System Audit Management Guidelines, contains

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	requirements for creating audit-related processes at both the application, auditing must be enabled to the extent necessary to capture access, modification, deletion and movement of FTI by each unique user. This auditing requirement also applies to data tables or databases embedded in or residing outside of the application that contain FTI. Information systems generate audit records containing details to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected in the audit records for audit events identified by type, location, or subject. Audit logging must be implemented to properly track all email that contains FTI. Multifunction Devices (MFDs) and its print spoolers shall have auditing enabled, including the auditing of user access and fax logs (if fax is enabled). SAN components must maintain an audit trail of access to FTI in the SAN environment. To use FTI in an 802.11 WLAN environment, the agency must enable security event logging on WLAN components.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	The information system includes the capability to include more detailed information in the audit records for audit events identified by type, location, or subject.

PCI-DSS Requirements

PCI Data:	A service provider shall protect each organization's hosted environment and data by ensuring logging and audit trails are enabled and unique to each organization's (customer's) cardholder data environment and consistent with PCI DSS v3 Requirement 10.

Control Reference: 09.ab Monitoring System Use

Control Specification:	Procedures for monitoring use of information processing systems and facilities shall be established to check for use and effectiveness of implemented controls. The results of the monitoring activities shall be reviewed regularly. *Required for HITRUST Certification 2015
Factor Type:	System

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Topics:	Incident Response Monitoring Requirements (Legal and Contractual) User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The organization shall comply with all relevant legal requirements applicable to its monitoring activities. Items that shall be monitored include: i. authorized access; and ii. unauthorized access attempts.
Level 1 Control Standard Mapping:	• HIPAA § 164.308(a)(1)(ii)(D) • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(4)(i) • HIPAA § 164.308(a)(4)(ii)(B) • HIPAA § 164.308(a)(5)(ii)(B) • HIPAA § 164.308(a)(5)(ii)(C) • HIPAA § 164.312(b) • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework DE.DP-2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.03(2)(h) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Number of Transactions Per Day: > 6,750, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to FTC Red Flags Rule Compliance, Subject to State of Massachusetts Data Protection Act

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Implementation:	Level 1 plus: Information systems containing covered information shall actively be provided with automated assets for monitoring events of the system(s), detecting attacks, and analyzing logs and audit trails that: i. allow the identification of all system users who have accessed or modified a given record(s) over a given period of time; and ii. allow the identification of all records that have been accessed or modified by a given system user over a given period of time. Monitoring devices shall be strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. Monitoring devices shall also be deployed at ad hoc locations within the system to track specific transactions. Additionally, these devices shall be used to track the impact of security changes to the information system. The organization: i. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; ii. Reviews physical access logs weekly and upon occurrence of security incidents involving physical security; and iii. Coordinates results of reviews and investigations with the organization's incident response capability. Monitoring of authorized access shall include: i. the user ID; ii. the date and time of key events; iii. the types of events; iv. the files accessed; and v. the program/utilities used. All privileged operations shall be monitored including: i. the use of privileged accounts (e.g., supervisor, root, administrator); ii. the system start-up and stop; and iii. I/O device attachment/detachment. Monitoring of unauthorized access attempts shall include: i. failed or rejected user actions; ii. failed or rejected actions involving data and other resources; iii. access policy violations and notifications for network gateways and firewalls; and iv. alerts from proprietary intrusion detection systems. System alerts or failures shall be monitored including: i. console alerts or messages; ii. system log exceptions; iii. network management alarms;

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	iv. alarms raised by the access control system (e.g., intrusion detection, intrusion prevention, or networking monitoring software); and v. changes to, or attempts to change, system security settings and controls. The information system shall provide the capability to automatically process audit records in the information system for events of interest based on selectable event criteria. Systems shall support audit reduction and report generation that supports expeditious, on-demand review, analysis, reporting and after-the-fact incident investigations of security incidents and does not alter the original content or time marking of audit records.
Level 2 Control Standard Mapping:	• 16 CFR Part §681 Appendix A III(b) • CMSRs 2013v2 AU-7 (HIGH) • CMSRs 2013v2 AU-7(1) (HIGH) • CMSRs 2013v2 PE-6 (HIGH) • COBIT 4.1 DS5.7 • COBIT 5 DSS05.05 • IRS Pub 1075 v2014 4.3.2 • IRS Pub 1075 v2014 9.3.3.8 • IRS Pub 1075 v2014 9.3.11.6 • ISO/IEC 27002-2005 10.10.2 • ISO/IEC 27002-2005 12.5.4 • ISO/IEC 27002-2013 A.12.4.1 • ISO 27799-2008 7.7.10.3 • MARS-E v1 AU-7 • MARS-E v1 AU-7(1) • MARS-E v1 PE-6 • NIST Cybersecurity Framework PR.PT-1 • NIST Cybersecurity Framework DE.AE-2 • NIST Cybersecurity Framework DE.AE-3 • NIST Cybersecurity Framework DE.CM-1 • NIST Cybersecurity Framework RS.CO-3 • NIST SP 800-53 R4 AU-7 • NIST SP 800-53 R4 AU-7(1) • NIST SP 800-53 R4 PE-6 • NIST SP 800-53 R4 AR-4 • (State of Mass.) 201 CMR 17.04(4) • 1 TAC § 390.2(a)(3)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 5,500, Number of Transactions Per Day: > 85,000, Number of Interfaces to Other Systems: > 75
Level 3 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: Unauthorized remote connections to the information systems shall be monitored and reviewed at least quarterly, and appropriate action shall be taken if an unauthorized connection is discovered. The results of monitoring activities shall be reviewed daily, through the use of automated tools, for: i. all security events, ii. logs of all critical system components, and iii. logs of all servers that perform security functions like intrusion detection system (IDS), intrusion prevention system (IPS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). The automated tools shall generate alert notification for technical staff review and assessment. The organization shall review logs of all other system components periodically based on its policies and risk management strategy, as determined by the organization's annual risk assessment. System records shall be reviewed for: i. initialization sequences; ii. log-ons and errors; iii. system processes and performance; and iv. system resources utilization. The reviews shall be conducted daily and the results shall be used to determine anomalies on demand. An alert notification shall be generated for technical personnel review and analyze. Suspicious activity or suspected violations on the information system identified during the review process shall be investigated, with findings reported to appropriate officials and take appropriate action. Manual reviews of system audit records shall be performed randomly on demand, but at least once every thirty (30) days. The organization shall employ automated mechanisms to integrate the audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization shall employ automated tools to support near real-time analysis of events and maintain an audit log to track prohibited sources and services. Inbound and outbound communications shall be monitored at an organization-defined frequency for unusual or unauthorized activities or conditions. The organization shall specify the permitted actions for information system processes, roles, and/or users associated with review, analysis, and reporting of audit records (e.g., read, write, execute, append, and delete). The organization shall deploy a change-detection mechanism (e.g., file-integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; configures the software to perform critical file comparisons at least weekly, and responds to any alerts generated. The information system shall provide near real-time alerts when the following indications of compromise or potential compromise occur: i. presence of malicious code; ii. unauthorized export of information; iii. signaling to an external information system; or iv. potential intrusions. The organization analyzes and correlates audit records across different repositories and correlates this information with input from non-technical sources to gain and enhance organization-wide situational awareness.
Level 3 Control Standard Mapping:	• IRS Pub 1075 v2014 9.3.17.4 • CMSRs 2013v2 AC-2(12) (HIGH) • CMSRs 2013v2 AU-6 (HIGH) • CMSRs 2013v2 AU-6(1) (HIGH) • CMSRs 2013v2 AU-6(3) (HIGH) • CMSRs 2013v2 AU-6(5) (HIGH) • CMSRs 2013v2 AU-6(6) (HIGH) • CMSRs 2013v2 PE-6(4) (HIGH) • CMSRs 2013v2 SI-4 (HIGH) • CMSRs 2013v2 SI-4(1) (HIGH) • CMSRs 2013v2 SI-4(2) (HIGH) • CMSRs 2013v2 SI-4(3) (HIGH) • CMSRs 2013v2 SI-4(4) (HIGH) • CMSRs 2013v2 SI-4(5) (HIGH) • CSA SA-14 • IRS Pub 1075 v2014 6.4.1 • IRS Pub 1075 v2014 9.3.3.7 • IRS Pub 1075 v2014 9.3.16.6 • IRS Pub 1075 v2014 9.4.2 (E.10) • IRS Pub 1075 v2014 9.4.9

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• IRS Pub 1075 v2014 9.4.11 • IRS Pub 1075 v2014 9.4.13 • IRS Pub 1075 v2014 9.4.14 • IRS Pub 1075 v2014 9.4.15 • IRS Pub 1075 v2014 9.4.18 • MARS-E v1 AC-17 • MARS-E v1 AU-6 • MARS-E v1 AU-6(1) • MARS-E v1 SI-4 • MARS-E v1 SI-4(1) • MARS-E v1 SI-4(2) • MARS-E v1 SI-4(4) • MARS-E v1 SI-4(5) • NIST Cybersecurity Framework ID.RA-1 • NIST Cybersecurity Framework DE.CM-4 • NIST Cybersecurity Framework DE.CM-7 • NIST Cybersecurity Framework DE.DP-4 • NIST Cybersecurity Framework RS.AN-1 • NIST Cybersecurity Framework RS.CO-2 • NIST SP 800-53 R4 AU-6 • NIST SP 800-53 R4 AU-6(1) • NIST SP 800-53 R4 AU-6(3) • NIST SP 800-53 R4 AU-6(9) • NIST SP 800-53 R4 SI-4 • NIST SP 800-53 R4 SI-4(2) • NIST SP 800-53 R4 SI-4(4) • NIST SP 800-53 R4 SI-4(5) • NRS 603A.215.1 • PCI DSS v3 10.6 • PCI DSS v3 10.6.1 • PCI DSS v3 10.6.2 • PCI DSS v3 10.6.3 • PCI DSS v3 11.5

CMS Contractor Requirements

CMS Contractors:	The organization shall interconnect and configure individual intrusion detection tools into a system-wide intrusion detection system (IDS) using common protocols. The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination. The organization shall: i. monitor events on the information system in accordance with the current Risk Management Handbook (RMH), Volume II, Procedure

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	7.2, Incident Handling, and detect information system attacks; ii. heighten the level of information system monitoring activity whenever there is an indication of increased risk to CMS operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. The organization monitors physical access to the information system, in addition to the physical access monitoring of the facility, at defined physical spaces (defined in the applicable security plan) containing a concentration of information system components (e.g., server rooms, media storage areas, data and communications centers, etc.). The organization: i. Monitors information system accounts for atypical use; and ii. Reports atypical usage of information system accounts to defined personnel or roles (defined in the applicable security plan), and if necessary, incident response team. The organization integrates analysis of audit records with analysis of (one-or-more, defined in the applicable security plan): vulnerability scanning information; performance data; information system monitoring information; and/or other defined data/information (defined in the applicable security plan) collected from other sources, to further enhance the ability to identify inappropriate or unusual activity. The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.

FTI Requirements

FTI Custodians:	All requests for return information, including receipt and/or disposal of returns or return information, shall be maintained in a log. Report findings from the review and analysis of information system audit records according to the agency incident response policy. If the finding involves a potential unauthorized disclosure of FTI, the appropriate special agent-in-charge, Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards must be contacted, as described in Section 10.0, Reporting Improper Inspections or Disclosures. Intrusion-detection software shall be installed and maintained to monitor networks for any unauthorized attempt to access tax data in a data warehouse. The organization must employ automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications,

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	and implement host-based monitoring mechanisms (e.g., Host intrusion prevention system (HIPS)) on information systems that receive, process, store, or transmit FTI. The information system must notify designated agency officials of detected suspicious events and take necessary actions to address suspicious events. The agency shall ensure that audit reports are created and reviewed for data warehousing related access attempts. If a query is submitted, the audit log must identify the actual query made, the originator of the query, and relevant time and stamp information. A security administrator shall periodically collect and review audit logs from Multifunction Devices (MFDs) and its print spoolers. The organization reviews the audit logs (trails) of SAN components on a regular basis to track access to FTI in the SAN environment. To use a virtual environment that receives, processes, stores, or transmits FTI, the agency must ensure virtualization providers must be able to monitor for threats and other activity that is occurring within the virtual environment—this includes being able to monitor the movement of FTI into and out of the virtual environment. To use a VoIP network that provides FTI to a customer, the agency must be able to track and audit all FTI-applicable conversations and access. To use FTI in an 802.11 WLAN, the agency must deploy wireless intrusion detection to monitor for unauthorized access.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	Review network traffic, bandwidth utilization rates, alert notifications, and border defense devices to determine anomalies on demand but no less than once within a twenty-four (24) hour period. Generate alerts for technical personnel review and assessment. Use automated utilities to review audit records at least once every seven (7) days for unusual, unexpected, or suspicious behavior. Inspect administrator groups on demand but at least once every fourteen (14) days to ensure unauthorized administrator accounts have not been created.

PCI-DSS Requirements

PCI Data:	The organization shall review, at least daily, the logs of all system

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	components that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

Control Reference: 09.ac Protection of Log Information

Control Specification:	Logging systems and log information shall be protected against tampering and unauthorized access. *Required for HITRUST Certification 2015
Factor Type:	System
Topics:	Audit and Accountability Documentation and Records User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Access to system audit tools and audit trails shall be safeguarded from unauthorized access and use to prevent misuse or compromise of logs.
Level 1 Control Standard Mapping:	• ISO/IEC 27002:2005 10.10.3 • ISO/IEC 27002:2013 12.4.2 • ISO/IEC 27002:2013 12.4.3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Number of Transactions Per Day: > 6,750, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Access to audit tools and audit trails shall be limited to those with a job-related need. Authorized and unauthorized access attempts to the audit system and audit trails shall be logged and protected from modification. Controls shall protect against unauthorized changes and operational problems with the logging system(s) including: i. promptly back up audit trail files to a centralized log server or media that is difficult to alter. ii. alterations to the message types that are recorded (e.g., write-once media); iii. log files being edited or deleted. The organization authorizes access to management of audit functionality to a specific subset of privileged users defined by the organization.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 AU-9 (HIGH) • CMSRs 2013v2 AU-9(2) (HIGH) • CMSRs 2013v2 AU-9(3) (HIGH) • CMSRs 2013v2 AU-9(4) (HIGH) • COBIT 4.1 DS5.7 • COBIT 5 DSS05.05 • IRS Pub 1075 v2014 5.4 • IRS Pub 1075 v2014 9.3.3.10 • IRS Pub 1075 v2014 9.3.3.13 • IRS Pub 1075 v2014 9.4.1 • ISO 27799-2008 7.7.10.4 • MARS-E v1 AU-9 • NIST Cybersecurity Framework PR.PT-1 • NIST SP 800-53 R4 AU-9 • NIST SP 800-53 R4 AU-9(4) • PCI DSS v3 10.2.3 • PCI DSS v3 10.5 • PCI DSS v3 10.5.1 • PCI DSS v3 10.5.2 • PCI DSS v3 10.5.3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation:	Level 2 plus: The organization shall implement file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert), and respond to any alerts generated. The information system: i. Alerts defined personnel or roles (defined in the applicable security plan) in the event of an audit processing failure; and ii. Takes the following additional actions in response to an audit failure: a. Shutdown the information system, b. Stop generating audit records, or c. Overwrite the oldest records, in the case that storage media is unavailable. Write logs for external-facing technologies (wireless, firewalls, DNS, mail) onto a secure, centralized log server or media device on the internal LAN.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 AU-5 (HIGH) • CMSRs 2013v2 AU-5(1) (HIGH) • CMSRs 2013v2 AU-5(2) (HIGH) • IRS Pub 1075 v2014 9.3.3.6 • MARS-E v1 AU-5 • NRS 603A.215.1 • NIST SP 800-53 R4 AU-5 • PCI DSS v3 10.5.4 • PCI DSS v3 10.5.5 • PCI DSS v3 11.5 • PCI DSS v3 11.5.1

CMS Requirements

CMS Contractors	The information system shall provide a warning to defined personnel, roles, and/or locations (defined in the applicable security plan), within a defined time period (defined in the applicable security plan), when allocated audit record storage volume reaches 80% of repository maximum audit record storage capacity. The information system provides an alert in real-time to defined personnel, roles, and/or locations (defined in the applicable security plan) when the following audit failure events occur: i. Record log is full; ii. Authentication logging failure; and iii. Encryption logging failure. The information system backs up audit records at least weekly onto a physically different system or system component than the system or

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	component being audited. The information system implements cryptographic mechanisms to protect the integrity of audit information and audit tools.

FTI Requirements

FTI Custodians	The information system must monitor system operational status using operating system or system audit logs and verify functions and performance of the system. Logs shall be able to identify where system process failures have taken place and provide information relative to corrective actions to be taken by the system administrator. The information system does not shut down the system, stop the generation of audit reports or overwrite the oldest records in the event of an audit failure or audit storage capacity issue. The agency must employ mechanisms for coordinating the access and protection of audit information among external organizations when audit information is transmitted across agency boundaries. For additional requirements, see IRS Pub 1075 v2014 9.4.1 for cloud computing environments and 5.4 for consolidated data centers.

Control Reference: 09.ad Administrator and Operator Logs

Control Specification:	System administrator and system operator activities shall be logged and regularly reviewed.
Factor Type:	System
Topics:	Audit and Accountability Documentation and Records Monitoring

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements; Subject to FISMA Compliance; Subject to PCI Compliance
Level 1 Implementation:	Organizations shall ensure that proper logging is enabled in order to audit administrator activities.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	System administrator and operator logs shall be reviewed on a regular basis.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AU-2 (HIGH) • HIPAA § 164.308(a)(5)(ii)(C) • HIPAA § 164.312(b) • MARS-E v1 AU-2 • NIST Cybersecurity Framework PR.PT-1 • NIST SP 800-53 R4 AU-2 • NIST SP 800-53 R4 AR-4 • NRS 603A.215.1 • PCI DSS v3 10.2.2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 5,500, Number of Transactions Per Day: > 85,000, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: An intrusion detection system managed outside of the control of system and network administrators shall be used to monitor system and network administration activities for compliance.
Level 2 Control Standard Mapping:	• CSA SA-14 • ISO/IEC 27002-2005 10.10.4 • ISO/IEC 27002:2013 12.4.3 • ISO 27799-2008 7.7.10.5

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 09.ae Fault Logging

Control Specification:	Faults shall be logged, analyzed, and appropriate remediation action taken.
Factor Type:	System
Topics:	Audit and Accountability Documentation and Records Incident Response
Products and Services Guide:	09.ae Fault Logging

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Faults reported by users or by system programs related to problems with information processing or communications systems shall be logged. There shall be clear rules for handling reported faults including: i. review of fault logs by authorized personnel in an expeditious manner to ensure that faults have been satisfactorily resolved; and ii. review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized. Error logging shall be enabled if this system function is available.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AU-2 (HIGH) • CSA SA-14 • HIPAA § 164.308(a)(5)(ii)(C) • HIPAA § 164.312(b) • ISO/IEC 27002-2005 10.10.5 • ISO/IEC 27002:2013 12.4.1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• ISO 27799-2008 7.7.10.6 • MARS-E v1 AU-2 • NIST Cybersecurity Framework PR.PT-1 • NIST SP 800-53 R4 AU-2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Number of Transactions Per Day: > 6,750, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements; Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: The information system shall: i. identify potentially security-relevant error conditions; ii. generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries in error logs and administrative messages that could be exploited by adversaries; and iii. reveal error messages only to authorized personnel. The information system shall provide automated real-time alerts when faults or errors occur. Covered information shall not be listed in the logs or associated administrative messages.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 SI-11 (HIGH) • IRS Pub 1075 v2014 9.3.17.8 • MARS-E v1 SI-11 • NIST SP 800-53 R4 SI-11

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 09.af Clock Synchronization

Control Specification:	The clocks of all relevant information processing systems within the organization or security domain shall be synchronized with an agreed accurate time source to support tracing and reconstitution of activity timelines. *Required for HITRUST Certification 2015
Factor Type:	System
Topics:	Audit and Accountability Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 1 Implementation:	The organization shall synchronize all system clocks and times where a computer or communications device has the capability to operate a real-time clock. This clock shall be set to an agreed standard received from industry-accepted time sources, either Coordinated Universal Time (UTC) or International Atomic Time and shall be accurate to within thirty (30) seconds. The correct interpretation of the date/time format shall be used to ensure that the timestamp reflects the real date/time (e.g., daylight savings). The information system's internal information system clocks shall synchronize daily and at system boot to one or more authoritative sources (e.g., NIST Internet Time Servers or the U.S. Naval Observatory Stratum-1 NTP servers) when the time difference is greater than thirty (30) seconds.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 AU-8 (HIGH) • CMSRs 2013v2 AU-8(1) (HIGH) • CSA SA-12

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• IRS Pub 1075 v2014 9.3.3.9 • ISO/IEC 27002-2005 10.10.6 • ISO/IEC 27002:2013 12.4.4 • ISO 27799-2008 7.7.10.7 • MARS-E v1 AU-8 • MARS-E v1 AU-8(1) • NIST Cybersecurity Framework PR.PT-1 • NIST SP 800-53 R4 AU-8 • NIST SP 800-53 R4 AU-8(1) • PCI DSS v3 10.4 • PCI DSS v3 10.4.1 • PCI DSS v3 10.4.3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None, Processing PHI: Yes - AND -, Number of Users: > 500, Number of Transactions Per Day: > 6,750, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: Time data shall be protected according to the organizations access controls (see 01.c) and logging controls (see 09.ad).
Level 2 Control Standard Mapping:	• NRS 603A.215.1 • PCI DSS v3 10.4.2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Category: 10.0 - Information Systems Acquisition, Development, and Maintenance

Objective Name: 10.01 Security Requirements of Information Systems

Control Objective:	To ensure that security is an integral part of information systems.

Control Reference: 10.a Security Requirements Analysis and Specification

Control Specification:	Statements of business requirements for new information systems (developed or purchased), or enhancements to existing information systems shall specify the requirements for security controls.
Factor Type:	Organizational
Topics:	Documentation and Records Requirements (Legal and Contractual) Risk Management and Assessments Services and Acquisitions

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The organization shall develop, disseminate, and review/update annually: i. a formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and ii. formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls. Specifications for the security control requirements shall include that security controls be incorporated in the information system, supplemented by manual controls as needed. These considerations shall be applied when evaluating software packages, developed or purchased.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Security requirements and controls shall reflect the business value of the information assets involved (see 7.d), and the potential business damage that might result from a failure or absence of security. For purchased commercial product, a formal acquisition process shall be followed. Contracts with the supplier shall include the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement, then the risk introduced and associated controls shall be reconsidered prior to purchasing the product. Where additional functionality is supplied and causes a security risk, this shall be disabled or mitigated through application of additional controls. The organization shall require developers of information systems, components, and services to identify (document) early in the system development life cycle, the functions ports, protocols, and services intended for organizational use.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 SA-4(9) (HIGH) • HIPAA § 164.314(a)(2)(i) • NIST Cybersecurity Framework PR.IP-2 • NIST SP 800-53 R4 SA-4(9) • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: Information security and privacy shall be addressed in all phases of the project management methodology. Organizations shall establish and appropriately protect secure development environment for system development and integration efforts that cover the entire system development lifecycle. The organization shall apply information system security engineering principles in the specification, design, development, implementation, and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	modification of security requirements and controls in developed and acquired information systems. Organizations shall include business requirements for the availability of information systems when specifying security and privacy requirements. Where availability cannot be guaranteed using existing architectures, redundant components or architectures should be considered along with the risks associated with implementing such redundancies. Specifications for the security and privacy control requirements shall include that automated controls be incorporated in the information system, supplemented by manual controls as needed. This shall be evidenced in a formal System Development Lifecycle (SDLC), which shall cover request initiation, requirements definition, analysis, communication, conflict detection and resolution, and evolution of requirements. The organization's security risk management process shall be integrated into all SDLC activities. System requirements for information security and processes for implementing security shall be integrated in the requirements definition phase. Also in the SDLC initial planning or requirement stage, Data Classification and risk of the assets shall be assigned to ensure appropriate controls will be considered and the correct project team members are involved. The risk and classification activities shall require sign-off by management. Organizations developing software or systems shall perform thorough testing and verification during the development process. Independent acceptance testing should then be undertaken (both for in-house and for outsourced developments) to ensure the system works as expected and only as expected. The extent of testing should be in proportion to the importance and nature of the system. Information security roles and responsibilities are defined and documented throughout the system development life cycle. Commercial products sought to store and/or process covered information shall undergo a security assessment and/or security certification by a qualified assessor prior to implementation. (Not applicable to operating system software).
Level 2 Control Standard Mapping:	• CMSRs 2013v2 SA-3 (HIGH) • CMSRs 2013v2 SA-8 (HIGH) • CSA IS-04 • IRS Pub 1075 v2014 9.3.15.3 • IRS Pub 1075 v2014 9.3.15.6 • ISO/IEC 27002-2005 12.1.1 • ISO/IEC 27001:2013 6.1.5 • ISO/IEC 27002:2013 14.1.1 • ISO/IEC 27002:2013 14.2.1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• ISO/IEC 27002:2013 14.2.5 • ISO/IEC 27002:2013 14.2.6 • ISO/IEC 27002:2013 14.2.8 • ISO/IEC 27002:2013 17.2.1 • ISO 27799-2008 7.9.1 • MARS-E v1 SA-3 • MARS-E v1 SA-8 • NIST SP 800-53 R4 SA-3 • NIST SP 800-53 R4 SA-8 • NRS 603A.215.1 • PCI DSS v3 6.3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: The organization develops enterprise architecture with consideration for information security and privacy, and the resulting risk to organizational operations, organizational assets, individuals, and other organizations. The organization shall: i. Develop an information security architecture for the information system that: a. Describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; b. Describes how the information security architecture is integrated into and supports the enterprise architecture; and c. Describes any information security assumptions about, and dependencies on, external services. ii. Reviews and updates (as necessary) the information security and privacy architecture whenever changes are made to the enterprise architecture; and iii. Ensures that planned information security and privacy architecture

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	changes are reflected in the security plan and organizational procurements/acquisitions. The organization shall include security functional, strength and assurance requirements; security-related documentation requirements; and developmental and evaluation-related assurance requirements in information system acquisition contracts based on applicable laws, policies, standards, guidelines and business needs. The organization requires the developer of the information system, system component, or information system service to provide: i. a description of the functional properties of the security and privacy controls to be employed and ii. design and implementation information for the security and privacy controls to be employed that includes: security- and privacy-relevant external system interfaces at sufficient detail to understand the existence, purpose, and use of all such interfaces and high-level design documentation at sufficient detail to prove the security and privacy control implementation.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 PL-8 (HIGH) • CMSRs 2013v2 PM-7 (HIGH) • CMSRs 2013v2 SA-4 (HIGH) • CMSRs 2013v2 SA-4(1) (HIGH) • CMSRs 2013v2 SA-4(2) (HIGH) • CMSRs 2013v2 SA-15 (HIGH) • CMSRs 2013v2 SA-17 (HIGH) • IRS Pub 1075 v2014 9.3.15.4 • IRS Pub 1075 v2014 9.4.2 (E.10) • MARS-E v1 PM-7 • MARS-E v1 SA-4 • MARS-E v1 SA-4(1) • MARS-E v1 SA-4(4) • MARS-E v1 SA-5(1) • MARS-E v1 SA-5(2) • MARS-E v1 SA-5(3) • NIST SP 800-53 R4 PL-8 • NIST SP 800-53 R4 PM-7 • NIST SP 800-53 R4 SA-4 • NIST SP 800-53 R4 SA-4(1) • NIST SP 800-53 R4 AR-7

CMS Contractor Requirements

CMS Contractors:	The organization shall manage the information system using the information security steps of IEEE 12207.0 standard for SDLC, as provided in the CMS eXpedited Life Cycle (IXLC) that incorporates information security control

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	considerations. Each contract and Statement of Work (SOW) that requires development or access to CMS information must include language requiring adherence to CMS security and privacy policies and standards, define security roles and responsibilities, and receive approval from CMS officials. The organization: i. Requires the developer of the information system, system component, or information system service to follow a documented development process that: a. Explicitly addresses security requirements; b. Identifies the standards and tools used in the development process; c. Documents the specific tool options and tool configurations used in the development process; and d. Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and ii. Reviews the development process, standards, tools, and tool options/configurations within every three hundred sixty-five (365) days to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy all applicable System Acquisition (SA) and Configuration Management (CM) security controls. The organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that: i. Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; ii. Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and iii. Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection.

FTI Requirements

FTI Custodians:	Whenever information systems contain FTI, the agency shall include security requirements (e.g., the capacity to block information to contractors when they are not authorized to access FTI) and/or security specifications, either explicitly or by reference, in information system acquisition contracts based on an assessment of risk. The contract for the acquisition must contain IRS Pub 1075 Exhibit 7 (E.7) language.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Agencies using a consolidated data center must implement appropriate controls to ensure the protection of FTI, including a Service Level Agreement (SLA) between the agency authorized to receive FTI and the data center. The agency shall document online and architectural adjustments that occur during the life cycle of a data warehouse and ensure that FTI is always secured from unauthorized access or disclosure. For critical online resources, redundant systems in a data warehouse shall be employed with automatic failover capability.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	Each contract and Statement of Work (SOW) that requires development or access to ACA information must include language requiring adherence to organizational security policies and standards, define security roles and responsibilities, and receive approval from organization officials. The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.

Objective Name: 10.02 Correct Processing in Applications

Control Objective:	To ensure the prevention of errors, loss, unauthorized modification or misuse of information in applications, controls shall be designed into applications, including user developed applications to ensure correct processing. These controls shall include the validation of input data, internal processing and output data.

Control Reference: 10.b Input Data Validation

Control Specification:	Data input to applications and databases shall be validated to ensure that this data is correct and appropriate. *Required for HITRUST Certification 2015
Factor Type:	System
Topics:	Policies and Procedures Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to FTC Red Flags Rule Compliance, Subject to Joint Commission Accreditation
Level 1 Implementation:	For organizations doing system development (e.g., applications, databases) checks shall be applied to the input of business transactions, standing data, and parameter tables and minimally for covered information. The organization shall develop applications based on secure coding guidelines to prevent common coding vulnerabilities in software development processes including but not limited to: i. injection flaws, particularly SQL injection. (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.) ii. buffer overflow (Validate buffer boundaries and truncate input strings.) iii. insecure cryptographic storage (Prevent cryptographic flaws) iv. insecure communications (Properly encrypt all authenticated and sensitive communications) v. improper error handling (Do not leak information via error messages) vi. broken authentication/sessions (Prevent unauthorized individuals from compromising legitimate account credentials, keys or session tokens that would otherwise enable an intruder to assume the identity of an authorized user) For web applications and application interfaces (internal or external) this also includes but is not limited to: i. cross-site scripting (XSS) (Validate all parameters before inclusion, utilize context-sensitive escaping, etc.) ii. improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access functions (Properly authenticate users and sanitize input. Do not expose internal object references to users.) iii. cross-site request forgery (CSRF). (Do not reply on authorization credentials and tokens automatically submitted by browsers.) Web-based applications shall be checked for the most current OWASP top 10 input-validation related vulnerabilities. Alternatively, the inclusion of input validation checks in the testing methodology shall be in place, and performed at least annually. Input validation testing can be manually performed. The following input validation procedures shall be performed: i. dual input or other input checks, such as boundary checking or

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	limiting fields to specific ranges of input data, to detect the following errors: a. out-of-range values b. invalid characters in data fields c. missing or incomplete data d. exceeding upper and lower data volume limits e. unauthorized or inconsistent control data ii. periodic review of the content of key fields or data files to confirm their validity and integrity; iii. procedures for responding to validation errors; iv. procedures for testing the plausibility of the input data; v. verifying the identity of an individual opening or updating an account; vi. defining the responsibilities of all personnel involved in the data input process; and vii. creating a log of the activities involved in the data input process (see 9.aa).
Level 1 Control Standard Mapping:	• 16 CFR Part §681 Appendix A III(a) • 16 CFR Part §681 Appendix A III(b) • CSA SA-04 • CSA SA-05 • ISO/IEC 27002-2005 12.2.1 • ISO 27799-2008 7.9.2.2 • JCAHO IM.04.01.01, EP 1 • NIST Cybersecurity Framework PR.DS-5 • NIST Cybersecurity Framework PR.DS-6 • NIST SP 800-53 R4 SI-10 • PCI DSS v3 6.5 • PCI DSS v3 6.5.1 • PCI DSS v3 6.5.2 • PCI DSS v3 6.5.3 • PCI DSS v3 6.5.4 • PCI DSS v3 6.5.5 • PCI DSS v3 6.5.6 • PCI DSS v3 6.5.7 • PCI DSS v3 6.5.8 • PCI DSS v3 6.5.9 • PCI DSS v3 6.5.10 • 1 TAC § 390.2(a)(3)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System	Processing PHI: Yes - AND -, Accessible from the Internet: Yes, Number of

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	Users: > 5,500, Number of Transactions Per Day: > 85,000, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Applications that store, process or transmit covered information shall undergo application vulnerability testing at least annually by a qualified party, with an emphasis on input validation controls. Application input validation testing shall be automated through use of tools or other non-manual methods. Additionally, the organization shall: i. develop and document system and information integrity policy and procedures; ii. disseminate the system and information integrity policy and procedures to appropriate areas within the organization; iii. assign responsible parties within the organization to annually review system and information integrity policy and procedures; and iv. update the system and information integrity policy and procedures when organizational review indicates updates are required. The information system shall check the validity of organization-defined information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible. For public-facing Web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: i. reviewing applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; ii. installing an automated technical solution that detects and prevents Web-based attacks (e.g., a Web-application firewall) in front of public-facing Web applications, to continually check all traffic.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 SI-10 (HIGH) • IRS Pub 1075 v2014 9.3.17.7 • IRS Pub 1075 v2014 9.4.2 (E.10) • MARS-E v1 SI-10 • NRS 603A.215.1 • PCI DSS v3 6.6

Level 3 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

FTI Requirements

FTI Custodians:	Web-enabled application software in a data warehouse shall: i. Prohibit generic meta-characters in input data; ii. Arrange to have all database queries constructed with parameterized stored; iii. procedures to prevent structured query language (SQL) injection; iv. Protect any variable used in scripts to prevent direct OS command attacks; v. Arrange to have all comments removed for any code passed to the browser; vi. Prevent users from seeing any debugging information on the client; and vii. Undergo a check before production deployment to ensure that all sample, test, and unused files have been removed from the production system.

Control Reference: 10.c Control of Internal Processing

Control Specification:	Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
Factor Type:	System
Topics:	Documentation and Records Risk Management and Assessments
Products and Services Guide:	10.c Control of Internal Processing

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System	Applicable to all systems

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 Regulatory Factors:	Subject to Joint Commission Accreditation
Level 1 Implementation:	For organizations doing system development (e.g., applications, databases) the design and implementation of applications shall ensure that the risks of processing failures leading to a loss of integrity are minimized. Data integrity controls shall address: i. the use of add, modify, and delete functions to implement changes to data; ii. the procedures to prevent programs running in the wrong order or running after failure of prior processing (see 9.a); iii. the use of appropriate programs to recover from failures to ensure the correct processing of data; and iv. protection against attacks using buffer overruns/overflows. A checklist for validation checking shall be prepared, activities documented, and the results shall be kept secure. The checks to be incorporated include the following and can be manual: i. session or batch controls, to reconcile data file balances after transaction updates; ii. balancing controls, to check opening balances against previous closing balances, namely: a. run-to-run controls b. file update totals c. program-to-program controls iii. validation of system-generated input data (see 10.b); iv. checks on the integrity, authenticity or any other security feature of data or software downloaded, or uploaded, between central and remote computers; v. hash totals of records and files; vi. checks to ensure that application programs are run at the correct time; vii. checks to ensure that programs are run in the correct order and terminate in case of a failure, and that further processing is halted until the problem is resolved; and viii. creating an automated log of the activities involved in the processing (see 9.aa).
Level 1 Control Standard Mapping:	• CSA SA-04 • HIPAA § 164.312(c)(1) • HIPAA § 164.312(c)(2) • HIPAA § 164.312(e)(2)(i) • ISO/IEC 27002-2005 12.2.2 • ISO 27799-2008 7.9.2.3 • JCAHO IM.04.01.01, EP 1 • NIST Cybersecurity Framework PR.DS-6 • NIST SP 800-53 R4 SI-10

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST SP 800-53 R4 DI-2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Accessible from the Internet: Yes, Number of Users: > 5,500, Number of Transactions Per Day: > 85,000, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: Applications shall undergo application vulnerability testing annually by a qualified party, focusing on the use of add, modify, and delete functions to implement changes to data, and attacks using buffer overruns/overflows. Automated validation checks shall be conducted at an organization-defined frequency but no less than monthly and/or after organization-defined security-relevant events through use of tools or other non-manual methods to detect unauthorized changes to information, firmware and software. Information system flaws shall be identified, reported, and corrected. All appropriate information pertaining to the discovered flaws in the information system, including the cause of the flaws, mitigation activities, and lessons learned shall be collected. The organization shall perform an integrity check of software and information daily. The organization incorporates the detection of unauthorized security-relevant changes to the information system into the organization incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes. The information system shall provide notification of failed security verification tests. Automated validation checks shall be conducted at an organization-defined frequency but no less than monthly and/or after organization-defined security-relevant events automated through use of tools or other non-manual methods to detect unauthorized changes to information, firmware and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	software. The organization shall employ integrity verification tools to detect unauthorized, security-relevant configuration changes to software and information.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 SC-24 (HIGH) • CMSRs 2013v2 SI-6 (HIGH) • CMSRs 2013v2 SI-6(2) (HIGH) • CMSRs 2013v2 SI-7 (HIGH) • CMSRs 2013v2 SI-7(1) (HIGH) • CMSRs 2013v2 SI-7(2) (HIGH) • CMSRs 2013v2 SI-7(5) (HIGH) • CMSRs 2013v2 SI-7(7) (HIGH) • CMSRs 2013v2 SI-10 (HIGH) • ISO 27799-2008 7.9.2.1 • IRS Pub 1075 v2014 9.3.17.7 • MARS-E v1 CM-6(3) • MARS-E v1 SI-7 • MARS-E v1 SI-7(1) • MARS-E v1 SI-9 • MARS-E v1 SI-10 • NIST SP 800-53 R4 SI-7 • NIST SP 800-53 R4 SI-7(1) • NIST SP 800-53 R4 SI-7(7) • NRS 603A.215.1 • PCI DSS v3 6.6

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The information system automatically implements security safeguards (defined in the applicable security plan) when integrity violations are discovered.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The information system shall fail to a known secure state of all failures preserving the maximum amount of state information in failure. The information system shall verify the correct operation of system security functions upon system startup and restart, upon command by a user with appropriate privilege, periodically on a monthly basis, provide notification of failed automated security tests, notify system administration when anomalies are discovered, and shut down, restart or perform some other defined alternative action (defined in the applicable security plan) when anomalies are discovered. The information system shall provide automated mechanisms to support the management of distributed security function testing. The organization shall employ automated tools that provide notification to designated individuals (defined in the applicable security plan) upon discovering discrepancies during integrity verification.

Provider Requirements

Providers:	Health information systems processing personal health information shall: i. ensure that each subject of care can be uniquely identified within the system; ii. be capable of merging duplicate or multiple records if it is determined that multiple records for the same subject of care have been created unintentionally or during a medical emergency.

Control Reference: 10.d Message Integrity

Control Specification:	Requirements for ensuring authenticity and protecting message integrity in applications shall be identified and controls implemented.
Factor Type:	System
Topics:	Cryptography

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Processing PHI: Yes -AND-, Accessible from the Internet: Yes, Exchanges Data with a Business Partner: Yes
Level 1 Regulatory Factors:	Subject to Joint Commission Accreditation, Subject to FISMA Compliance, Subject to CMS Minimum Security Requirements (High), Subject to MARS-E

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Requirements, Subject to FTI Compliance
Level 1 Implementation:	The information system provides mechanisms to protect the authenticity of communications sessions. Cryptographic controls (see 10.f) shall be implemented to ensure message authentication and integrity for covered information applications. The system shall implement one of the following integrity protection algorithms: i. HMAC-SHA-1 ii. HMAC-MD5 See NIST SP800-52 Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations for more information on implementing integrity checks for information transmissions.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 SC-8 (HIGH) • CMSRs 2013v2 SC-23 (HIGH) • Guidance to render PHI unusable, unreadable, or indecipherable (1)(ii) • HIPAA § 164.312(c)(1) • HIPAA § 164.312(c)(2) • HIPAA § 164.312(e)(2)(i) • IRS Pub 1075 v2014 9.3.16.14 • ISO/IEC 27002-2005 12.2.3 • ISO 27799-2008 7.9.2.4 • JCAHO IM.02.01.03, EP 6 • MARS-E v1 SC-8 • MARS-E v1 SC-23 • NIST Cybersecurity Framework PR.DS-2 • NIST Cybersecurity Framework PR.DS-5 • NIST Cybersecurity Framework PR.DS-6 • NIST SP800-53r3 SC-8 • NIST SP 800-53 R4 SC-23 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 10.e Output Data Validation

Control Specification:	Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
Factor Type:	System
Topics:	None

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	Subject to Joint Commission Accreditation
Level 1 Implementation:	For organizations doing system development (e.g., applications, databases) output validation shall be manually or automatically performed. Output validation shall include: i. plausibility checks to test whether the output data is reasonable; ii. reconciliation control counts to ensure processing of all data; iii. providing sufficient information for a reader (i.e. to ensure that the patient they are treating matches the information retrieved, or subsequent processing system to determine the accuracy,

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	completeness, precision, and classification of the information); iv. procedures for responding to output validation tests; v. defining the responsibilities of all personnel involved in the data output process; and vi. creating an automated log of activities in the data output validation process.
Level 1 Control Standard Mapping:	• CSA SA-04 • CSA SA-05 • ISO/IEC 27002-2005 12.2.4 • ISO 27799-2008 7.9.2.5 • JCAHO IM.04.01.01, EP 1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Accessible from the Internet: Yes, Number of Users: > 5,500, Number of Transactions Per Day: > 85,000, Number of Interfaces to Other Systems: > 25
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: Output validation checks shall be automated.
Level 2 Control Standard Mapping:	None

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Objective Name: 10.03 Cryptographic Controls

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Objective:	To protect the confidentiality, authenticity and integrity of information by cryptographic means. A policy shall be developed on the use of cryptographic controls. Key management should be in place to support the use of cryptographic techniques.

Control Reference: 10.f Policy on the Use of Cryptographic Controls

Control Specification:	A policy on the use of cryptographic controls for protection of information shall be developed and implemented, and supported by formal procedures. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Communications and Transmissions Cryptography Media and Assets Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to the State of Nevada Security of Personal Information Requirements, Subject to Joint Commission Accreditation
Level 1 Implementation:	The cryptographic policy shall address the use of encryption for protection of covered information transported by mobile or removable media, devices or across communication lines. Supporting cryptographic procedures shall address: i. the required level of protection (e.g., the type and strength of the encryption algorithm required); and ii. specifications for the effective implementation throughout the organization (i.e. which solution is used for which business processes). The cryptographic policy shall be aligned with the organization's data protection and privacy policy (see 06.d)
Level 1 Control Standard Mapping:	• CSA IS-18 • Guidance to render PHI unusable, unreadable, or indecipherable (1) • HIPAA 164.312(a)(2)(iv) • HIPAA 164.312(e)(2)(ii)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• JCAHO IM.02.01.03, EP 2 • NIST Cybersecurity Framework PR.DS-1 • NIST Cybersecurity Framework PR.DS-2 • NRS 603A.215.2.a • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: When implementing the organization's cryptographic policy and procedures, the regulations and national restrictions that apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information (see 06.f) shall be adhered to.
Level 2 Control Standard Mapping:	• COBIT 4.1 DS5.8 • COBIT 5 DSS05.03 • ISO/IEC 27002-2005 12.3.1 • ISO/IEC 27002:2013 10.1.1 • ISO 27799-2008 7.9.3.1 • NIST Cybersecurity Framework ID.GV-3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation:	No additional requirements

Control Reference: 10.g Key Management

Control Specification:	Key management shall be in place to support the organizations use of cryptographic techniques. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Authentication Cryptography Physical and Facility Security Requirements (Legal and Contractual) Services and Acquisitions

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to the State of Nevada Security of Personal Information Requirements, Subject to Joint Commission Accreditation
Level 1 Implementation:	All cryptographic keys shall be protected against modification, loss, and destruction. In addition, secret and private keys shall require protection against unauthorized disclosure. Cryptographic keys shall be limited to the fewest number of custodians necessary. Equipment used to generate, store and archive keys shall be physically protected. If manual clear-text key-management procedures are used, the organization shall split knowledge and control of keys (e.g., requiring multiple individuals knowing only their respective key comprising the whole key).
Level 1 Control Standard Mapping:	• CSA IS-19 • Guidance to render PHI unusable, unreadable, or indecipherable (1) • HIPAA § 164.312(a)(2)(iv) • HIPAA § 164.312(e)(2)(ii) • JCAHO IM.02.01.03, EP 6 • NIST Cybersecurity Framework PR.DS-1 • NIST Cybersecurity Framework PR.DS-2 • NRS 603A.215.2.a • PCI DSS v3 3.5.2 • PCI DSS v3 3.6.6

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: A key management system shall be based on a formal set of standards, procedures, and secure methods for: i. verifying user identity prior to generating new certificates or keys; ii. generating keys for different cryptographic systems and different applications; iii. generating and obtaining public key certificates; iv. distributing keys to intended users, including how keys should be activated when received; v. storing keys in the fewest possible locations, including how authorized users obtain access to keys; vi. changing or updating keys including rules on when keys should be changed and how this will be done: a. as deemed necessary and recommended by the associated application; and b. at least annually; vii. revoking keys including how keys should be withdrawn or deactivated (e.g., when keys have been compromised or suspected to have been compromised or when a user leaves an organization, in which case keys shall also be archived); viii. recovering keys that are lost or corrupted as part of business continuity management (e.g., for recovery of encrypted information); ix. archiving keys (e.g., for information archived or backed up); x. destroying keys; and xi. logging and auditing of key management related activities.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	In order to reduce the likelihood of compromise, activation, and deactivation, dates for keys shall be defined so that the keys can only be used for a limited period of time. This period of time shall be dependent on the circumstances under which the cryptographic control is being used, and the perceived risk, however shall not exceed one year. The organization shall prevent the unauthorized substitution of keys. Cryptographic key custodians shall be required to sign a form stating they understand and accept their key custodian responsibilities. In addition to securely managing secret and private keys, the authenticity of public keys shall also be addressed. This authentication process shall be done using public key certificates issued by a certification authority, which shall be a recognized organization with suitable controls and procedures in place to provide the required degree of trust.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 SC-12 (HIGH) • CMSRs 2013v2 SC-12(1) (HIGH) • CMSRs 2013v2 SC-17 (HIGH) • COBIT 4.1 DS5.8 • COBIT 5 DSS05.03 • IRS Pub 1075 v2014 9.3.16.8 • IRS Pub 1075 v2014 9.3.16.11 • ISO/IEC 27002-2005 12.3.2 • ISO/IEC 27002:2013 10.1.2 • ISO 27799-2008 7.9.3.2 • MARS-E v1 SC-12 • MARS-E v1 SC-17 • NIST SP 800-53 R4 SC-12 • NIST SP 800-53 R4 SC-17 • NRS 603A.215.1 • PCI DSS v3 3.5 • PCI DSS v3 3.5.1 • PCI DSS v3 3.5.3 • PCI DSS v3 3.6 • PCI DSS v3 3.6.1 • PCI DSS v3 3.6.2 • PCI DSS v3 3.6.3 • PCI DSS v3 3.6.4 • PCI DSS v3 3.6.5 • PCI DSS v3 3.6.7 • PCI DSS v3 3.6.8 • PCI DSS v3 8.2.2

Level 3 Implementation Requirements

Level 3	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Organizational Factors:	
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization maintains availability of information in the event of the loss of cryptographic keys by users. Mechanisms are employed to: i. prohibit the use of encryption keys that are not recoverable by authorized personnel, ii. require senior management approval to authorize recovery of keys by other than the key owner, and iii. comply with approved cryptography standards specified in 10.f.

PCI-DSS Requirements

PCI Data:	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: i. Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. ii. Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device). iii. As at least two full-length key components or key shares, in accordance with an industry- accepted method.

Objective Name: 10.04 Security of System Files

Control Objective:	To ensure the security of system files, access to system files and program source code shall be controlled, and IT projects and support activities conducted in a secure manner.

Control Reference: 10.h Control of Operational Software

Control Specification:	There shall be procedures in place to control the installation of software on operational systems.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	*Required for HITRUST Certification 2015
Factor Type:	System
Topics:	Authorization Documentation and Records Maintenance Monitoring Services and Acquisitions Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	To minimize the risk of corruption to operational systems, the following procedures shall be implemented to control changes: i. the updating of the operational software, applications, and program libraries shall only be performed by authorized administrators; and ii. operational systems shall only hold approved programs or executable code (i.e. no development code or compilers). Vendor supplied software used in operational systems shall be maintained at a level supported by the supplier. The organization shall maintain information systems according to a current baseline configuration and configure system security parameters to prevent misuse. Any decision to upgrade to a new release shall take into account the business requirements for the change, and the security and privacy impacts of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version). If systems or system components in production are no longer supported by the developer, vendor, or manufacturer, the organization must show evidence of a formal migration plan approved by management to replace the system or system components.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 CM-4 (HIGH) • CMSRs 2013v2 CM-6 (HIGH) • CMSRs 2013v2 CM-6 (1) (HIGH) • CMSRs 2013v2 CM-6 (2) (HIGH)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• CSA RM-05 • IRS Pub 1075 v2014 9.3.5.4 • IRS Pub 1075 v2014 9.3.5.6 • IRS Pub 1075 v2014 9.3.15.10 • IRS Pub 1075 v2014 9.4.18 • MARS-E v1 CM-4 • MARS-E v1 CM-6 • NIST Cybersecurity Framework PR.IP-1 • NIST Cybersecurity Framework PR.IP-3 • NIST SP 800-53 R4 CM-4 • NIST SP 800-53 R4 CM-6 • PCI DSS v3 2.2.4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 500, Third Party Support (Vendor Access or Maintenance): Yes, Number of Transactions Per Day: > 6,750
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Compliance
Level 2 Implementation:	Level 1 plus: Applications and operating system software shall only be implemented after successful testing. The tests shall include tests on usability, security, and effects on other systems, and shall be carried out on separate systems. It shall be ensured that all corresponding program source libraries have been updated. A configuration control system shall be used to keep control of all implemented software as well as the system documentation. A rollback strategy shall be in place before changes are implemented. An audit log shall be maintained of all updates to operational program libraries. Previous versions of application software shall be retained as a contingency measure. Old versions of software shall be archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data is retained in archive or as dictated by the organization's data retention policy.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Physical or logical access shall only be given to suppliers for support purposes when necessary, and with management approval. The supplier's activities shall be monitored.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CM-2(3) (HIGH) • CMSRs 2013v2 CM-3 (HIGH) • IRS Pub 1075 v2014 9.3.5.3 • IRS Pub 1075 v2014 9.4.17 • ISO/IEC 27002-2005 12.4.1 • ISO/IEC 27002:2013 12.5.1 • ISO 27799-2008 7.9.4.1 • MARS-E v1 CM-3 • NIST Cybersecurity Framework PR.DS-7 • NIST SP 800-53 R4 CM-2(3) • NIST SP 800-53 R4 CM-3 • NRS 603A.215.1 • PCI DSS v3 2.2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	Processing PHI: Yes - AND -, Number of Users: > 5,500, Number of Transactions Per Day: > 85,000
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization shall employ automated mechanisms to respond to unauthorized changes to authorization and/or auditing systems and system security-related configuration baselines, log files, and critical system files (including sensitive system and application executables, libraries, and configurations).

FTI Requirements

FTI Custodians:	To access FTI using a Web browser, the agency must determine the business use of Java and approve the use of Java if is required for core business functions.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 10.i Protection of System Test Data

Control Specification:	Test data shall be selected carefully, and protected and controlled in non-production environments.
Factor Type:	System
Topics:	Authorization Data Loss Prevention Documentation and Records User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The use of operational databases containing covered information for non-production (e.g., testing) purposes shall be avoided. If covered or otherwise sensitive information must be used for testing purposes, all sensitive details and content shall be removed or modified beyond recognition (e.g., de-identified) before use. The following requirements shall be applied to protect data, when used for testing purposes: i. the access control procedures, which apply to operational application systems, shall also apply to test application systems (see 1.0); ii. there shall be formal management authorization for instances where operational information is copied to a non-production application system; and iii. operational information and test accounts shall be erased from a test application system immediately after the testing is complete.
Level 1 Control Standard Mapping:	• CSA DG-06 • ISO 27799-2008 7.9.4.2 • NIST Cybersecurity Framework PR.AC-1 • NIST Cybersecurity Framework PR.AC-2 • NIST Cybersecurity Framework PR.AC-3 • NIST Cybersecurity Framework PR.AC-4 • NIST Cybersecurity Framework PR.AC-5

Level 2 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Accessible from the Internet: Yes, Number of Users: > 500, Number of Transactions Per Day: > 6,750
Level 2 Regulatory Factors:	Subject to FTI Compliance
Level 2 Implementation:	Level 1 plus: The following requirements shall be applied to protect operational data, when used for testing purposes: i. security controls shall be equally applied to non-production environments as production environments; ii. all instances where covered information is used in non-production environments must be documented; and iii. the copying, use and erasure of operational information shall be logged to provide an audit trail. Personnel developing and testing system code shall not have access to production libraries.
Level 2 Control Standard Mapping:	• ISO/IEC 27002-2005 12.4.2 • ISO/IEC 27002:2013 14.3.1 • IRS Pub 1075 v2014 9.4.6 • NIST Cybersecurity Framework PR.DS-1 • NIST Cybersecurity Framework PR.DS-2 • NIST Cybersecurity Framework PR.PT-1 • NIST Cybersecurity Framework PR.PT-3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

FTI Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

FTI Custodians:	The agency avoids (limits) the use of live FTI—primarily unmodified, non-sanitized data extracted from taxpayer files that identifies specific individual or corporate taxpayers and includes taxpayer information or tax return information—in pre-production (e.g., test environments) and is not authorized unless specifically approved by the Office of Safeguards through the submission of a Data Testing Request (DTR) form. The DTR must provide a detailed explanation of the safeguards in place to protect the data and the necessity for using live data during testing. The organization revises its Need and Use Justification to cover this use of IRS data if not already addressed. For one-time testing efforts, the agency detects the FTI from systems and databases upon completion of testing efforts and electronically clears the hard drive(s) of the test systems prior to repurposing the system for other agency testing efforts. The agency agrees with the Office of Safeguards to a specific duration for ongoing test activities.

Control Reference: 10.j Access Control to Program Source Code

Control Specification:	Access to program source code shall be restricted.
Factor Type:	System
Topics:	Authorization Policies and Procedures Risk Management and Assessments Services and Acquisitions User Access

Level 1 Implementation Requirements

Level 1 Organizational Factors:	None
Level 1 System Factors:	Applicable to all systems
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Access to program source code (code written by programmers, which is compiled and linked to create executables) and associated items (such as designs, specifications, verification plans and validation plans) shall be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes. An organization will not have access to source code for the majority of purchased software applications, and this requirement does not apply.
Level 1 Control	• NIST Cybersecurity Framework PR.DS-5

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Standard Mapping	• NIST Cybersecurity Framework PR.PT-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	Processing PHI: Yes - AND -, Accessible from the Internet: Yes, Number of Users: > 500, Number of Transactions Per Day: > 6,750
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: Program source code shall be stored in a central location, specifically in program source libraries. The following requirements shall be implemented (see 1.0) to control access to such program source libraries in order to reduce the potential for corruption of computer programs: i. program source libraries shall not be held in operational systems; ii. the program source code and the program source libraries shall be managed according to established procedures; iii. access to program source libraries shall be strictly limited to that which is needed to perform a job function; iv. the updating of program source libraries and associated items, and the issuing of program sources to programmers shall only be performed after appropriate authorization has been received; v. program listings shall be held in a secure environment (see 9.r); vi. an audit log shall be maintained of all accesses to program source libraries; and vii. maintenance and copying of program source libraries shall be subject to strict change control procedures (see 10.k).
Level 2 Control Standard Mapping:	• CSA IS-33 • ISO/IEC 27002-2005 12.4.3 • ISO/IEC 27002:2013 9.4.5 • ISO 27799-2008 7.9.4.3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Objective Name: 10.05 Security in Development and Support Processes

Control Objective:	To ensure the security of application system software and information through the development process, project and support environments shall be strictly controlled.

Control Reference: 10.k Change Control Procedures

Control Specification:	The implementation of changes, including patches, service packs, and other updates and modifications, shall be controlled by the use of formal change control procedures.
Factor Type:	Organizational
Topics:	Documentation and Records IT Organization and Management Roles and Responsibilities Requirements (Legal and Contractual)

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Project and support environments shall be strictly controlled. Managers responsible for application systems shall also be responsible for the security of the project or support environment. They shall ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.
Level 1 Control Standard Mapping:	• ISO/IEC 27002-2005 12.5.2 • ISO/IEC 27001:2013 8.1 • ISO/IEC 27002:2013 14.2.3 • NIST Cybersecurity Framework PR.IP-3

Level 2 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance
Level 2 Implementation:	Level 1 plus: A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance shall be developed. Configuration management policy/procedures shall be reviewed/updated annually. The organization shall develop, document, and implement a configuration management plan for the information system that: i. addresses roles, responsibilities, and configuration management processes and procedures; ii. defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and iii. establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items. Formal change control procedures shall be documented and enforced in order to minimize the corruption of information systems. Introduction of new systems and major changes to existing systems shall follow a formal process of documentation, specification, testing, quality control, and managed implementation. This process shall include a risk assessment, analysis of the security and privacy impacts of changes, and specification of security controls needed. This process shall also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained. Installation checklists shall be used to validate the configuration of servers, devices and appliances. In addition, vulnerability port scanning shall occur on server and desktops to ensure configuration meets minimum security standards.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The change procedures shall minimally include: i. ensuring changes are submitted by authorized users; ii. maintaining a record of agreed authorization levels; iii. reviewing controls and integrity procedures to ensure that they will not be compromised by the changes; iv. identifying all software, information, database entities, and hardware that require amendment; v. obtaining formal approval for detailed proposals requesting changes before work commences; vi. documenting unit, system, and user acceptance testing procedures in an environment segregated from development and production; vii. ensuring all system components are tested and approved (operating system, utility, applications) prior to promotion to production; viii. documenting rollback procedures for failed changes; ix. ensuring authorized users accept changes prior to implementation based on the results on the completion of each change of testing the changes; x. ensuring that the system documentation set is updated and that old documentation is archived or disposed of; xi. maintaining a version control for all software updates; xii. maintaining an audit trail of all change requests and approvals; and xiii. ensuring that operating documentation (see 9.a) and user procedures are changed as necessary to remain appropriate. If development is outsourced, change control procedures to address security are included in the contract(s). Automated updates shall not be used on critical systems, as some updates may cause critical applications to fail. The organization shall require the developer of the information system, system component, or information system service to track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel or roles.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CM-1 (HIGH) • CMSRs 2013v2 CM-3 (HIGH) • CMSRs 2013v2 CM-3(1) (HIGH) • CMSRs 2013v2 CM-3(2) (HIGH) • CMSRs 2013v2 CM-4 (HIGH) • CMSRs 2013v2 CM-4(1) (HIGH) • CMSRs 2013v2 CM-4(2) (HIGH) • CMSRs 2013v2 CM-5 (HIGH) • CMSRs 2013v2 CM-5(1) (HIGH) • CMSRs 2013v2 CM-5(3) (HIGH) • CMSRs 2013v2 CM-9 (HIGH) • CMSRs 2013v2 SA-10 (HIGH) • CSA RM-02 • IRS Pub 1075 v2014 9.3.5.1 • IRS Pub 1075 v2014 9.3.5.3

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• IRS Pub 1075 v2014 9.3.5.4 • IRS Pub 1075 v2014 9.3.5.5 • IRS Pub 1075 v2014 9.3.5.9 • IRS Pub 1075 v2014 9.3.15.8 • ISO/IEC 27002-2005 12.5.1 • ISO/IEC 27002-2005 12.5.3 • ISO/IEC 27002:2013 14.2.2 • ISO/IEC 27002:2013 14.2.4 • ISO 27799-2008 7.9.5 • MARS-E v1 CM-1 • MARS-E v1 CM-3 • MARS-E v1 CM-3(2) • MARS-E v1 CM-4 • MARS-E v1 CM-4(1) • MARS-E v1 CM-4(2) • MARS-E v1 CM-5 • MARS-E v1 CM-9 • MARS-E v1 SA_10 • NIST Cybersecurity Framework ID.AM-6 • NIST Cybersecurity Framework ID.RA-4 • NIST Cybersecurity Framework ID.RA-5 • NIST Cybersecurity Framework PR.AT-3 • NIST Cybersecurity Framework PR.IP-2 • NIST Cybersecurity Framework PR.PT-3 • NIST SP 800-53 R4 CM-1 • NIST SP 800-53 R4 CM-3 • NIST SP 800-53 R4 CM-3(2) • NIST SP 800-53 R4 CM-4 • NIST SP 800-53 R4 CM-5 • NIST SP 800-53 R4 CM-9 • NIST SP 800-53 R4 SA-10 • NRS 603A.215.1 • PCI DSS v3 6.4

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Pharmaceutical Companies: > 70,000,000 Prescriptions Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: The organization shall develop, document, and maintain under configuration control, a current baseline configuration of the information system. The organization shall review and update the baseline configuration of the information system: i. at least once every six (6) months; ii. when required due to critical security patches, upgrades and emergency changes (e.g., unscheduled changes, system crashes, replacement of critical hardware components), major system changes/upgrades; a. as an integral part of information system component installations, b. upgrades, and c. supporting baseline configuration documentation reflects ongoing implementation of operational configuration baseline updates, either directly or by policy. The organization shall i. establish and documents mandatory configuration settings for information technology products employed within the information system using the latest security configuration baselines established by the HHS, U.S. Government Configuration Baselines (USGCB), and the National Checklist Program (NCP) defined by NIST SP 800-70 Rev. 2 that reflect the most restrictive mode consistent with operational requirements; ii. identify, document, and approve exceptions from the mandatory established configuration settings for individual components within the information system based on explicit operational requirements; and iii. monitor and control changes to the configuration settings in accordance with organizational policies and procedures. The organization shall employ automated mechanisms to centrally manage, apply, and verify configuration settings. The organization shall employ automated mechanisms to respond to unauthorized changes to network and system security-related configuration settings. The information system enforces access restrictions and supports auditing of the enforcement actions.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 CM-2 (HIGH) • CMSRs 2013v2 CM-2(1) (HIGH)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• CMSRs 2013v2 CM-2(2) (HIGH) • CMSRs 2013v2 CM-2(3) (HIGH) • CMSRs 2013v2 CM-2(6) (HIGH) • CMSRs 2013v2 CM-5(2) (HIGH) • CMSRs 2013v2 CM-6 (HIGH) • CMSRs 2013v2 CM-6(1) (HIGH) • CMSRs 2013v2 CM-6(2) (HIGH) • IRS Pub 1075 v2014 9.3.5.2 • IRS Pub 1075 v2014 9.3.5.6 • IRS Pub 1075 v2014 9.4.2 (E.10) • IRS Pub 1075 v2014 9.4.3 • IRS Pub 1075 v2014 9.4.5 • IRS Pub 1075 v2014 9.4.8 • IRS Pub 1075 v2014 9.4.9 • IRS Pub 1075 v2014 9.4.11 • IRS Pub 1075 v2014 9.4.13 • IRS Pub 1075 v2014 9.4.14 • IRS Pub 1075 v2014 9.4.15 • IRS Pub 1075 v2014 9.4.16 • IRS Pub 1075 v2014 9.4.17 • IRS Pub 1075 v2014 9.4.18 • MARS-E v1 CM-2 • MARS-E v1 CM-2(1) • MARS-E v1 CM-6 • NIST Cybersecurity Framework PR.IP-1 • NIST Cybersecurity Framework DE.CM-1 • NIST Cybersecurity Framework DE.CM-7 • NIST SP 800-53 R4 CM-2 • NIST SP 800-53 R4 CM-2(1) • NIST SP 800-53 R4 CM-6

CMS Contractor Requirements

CMS Contractors:	HHS-specific minimum security configurations shall be used for the following Operating System (OS) and Applications: i. HHS FDCC Windows XP Standard ii. HHS FDCC Windows Vista Standard iii. Blackberry Server iv. Websense. For all other OS's and applications, and to resolve configuration conflicts among multiple security guidelines, the CMS hierarchy for implementing security configuration guidelines is as follows: i. USGCB ii. NIST National Checklist Program (NCP); Tier IV, then Tier III, Tier II, and Tier I, in descending order.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

iii. Defense Information Systems Agency (DISA) STIGs
iv. National Security Agency (NSA) STIGs
v. If formal government-authored checklists do not exist, then organizations are encouraged to use vendor or industry group (such as The Center for Internet Security [CIS]) checklists.
vi. In situations where no guidance exists, coordinate with CMS for guidance. CMS shall collaborate within CMS and the HHS Cybersecurity Program, and other OPDIVs through the HHS Continuous Monitoring and Risk Scoring (CMRS) working group to establish baselines and communicate industry and vendor best practices.
vii. All deviations from existing USGCB, NCP, DISA and/or NSA configurations must be documented in an approved HHS waiver (available at http://intranet.hhs.gov/it/cybersecurity/policies_by_document_type/index.html#Policy%20and%20Standard%20Waiver), with copies submitted to the Department.

The organization shall maintain a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

The organization shall employ automated mechanisms to enforce access restrictions and support auditing of the enforcement actions. The organization reviews information system changes weekly and when indications so warrant to determine whether unauthorized changes have occurred.

The information system shall prevent the installation of network and server software and firmware components without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.

The organization shall employ automated mechanisms to:
i. document proposed changes to the information system;
ii. notify designated approval authorities and request change approval;
iii. highlight approvals that have not been approved or disapproved in a timely manner;
iv. prohibit change until designated approvals are received; and
v. document all changes to the information system; and
vi. notify identified stakeholders when approved changes to the information system are completed.

The organization shall analyze changes to the information system in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization shall employ automated mechanisms to maintain up-to-date, complete, accurate, and readily available baseline configuration of the information system.

FTI Requirements

FTI Custodians:	All agency information systems used for receiving, processing, storing and transmitting FTI must be hardened (securely configured) using, when available for the specific technologies used, Safeguard Computer Security Evaluation Matrices (SCSEMs) publicly available on the Office of Safeguards IRS.gov website, keyword: safeguards program. This requirement includes but is not limited to: i. email servers and clients; ii. integrated voice response (IVR) operating system (OS) and associated software for each system within the architecture providing FTI to a customer; iii. mobile devices; iv. multi-functional devices (MFDs); v. storage area network (SAN) components; vi. virtual desktop infrastructure (VDI) components such as the hypervisor and management console; vii. virtual machine (VM) and hypervisor/host OS software for each system within a virtual environment; viii. voice over IP (VoIP) systems; ix. each system within the architecture that receives, processes, stores or transmits FTI through a Web-based system or Website; and x. each system within the agency's network that transmits FTI through a wireless local area network (WLAN). In particular, to use a virtual environment that receives, processes, stores or transmits FTI, the VMs and hypervisor/host operating system (OS) software for each system within the virtual environment that receives, processes, stores, or transmits FTI must be configured such that: i. special VM functions available to system administrators in a virtualized environment that can leverage the shared memory space in a virtual environment between the hypervisor and VM are disabled, and ii. virtual systems are configured to prevent FTI from being dumped outside of the VM when system errors occur. The organization shall provide a detailed definition of configurations and the functions of the hardware and software involved in a data warehouse. To access FTI using a Web browser, the agency must meet the following mandatory requirements: i. private browsing must be enabled on the Web browser and configured to delete temporary files and cookies upon exiting the

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	session; ii. Security enhancements, such as pop-up blocker and content filtering, must be enabled on the Web browser; iii. Configure the designated Web browser in accordance to the principle of least functionality and disable items, such as third-party add-ons.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	Security configuration guidelines may be developed by different federal agencies, so it is possible that a guideline could include configuration information that conflicts with another agency or the organization's guideline. To resolve configuration conflicts among multiple security guidelines, the organization's hierarchy for implementing all security configuration guidelines is as follows: i. NIST ii. CMS iii. DISA iv. OMB

Control Reference: 10.l Outsourced Software Development

Control Specification:	Outsourced software development shall be supervised and monitored by the organization. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Documentation and Records Media and Assets Requirements (Legal and Contractual) Services and Acquisitions

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to MARS-E Requirements, Subject to FTI Compliance
Level 1 Implementation:	Where software development is outsourced, the following points shall be addressed contractually (either in a contract or Security Service Level Agreement): i. licensing arrangements, code ownership, and intellectual property

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	rights (see 6.b); ii. certification of the quality and accuracy of the work carried out; iii. escrow arrangements in the event of failure of the third party; iv. rights of access for audit of the quality and accuracy of work done; v. contractual requirements for quality and security functionality of code; and vi. testing before installation to detect malicious code.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 SA-11 (HIGH) • CMSRs 2013v2 SA-13 (HIGH) • IRS Pub 1075 v2014 9.3.15.9 • ISO/IEC 27002-2005 12.5.5 • ISO/IEC 27001:2013 8.1 • ISO/IEC 27002:2013 14.2.7 • ISO 27799-2008 7.9.5 • MARS-E v1 SA-11 • NIST Cybersecurity Framework ID.BE-1 • NIST Cybersecurity Framework ID.RA-3 • NIST Cybersecurity Framework ID.RA-6 • NIST Cybersecurity Framework DE.CM-4 • NIST Cybersecurity Framework PR.AT-3 • NIST SP 800-53 R4 SA-11 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Pharmaceutical Companies: > 10,000,000 Prescriptions Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to CMS Minimum Security Requirements (High)
Level 2 Implementation:	Level 1 plus: The development of all outsourced software shall be supervised and monitored by the organization and must include security requirements, independent security review of the outsourced environment by a certified

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	individual, certified security training for outsourced software developers, and code reviews. Certification for the purposes of this control shall be defined as a legally recognized license or certification in the legislative jurisdiction the organization outsourcing the development has chosen as its domicile. The organization shall protect against supply chain threats by employing best practices and methodologies, such as including the security organization in all IT procurement considerations.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 SA-12 (HIGH) • CSA RM-04 • NIST Cybersecurity Framework PR.IP-2 • NIST Cybersecurity Framework DE.CM-6 • NIST SP 800-53 R4 SA-12

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization shall protect against supply chain threats by employing best practices and methodologies, wherever possible, selecting components that have been previously reviewed by other government entities (e.g., National Information Assurance Partnership [NIAP]) as part of a comprehensive, defense-in-breadth information security strategy. The organization shall require that all information systems meet a level of security functionality and security assurance that is sufficient to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system by establishing system trustworthiness objectives as part of the security authorization by following the CMS eXpedited Life Cycle (XLC).

Objective Name: 10.06 Technical Vulnerability Management

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Objective:	To reduce the risks resulting from exploitation of published technical vulnerabilities, technical vulnerability management shall be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness.

Control Reference: 10.m Control of Technical Vulnerabilities

Control Specification:	Timely information about technical vulnerabilities of information systems being used shall be obtained; the organization's exposure to such vulnerabilities evaluated; and appropriate measures taken to address the associated risk. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Incident Response IT Organization and Management Roles and Responsibilities Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g., what software is installed on what systems) and the person(s) within the organization responsible for the software. Appropriate, timely action shall be taken in response to the identification of potential technical vulnerabilities. Once a potential technical vulnerability has been identified, the organization shall identify the associated risks and the actions to be taken. Such action shall involve patching of vulnerable systems and/or applying other controls.
Level 1 Control Standard Mapping:	• (State of Mass.) 201 CMR 17.04(6) • NIST Cybersecurity Framework ID.RA-1 • NIST Cybersecurity Framework ID.RA-2 • NIST Cybersecurity Framework ID.RA-4 • NIST Cybersecurity Framework ID.RA-6

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST Cybersecurity Framework RS.MI-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: The organization shall define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required. Information resources (including tools and vulnerability mailing lists/other information sources), that will be used to identify relevant technical vulnerabilities and to maintain awareness about them, shall be identified for software and other technology (based on the asset inventory list, see 7.a). These information resources shall be updated based on changes in the inventory, or when other new or useful resources are found. Internal and external vulnerability assessments of sensitive information systems (e.g., systems containing covered information, cardholder data) and networked environments shall be performed on a quarterly basis, and after any significant change in the network (e.g., new system component installations, changes in network topology, firewall rule modifications, product upgrades), by a qualified individual. These tests shall include both network- and application-layer tests. The action taken shall be carried out according to the controls related to change management (see 10.k) or by following information security incident response procedures (see 11.c). If a patch is available, change control procedures for the implementation of security patches and software modifications shall be followed (see 09.b). This shall include assessing the risks associated with installing the patch shall be assessed (the risks posed by the vulnerability should be

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	compared with the risk of installing the patch). Patches shall be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated. If no patch is available, other controls shall be applied including: i. documentation of impact. ii. documented change approval by authorized parties. iii. functionality testing to verify that the change does not adversely impact the security of the system. iv. back-out procedures. v. turning off services or capabilities related to the vulnerability. vi. adapting or adding access controls (e.g., firewalls) at network borders (see 9.m). vii. increased monitoring to detect or prevent actual attacks. viii. raising awareness of the vulnerability. An audit log shall be kept for all procedures undertaken. Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. The risk ranking shall consider the CVSS score, classification of the vendor supplied patch, and/or the classification and criticality of the affected system. The technical vulnerability management process shall be evaluated on a quarterly basis in order to ensure its effectiveness and efficiency. Systems at high risk shall be addressed first. A configuration standard shall be developed for all system components (workstations, databases, servers, applications). The standards shall be hardened to address, to the extent practical, all known security vulnerabilities. The organizations configuration standards shall be consistent with industry-accepted system hardening standards, including: i. Center for Internet Security (CIS) ii. International Organization for Standardization (ISO) iii. SysAdmin Audit Network Security (SANS) iv. Institute National Institute of Standards Technology (NIST) Enable only necessary and secure services, protocols, daemons, etc., as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, SSL, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.).
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CM-7 (HIGH) • IRS Pub 1075 v2014 9.3.5.7 • IRS Pub 1075 v2014 9.3.14.3 • ISO/IEC 27002-2005 12.6.1 • ISO/IEC 27002:2013 12.6.1 • ISO 27799-2008 7.9.5

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• MARS-E v1 CM-7 • MARS-E v1 RA-5 • NIST Cybersecurity Framework ID.AM-6 • NIST Cybersecurity Framework ID.RA-5 • NIST Cybersecurity Framework PR.IP-12 • NIST Cybersecurity Framework PR.PT-1 • NIST Cybersecurity Framework DE.CM-8 • NIST Cybersecurity Framework RS.CO-3 • NIST SP 800-53 R4 CM-7 • NIST SP 800-53 R4 RA-5 • NIST SP 800-53 R4 SI-2 • PCI DSS v3 2.2 • PCI DSS v3 2.2.2 • PCI DSS v3 2.2.3 • PCI DSS v3 6.1 • PCI DSS v3 6.4.5 • PCI DSS v3 6.4.5.1 • PCI DSS v3 6.4.5.2 • PCI DSS v3 6.4.5.3 • PCI DSS v3 6.4.5.4 • PCI DSS v3 11.2 • PCI DSS v3 11.2.1 • PCI DSS v3 11.2.2 • PCI DSS v3 11.2.3

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: Perform an enterprise security posture review annually. The organization shall employ automated mechanisms monthly to determine the state of information system components with regard to flaw remediation. Vulnerability scanning tools shall include the capability to readily update the information system vulnerabilities scanned. The organization scans for vulnerabilities in the information system and hosted applications within

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	every thirty (30) days and when new vulnerabilities potentially affecting the systems and networked environments are identified and reported. The organization updates the list of information system vulnerabilities scanned within every thirty (30) days or when new vulnerabilities are identified and reported. The organization includes privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities to facilitate more thorough scanning.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 CA-8 (HIGH) • CMSRs 2013v2 RA-5 (HIGH) • CMSRs 2013v2 RA-5(1) (HIGH) • CMSRs 2013v2 RA-5(2) (HIGH) • CMSRs 2013v2 RA-5(4)(HIGH) • CMSRs 2013v2 RA-5(5) (HIGH) • CMSRs 2013v2 SI-2 (HIGH) • CMSRs 2013v2 SI-2(1) (HIGH) • CMSRs 2013v2 SI-2(2) (HIGH) • CSA IS-20 • IRS Pub 1075 v2014 9.3.14.3 • IRS Pub 1075 v2014 9.3.17.2 • IRS Pub 1075 v2014 9.4.9 • IRS Pub 1075 v2014 9.4.14 • IRS Pub 1075 v2014 9.4.15 • IRS Pub 1075 v2014 9.4.16 • IRS Pub 1075 v2014 9.4.17 • MARS-E v1 RA-5 • MARS-E v1 RA-5(1) • MARS-E v1 SI-2 • MARS-E v1 SI-2(1) • MARS-E v1 SI-2(2) • NIST Cybersecurity Framework PR.PT-3 • NIST SP800-53 R4 RA-5(1) • NIST SP 800-53 R4 RA-5(2) • NIST SP 800-53 R4 RA-5(5) • NIST SP 800-53 R4 SI-2(2) • NRS 603A.215.1 • PCI DSS v3 6.2 • PCI DSS v3 11.3 • PCI DSS v3 11.3.1 • PCI DSS v3 11.3.2 • PCI DSS v3 11.3.3 • PCI DSS v3 11.3.4

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

CMS Requirements

CMS Contractors:	The organization shall correct identified information system flaws on production equipment within ten (10) business days and all others within thirty (30) calendar days. A risk-based decision is documented through the configuration management process in the form of written authorization from the CMS CIO or his/her designated representative (e.g., the system data owner or CMS CISO) if a security patch is not applied to a security-based system or network. For critical infrastructure and systems (e.g., public-facing, internet accessible), critical security patches shall be applied within one month of release. For less-critical infrastructure and systems (e.g., only accessible internally) or for non-critical security patches, patches shall be applied within three months of release. The organization shall attempt to determine what information about the information system environment is discernible by adversaries and subsequently takes appropriate corrective action to limit discoverable system information. The organization shall centrally manage the flaw remediation process and shall install software updates automatically where possible. The organization conducts both internal and external penetration testing, within every three hundred sixty-five (365) days, on defined information systems or system components (defined in the applicable security plan).

FTI Requirements

FTI Custodians:	At a minimum, systems containing FTI shall be scanned quarterly to identify any vulnerability in the information system. Multifunction Device (MFD) firmware is supported by the vendor and is kept up-to-date with the most current firmware available. Vulnerability assessments must be performed on systems in a virtualized environment prior to system implementation and frequently thereafter. To use a VoIP network that provides FTI to a customer, each system within the agency's network that transmits FTI to an external customer through the VoIP network is subject to frequent vulnerability testing. To use an external Web-based system or website that provides FTI over the Internet to a customer, the agency must ensure each system within the

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	architecture that receives, processes, stores, or transmits FTI to an external customer through the Web-based system or website is subject to frequent vulnerability testing To access FTI using a Web browser, the agency must install vendor-specified security patches and hot fixes regularly for the Web browser, add-ons, and Java. To use FTI in an 802.11 WLAN, the agency must conduct vulnerability scanning as part of periodic technical security assessments for the organization's WLAN.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	Perform external network penetration testing and conduct enterprise security posture review as needed but no less than once within every three-hundred-sixty-five (365) days, in accordance with organizational IS procedures.

PCI-DSS Requirements

PCI Data:	Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel. Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. Implement a methodology for penetration testing that: i. is based on industry-accepted penetration testing approaches (e.g., NIST SP 800-115), ii. includes coverage for the entire card data environment (CDE) perimeter and critical systems, iii. includes testing from both inside and outside the network, iv. includes testing to validate any segmentation and scope-reduction controls, v. defines application-layer penetration tests to include, at a minimum, the vulnerabilities identified in 10.b, level 1 (reference PCI DSS v3 6.5), vi. defines network-layer penetration tests to include components that support network functions as well as operating systems,

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	vii. includes review and consideration of threats and vulnerabilities experienced in the last 12 months, and viii. specifies retention of penetration testing results and remediation activities' results. If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Category: 11.0 - Information Security Incident Management

Objective Name: 11.01 Reporting Information Security Incidents and Weaknesses

Control Objective:	To ensure information security events and weaknesses associated with information systems are handled in a manner allowing timely corrective action to be taken.

Control Reference: 11.a Reporting Information Security Events

Control Specification:	Information security events shall be reported through appropriate communications channels as quickly as possible. All employees, contractors and third party users shall be made aware of their responsibility to report any information security events as quickly as possible. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Awareness and Training Incident Response IT Organization and Management Roles and Responsibilities Personnel Policies and Procedures Risk Management and Assessments Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	Formal information security event reporting procedures to support the corporate direction (policy) shall be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event, treating the breach as discovered, and the timeliness of reporting and response. With the importance of Information Security Incident Handling, a policy shall be established to set the direction of management.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	A point of contact shall be established for the reporting of information security events. It shall be ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response. Employees and other workforce members, including third parties, are able to freely report security weaknesses (real and perceived) without fear of repercussion. The organization shall implement an insider threat program that includes a cross-discipline insider threat incident handling team. Organizations shall ensure workforce members do not interfere with federal or state investigations or disciplinary proceedings by willful misrepresentation or omission of facts or by the use of threats or harassment against any person. Organizations shall ensure violations of these requirements are incorporated into disciplinary procedures (see 02.f).
Level 1 Control Standard Mapping:	• (State of Mass.) 201 CMR 17.03(2)(j) • CMSRs 2013v2 PM-12 (HIGH) • CSA IS-23 • HIPAA § 164.308(a)(1)(ii)(D) • HIPAA § 164.308(a)(6)(i) • HIPAA § 164.308(a)(6)(ii) • HIPAA § 164.314(a)(2)(i) • HIPAA § 164.404(a)(2) • HIPAA § 164.410(a)(1) • HIPAA § 164.410(a)(2) • IRS Pub 1075 v2014 9.3.8.1 • MARS-E v1 IR-1 • NIST Cybersecurity Framework RS.CO-2 • NIST SP 800-53 R4 IR-1 • NIST SP 800-53 R4 PM-12 • PCI DSS v3 12.10 • PCI DSS v3 12.10.3 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(2) • 1 TAC § 390.2(a)(4)(A)(ix) • 1 TAC § 390.2(a)(4)(B)(xvi) • 1 TAC § 390.2(a)(4)(B)(xviii)(III) • 1 TAC § 390.2(a)(4)(B)(xviii)(IV)

Level 2 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to the State of Nevada Security of Personal Information Requirements, Subject to FISMA Compliance, Subject to CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The policy shall refer to the specific procedures and programs to address incidents and also refer to a forensic program. The organization shall institute a mechanism to anonymously report security issues. Procedures shall be developed to provide for the definition and assessment of information security incidents (e.g., an event/incident classification scale to decide whether an event classifies as an incident), roles and responsibilities, incident handling, reporting and communication processes. They shall also state the requirements for an incident handling team to address regulatory requirements, third party relationships, and the handling of third party security breaches. Reports and communications shall be made without unreasonable delay and no later than 60 days after the discovery of the incident, unless otherwise stated by law enforcement in writing or orally. If the statement is made in writing, the notification shall be delayed for the time specified by the official. If the statement is made orally, the organization shall document the statement, including the identity of the official making the statement, and delay the notification temporarily and no longer than 30 days from the date of the oral statement, unless a written statement from a law enforcement official is submitted during that time. All employees, contractors and third party users shall receive mandatory incident response training to ensure they are aware of their responsibilities to report any information security events as quickly as possible, the procedure for reporting information security events and the point(s) of contact. The reporting procedures shall include: i. feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed; ii. information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

actions in case of an information security event including:
    a. the correct behavior to be undertaken in case of an information security event and noting all important details (e.g., type of non-compliance or breach) occurring malfunction, messages on the screen, strange behavior, immediately; and
    b. not carrying out any own action, but immediately reporting to the point of contact;

iii. reference to an established formal disciplinary process for dealing with employees, contractors or third party users who commit security breaches;
iv. communication with each individual affected by, or who is reasonably believed to have been affected by, the incident;
v. communication with business associate(s) identifying each individual affected by, or who is reasonably believed to have been affected by, the incident;
vi. communicating incidents to local and federal law enforcement agencies; and
vii. automated work flow processes for incident management, reporting and resolution.

Reports to external organizations, individuals or federal or state agencies shall include:

i. a brief description of what happened;
ii. the date of the breach;
iii. the date of the discovery of the breach;
iv. a description of the types of information that were involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, disability code);
v. the recommended steps external entities should take to protect themselves from potential harm resulting from the breach;
vi. a brief description of the steps the organization is taking to:
    a. investigate the breach,
    b. mitigate damages, and
    c. protect against any further breaches
vii. contact procedures to ask questions or learn additional information, which shall include:
    a. a toll-free telephone number,
    b. an e-mail address,
    c. Web site, or
    d. postal address.

Reports to the individuals affected by the incident shall be provided with notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or by electronic mail if specified as a preference by the individual. Organizations may provide notifications by telephone in cases deemed urgent by the organization. In the case that there

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	are 10 or more individuals for whom there is insufficient or out-of-date contact information (including a phone number, email address, or any other form of appropriate communication), a conspicuous posting shall be placed on the home page of the Web site of the organization involved for a period of 90 days. A toll-free phone number shall be also be posted that remains active for at least 90 days where an individual can learn whether the individual's information may be included in the breach. For fewer than 10 individuals, a substitute form of notice reasonably calculated to reach the individual shall be provided, except when there is insufficient or out-of-date information that precludes written notification to the next of kin or personal representative. The organization shall also notify, without unreasonable delay, any consumer reporting agency of the time the notification is distributed and the content of the notification. If more than 500 residents of such State or jurisdiction were, or are reasonably believed to have been, affected by the breach, notice shall be immediately provided to the federal government (to publicly disclose) and prominent media outlets. The notification to individuals shall be written in plain language (e.g., at an appropriate reading level, using clear language and syntax, and not include any extraneous material that might diminish the message it is trying to convey). Alerts from the organization's intrusion-detection and intrusion-prevention systems shall be utilized for reporting information security events.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 IR-1 (HIGH) • CMSRs 2013v2 IR-6 (HIGH) • CMSRs 2013v2 IR-6(1) (HIGH) • COBIT 4.1 DS5.6 • COBIT 5 DSS02.01 • HIPAA § 164.404(a)(1) • HIPAA § 164.404(b) • HIPAA § 164.404(c)(1) • HIPAA § 164.404(c)(2) • HIPAA § 164.404(d)(1) • HIPAA § 164.404(d)(2) • HIPAA § 164.404(d)(3) • HIPAA § 164.406(a) • HIPAA § 164.406(b) • HIPAA § 164.406(c) • HIPAA § 164.408(a) • HIPAA § 164.408(b) • HIPAA § 164.408(c) • HIPAA § 164.410(b) • HIPAA § 164.410(c)(1) • HIPAA § 164.410(c)(2)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• HIPAA § 164.412 • HIPAA § 164.414(b) • IRS Pub 1075 v2014 9.3.8.6 • IRS Pub 1075 v2014 9.4.2 (E.10) • IRS Pub 1075 v2014 10.1 • IRS Pub 1075 v2014 10.2 • IRS Pub 1075 v2014 10.4 • ISO/IEC 27002-2013 A.16.1.4 • ISO 27799-2008 7.10.1 • MARS-E v1 IR-6 • MARS-E v1 IR-6(1) • NIST Cybersecurity Framework ID.GV-3 • NIST SP 800-53 R4 IR-6 • NIST SP 800-53 R4 IR-6(1) • NIST SP 800-53 R4 AR-6 • NRS 603A.215.1 • NRS 603A.220.1 • NRS 603A.220.2 • NRS 603A.220.3 • PCI DSS v3 12.10.1 • PCI DSS v3 12.10.4 • PCI DSS v3 12.10.5 • 1 TAC § 390.2(a)(3) • 1 TAC § 390.2(a)(4)(B)(xiii)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	Level 2 plus: A duress alarm shall be provided whereby a person under duress can indicate such problems. The procedures for responding to duress alarms shall reflect the high risk situation such alarms are indicating. An information security assessment shall be made either on all incidents or

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	on a sample, to further validate the effectiveness or otherwise of established controls and of the risk assessment that lead to them. Examples include: i. a break-in leading to theft of IT hardware, resulting in a confidentiality breach; or ii. a fire could be set to disguise misuse of IT equipment.
Level 3 Control Standard Mapping:	• ISO/IEC 27002-2005 13.1.1 • ISO/IEC 27002:2013 16.1.2 • NIST Cybersecurity Framework PR.IP-7

CMS Contractor Requirements

CMS Contractors:	The organization shall require personnel to report suspected security incidents to the organizational incident response capability within timeframe established in the current CMS Incident Handling and Breach Notification Standard.

FTI Requirements

FTI Custodians:	Any data incident potentially involving FTI must immediately be reported to the appropriate Treasury Inspector General for Tax Administration (TIGTA) field office and the IRS Office of Safeguards immediately, but no later than 24-hours after identification of a possible issue involving FTI. To notify the Office of Safeguards, the agency must document the specifics of the incident known at that time into a data incident report, including but not limited to: i. Name of agency and agency Point of Contact for resolving data incident with contact information ii. Date and time of the incident iii. Date and time the incident was discovered iv. How the incident was discovered v. Description of the incident and the data involved, including specific data vi. elements, if known vii. Potential number of FTI records involved; if unknown, provide a range if possible viii. Address where the incident occurred ix. IT involved (e.g., laptop, server, mainframe) x. Do not include any FTI in the data Incident report xi. Reports must be sent electronically and encrypted via IRS-approved encryption techniques. Use the term data incident report in the subject line of the email. The agency must inform the Office of Safeguards of notification activities

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	undertaken before release to individuals impacted by a breach of FTI. In addition, the agency must inform the Office of Safeguards of any pending media releases, including sharing the text, prior to distribution.

PCI-DSS Requirements

PCI Data:	The organization shall designate specific personnel to be available on a 24/7 basis to respond to alerts.

Texas Covered Entities

Texas Covered Entities:	Organizations or persons that conduct business in Texas and own or license computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized persons. The disclosure shall be made as quickly as possible, except at the request of a law enforcement agency that determines notification will impede a criminal investigation, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system. If the individual is a resident of a state that requires a person or entity to provide notice of a breach of system security, notice of the breach of system security may be provided in accordance with that state's law. A person or entity may give notice by providing: i. Written notice at the last known address; ii. Electronic notice, if the notice is provided in accordance with 15 U.S.C. Section 7001; or iii. If the person or entity required to give notice demonstrates that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person or entity does not have sufficient contact information, the notice may be given by: a. Electronic mail, if the person or entity has electronic mail addresses for the affected persons; b. Conspicuous posting of the notice on the person's or entity's Website; c. Notice published in or broadcast on major statewide media; or d. Notwithstanding the methods described above, a person or entity who maintains the their own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice under this section complies with this section if the person or entity notifies affected persons in accordance with that policy.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	If a person or entity is required by this section to notify more than 10,000 persons of a breach of system security at one time, the person or entity shall also notify each consumer reporting agency, as defined by 15 U.S.C. Section 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The person or entity shall provide the notice required by this subsection without unreasonable delay. Organizations shall incorporate procedures in their security and privacy incident response programs to assist with investigations conducted by TX state and local registrars or their representatives, when it is believed a person or persons intentionally or knowingly supplied false information, or intentionally or knowingly creates a false record, or directs another person to supply information or create a false record, for use in the preparation of a certificate, record or report, or amendment covered under THSC Title 3, as provided by THSC §§ 195.002 thru 195.005. Private psychiatric (mental) hospitals, crisis stabilization units and other mental health facilities shall incorporate procedures in their security and privacy incident response programs to assist with state investigations, including the release of otherwise confidential information related to the investigation, as required under THSC § 577.

Control Reference: 11.b Reporting Security Weaknesses

Control Specification:	All employees, contractors, and third party users of information systems and services shall be required to note and report any observed or suspected security weaknesses in systems or services.
Factor Type:	Organizational
Topics:	Awareness and Training Incident Response Personnel Third Parties and Contractors

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Compliance
Level 1 Implementation:	All employees, contractors and third party users shall report incident and event information, including violations of workforce rules of behavior and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	acceptable use agreement, to their management and/or directly to their service provider as quickly as possible in order to prevent information security incidents. The reporting mechanism shall be easy to use, widely accessible, and available to all employees. Employees, contractors and third party users shall be informed (including but not limited to policies and procedures and incident response training) that they shall not, in any circumstances, attempt to prove a suspected weakness.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PL-4 (HIGH) • CMSRs 2013v2 SI-2 (HIGH) • IRS Pub 1075 v2014 9.3.12.3 • IRS Pub 1075 v2014 9.3.17.2 • ISO/IEC 27002-2005 13.1.2 • ISO/IEC 27002:2013 16.1.3 • ISO 27799-2008 7.10.1 • MARS-E v1 PL-4 • MARS-E v1 SI-2 • NIST SP 800-53 R4 PL-4 • NIST SP 800-53 R4 SI-2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FTC Red Flags Rule Compliance
Level 2 Implementation:	Level 1 plus: All employees, contractors and third party users shall report potential weaknesses that may lead to organization or system breaches, or lead to identity theft for the following categories: i. alerts, notifications, or other warnings received from third parties, state or federal agencies or service providers, such as fraud detection services; ii. the presentation of suspicious documents associated with an individual's account; iii. the presentation of suspicious covered information (e.g., an address change that is inconsistent with existing information); iv. the unusual use of, or other suspicious activity related to, an

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	individual's account; and v. notice from customers, law enforcement authorities, or other persons regarding possible weaknesses in connection with accounts held by the organization.
Level 2 Control Standard Mapping:	• 16 CFR Part §681 Appendix A II(c) • 1 TAC § 390.2(a)(3)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Objective Name: 11.02 Management of Information Security Incidents and Improvements

Control Objective:	To ensure a consistent and effective approach to the management of information security incidents.

Control Reference: 11.c Responsibilities and Procedures

Control Specification:	Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Awareness and Training Contingency Planning Documentation and Records Incident Response IT Organization and Management Roles and Responsibilities Policies and Procedures Third Parties and Contractors

Level 1 Implementation Requirements

Level 1	Applicable to all organizations

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Organizational Factors:	
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FTC Red Flags Rule Compliance, Subject to State of Massachusetts Data Protection Act
Level 1 Implementation:	The organization shall implement a formal incident response program. The program shall be established to handle different types of information security incidents including: i. information system failures and loss of service; ii. malicious code; iii. denial of service; iv. errors resulting from incomplete or inaccurate business data; v. breaches of confidentiality and integrity; vi. disclosures of unprotected health information; vii. misuse of information systems; viii. identity theft; and ix. unauthorized wireless access points. In addition to normal contingency plans, the program shall also cover: i. analysis and identification of the cause of the incident; ii. containment; iii. increased monitoring of system use; iv. planning and implementation of corrective action to prevent recurrence including a. changing of password or security codes; b. changing of devices that permit access to the organization's systems or network; c. modifying or terminating an account of individuals involved directly or indirectly by the incident (e.g., employees, third party, contractors, customers); and v. assigning a single point of contact for the organization responsible for sharing information and coordinating responses.
Level 1 Control Standard Mapping:	• 16 CFR Part §681 Appendix A IV(a) • 16 CFR Part §681 Appendix A IV(b) • 16 CFR Part §681 Appendix A IV(c) • 16 CFR Part §681 Appendix A IV(d) • 16 CFR Part §681 Appendix A IV(e) • 16 CFR Part §681 Appendix A IV(f) • 16 CFR Part §681 Appendix A IV(g) • 16 CFR Part §681 Appendix A IV(h) • 16 CFR Part §681 Appendix A IV(i) • COBIT 4.1 DS5.6 • COBIT 5 DSS02.01 • CSA IS-22

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• HIPAA § 164.308(a)(1)(ii)(D) • HIPAA § 164.308(a)(6)(i) • HIPAA § 164.308(a)(6)(ii) • HIPAA § 164.404(a)(1) • NIST Cybersecurity Framework PR.IP-9 • NIST Cybersecurity Framework RS.AN-4 • NIST Cybersecurity Framework RS.MI-1 • NIST Cybersecurity Framework RS.MI-2 • PCI DSS v3 11.1.2 • PCI DSS v3 12.10 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • (State of Mass.) 201 CMR 17.03(2)(j) • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(3)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to the State of Nevada Security of Personal Information Requirements
Level 2 Implementation:	Level 1 plus: Audit trails and similar evidence shall be collected and secured, as appropriate, for: i. internal problem analysis; ii. use as forensic evidence in relation to a potential breach of contract or regulatory requirement or in the event of civil or criminal proceedings (e.g., under computer misuse or data protection legislation); and iii. negotiating for compensation from software and service suppliers. A log shall be maintained of any incident occurring and annually submit such a log to the federal government. Action to recover from security breaches and correct system failures shall be carefully and formally controlled. The procedures shall ensure that:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

i. only clearly identified and authorized personnel are allowed access to live systems and data;
ii. all emergency actions taken are documented in detail;
iii. emergency action is reported to management and reviewed in an orderly manner; and
iv. the integrity of business systems and controls is confirmed with minimal delay.

The organization shall disseminate incident response policy and procedures to appropriate elements within the organization. Responsible parties within the organization on a pre-defined frequency shall review incident response policy and procedures. The organization shall update incident response policy and procedures when organizational review indicates updates are required.

The organization shall respond to incidents in accordance with the documented procedures, which should include but not be limited to the following:

i. collecting evidence as soon as possible after the occurrence (see 11.e);
ii. conducting information security forensic analysis, as required (see 11.e);
iii. escalation, as required;
iv. ensuring that all involved response activities are properly logged for later analysis;
v. communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need-to-know;
vi. dealing with information security weakness(es) found to cause or contribute to the incident; and
vii. once the incident has been successfully addressed, formally closing and recording it.

The organization shall coordinate incident response testing with organization elements responsible for related plans.

Incident Response Testing and Exercises procedures shall include:

i. defining incident response tests/exercises, including automated mechanisms;
ii. defining the frequency of incident response tests/exercises;
iii. testing the incident response capability for the information system using organization-defined tests/exercises in accordance with organization-defined frequency; and
iv. documenting the results of incident response tests/exercises.

In addition to reporting of information security events and weaknesses, the monitoring of systems, alerts, and vulnerabilities shall be used to detect information security incidents.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization shall test and/or exercise the incident response capability for the information system within every three hundred sixty-five (365) days using reviews, analyses, and simulations to determine the incident response effectiveness and documents the results. A formal test need not be conducted if the organization actively exercises its response capability using real incidents.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 IR-1 (HIGH) • CMSRs 2013v2 IR-3 (HIGH) • CMSRs 2013v2 IR-3(2) (HIGH) • IRS Pub 1075 v2014 9.3.8.1 • IRS Pub 1075 v2014 9.3.8.3 • IRS Pub 1075 v2014 10.3 • ISO/IEC 27002-2005 13.2.1 • ISO/IEC 27002:2013 16.1.1 • ISO/IEC 27002:2013 16.1.5 • ISO 27799-2008 7.10.2.1 • MARS-E v1 IR-1 • MARS-E v1 IR-3 • NIST Cybersecurity Framework PR.AT-1 • NIST Cybersecurity Framework DE.AE-3 • NIST Cybersecurity Framework RS.CO-3 • NIST Cybersecurity Framework RS.CO-4 • NIST Cybersecurity Framework RS.IM-2 • NIST Cybersecurity Framework RS.RP-1 • NIST SP 800-53 R4 IR-1 • NIST SP 800-53 R4 IR-3 • NIST SP 800-53 R4 IR-3(2) • NIST SP 800-53 R4 SE-2 • NRS 603A.215.1 • NRS 603A.220.4.a • NRS 603A.220.4.b • NRS 603A.220.4.c.1 • NRS 603A.220.4.c.2 • NRS 603A.220.4.c.3 • NRS 603A.220.6 • PCI DSS v3 12.10.1 • PCI DSS v3 12.10.2 • PCI DSS v3 12.10.4

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Pharmaceutical Companies: > 70,000,000 Prescriptions Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >,0600,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 3 Implementation:	Level 2 plus: The organization shall: i. develop an incident response plan that: a. provides the organization with a roadmap for implementing its incident response capability; b. describes the structure and organization of the incident response capability; c. provides a high-level approach for how the incident response capability fits into the overall organization; d. meets the unique requirements of the organization, which relate to mission, size, structure, and functions; e. defines reportable incidents; f. provides metrics for measuring the incident response capability within the organization. g. defines the resources and management support needed to effectively maintain and mature an incident response capability; and h. is reviewed and approved by designated officials within the organization; ii. distribute copies of the incident response plan to incident response personnel and organizational elements; iii. review the incident response plan within every three hundred sixty-five (365) days; iv. revise the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and v. communicate incident response plan changes to incident response personnel and organizational elements. The organization shall provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The incident response support resource shall be an integral part of the organization's incident response capability. The organization shall track and document information system security incidents on an ongoing basis. The organization shall promptly report

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	incident information to appropriate authorities. The types of incident information reported, the content and timeliness of the reports, and the list of designated reporting shall be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. Weaknesses and vulnerabilities in the information system shall be reported to appropriate organizational officials in a timely manner to prevent security incidents. The organization shall communicate with outside parties regarding the incident. This includes reporting incidents to organizations such as the Federal Computer Incident Response Center (FedCIRC) and the CERT Coordination Center (CERT/CC), contacting law enforcement, and fielding inquiries from the media. The objectives for information security incident management shall be agreed to with management, and it shall be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents. The organization shall employ automated mechanisms to increase the availability of incident response-related information and support.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 IR-5 (HIGH) • CMSRs 2013v2 IR-7 (HIGH) • CMSRs 2013v2 IR-7(1) (HIGH) • CMSRs 2013v2 IR-8 (HIGH) • IRS Pub 1075 v2014 9.3.8.5 • IRS Pub 1075 v2014 9.3.8.7 • IRS Pub 1075 v2014 9.3.8.8 • IRS Pub 1075 v2014 9.3.8.9 • IRS Pub 1075 v2014 9.4.2 (E.10) • IRS Pub 1075 v2014 10.3 • MARS-E v1 IR-5 • MARS-E v1 IR-7 • MARS-E v1 IR-7(1) • MARS-E v1 IR-8 • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework RS.CO-1 • NIST Cybersecurity Framework RS.CO-2 • NIST Cybersecurity Framework RS.CO-5 • NIST Cybersecurity Framework RS.IM-1 • NIST SP 800-53 R4 IR-5 • NIST SP 800-53 R4 IR-7 • NIST SP 800-53 R4 IR-7(1) • NIST SP 800-53 R4 IR-8

CMS Contractor Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

CMS Contractors:	The organization shall employ automated mechanisms to assist in the tracking of security incidents. The organization shall distributes copies of the incident response plan to: i. CMS Chief Information Security Officer; ii. CMS Chief Information Officer; iii. Information System Security Officer; iv. CMS Office of the Inspector General/Computer Crimes Unit; v. All personnel within the organization Incident Response Team; vi. All personnel within the PII Breach Response Team; and vii. All personnel within the organization Operations Centers. The organization shall communicate incident response plan changes to the organizational elements listed above for distribution.

FTI Requirements

FTI Custodians:	The agency must track and document all physical and information system security incidents potentially affecting the confidentiality of FTI. The agency must not wait to conduct an internal investigation to determine if FTI was involved in an unauthorized disclosure or data breach. If FTI may have been involved, the agency must contact TIGTA and the IRS immediately. The agency will cooperate with TIGTA and Office of Safeguards investigators, providing data and access as needed to determine the facts and circumstances of the incident. The organization exercises its response to unauthorized FTI access and reporting unauthorized FTI access to IRS and TIGTA. Agencies must perform tabletop exercises using scenarios that include a breach of FTI and should test the agency's incident response policies and procedures. All employees and contractors with significant FTI incident response capabilities, including technical personnel responsible for maintaining consolidated data centers and off-site storage, must be included in tabletop exercises. Each tabletop exercise must produce an after-action report to improve existing processes, procedures, and policies. The agency shall provide an incident response support resource that offers advice and assistance to users of the federal tax information and any information system containing federal tax information for the handling and reporting of security incidents. The support resource is an integral part of the agency's incident response capability. The agency shall agency develop, document, and maintain a current incident response plan that describes the structure and organization of the incident response capability and includes incident response procedures specific to

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	FTI, including any data warehousing environment that contains FTI. The agency must respond to information spills by: i. Identifying the specific information involved in the information system ii. contamination; iii. Alerting authorized incident response personnel of the information spill using a method of communication not associated with the spill; iv. Isolating the contaminated information system or system component; v. Eradicating the information from the contaminated information system or component; and vi. v. Identifying other information systems or system components that may have been subsequently contaminated.

Control Reference: 11.d Learning from Information Security Incidents

Control Specification:	There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
Factor Type:	Organizational
Topics:	Awareness and Training Incident Response IT Organization and Management Roles and Responsibilities

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The information gained from the evaluation of information security incidents shall be used to identify recurring or high impact incidents.
Level 1 Control Standard Mapping:	• CSA IS-25 • HIPAA § 164.308(a)(1)(ii)(D) • HIPAA § 164.308(a)(6)(ii) • ISO/IEC 27002-2005 13.2.2 • ISO/IEC 27002:2013 16.1.6 • ISO 27799-2008 7.10.2.2 • NIST Cybersecurity Framework DE.AE-1 • NIST Cybersecurity Framework DE.AE-4 • NIST Cybersecurity Framework RS.AN-2 • NIST Cybersecurity Framework RS.RP-1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to FISMA Compliance, Subject to State of Massachusetts Data Protection Act, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The organization shall: i. implement an incident handling capability for security incidents that includes detection and analysis, containment, eradication, and recovery (including public relations and reputation management); ii. coordinate incident handling activities with contingency planning activities; and iii. incorporate lessons learned from ongoing incident handling activities and industry developments into incident response procedures, training and testing exercises, and implements the resulting changes accordingly. Components shall include: i. policy (setting corporate direction) and procedures defining roles and responsibilities; ii. incident handling procedures (business and technical); iii. communication; iv. reporting and retention; and v. references to vulnerability management program that includes network tools for IPS, IDS, forensics, vulnerability assessments and validation.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 IR-4 (HIGH) • CMSRs 2013v2 IR-4(1) (HIGH) • CMSRs 2013v2 IR-4(4) (HIGH)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• CMSRs 2013v2 IR-5 (HIGH) • CMSRs 2013v2 IR-5(1) (HIGH) • IRS Pub 1075 v2014 9.3.8.4 • IRS Pub 1075 v2014 10.3 • MARS-E v1 IR-4 • MARS-E v1 IR-4(1) • MARS-E v1 IR-5 • NIST Cybersecurity Framework ID.AM-6 • NIST Cybersecurity Framework DE.AE-2 • NIST Cybersecurity Framework DE.AE-3 • NIST Cybersecurity Framework RS.CO-3 • NIST Cybersecurity Framework RS.CO-4 • NIST Cybersecurity Framework RS.AN-1 • NIST Cybersecurity Framework RS.AN-3 • NIST Cybersecurity Framework RS.MI-1 • NIST Cybersecurity Framework RS.MI-2 • NIST Cybersecurity Framework RS.IM-1 • NIST Cybersecurity Framework RS.IM-2 • NIST Cybersecurity Framework RC.IM-1 • NIST Cybersecurity Framework RC.IM-2 • NIST Cybersecurity Framework RC.RP-1 • NIST Cybersecurity Framework RC.CO-1 • NIST Cybersecurity Framework RC.CO-2 • NIST Cybersecurity Framework RC.CO-3 • NIST SP 800-53 R4 IR-4 • NIST SP 800-53 R4 IR-4(1) • NIST SP 800-53 R4 IR-5 • NRS 603A.215.1 • PCI DSS v3 12.10.6 • (State of Mass.) 201 CMR 17.03(2)(j)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

CMS Contractor Requirements

CMS Contractors:	The organization shall implement an incident handling capability using the current CMS Incident Handling and Breach Notification Standard and Procedures. Relevant information related to a security incident shall be documented according to the current CMS Incident Handling and Breach Notification Standard and Procedures. The organization shall employ automated mechanisms to assist in the collection and analysis of incident information. The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

FTI Requirements

FTI Custodians:	The organization provides specific incident response guidance relative to a data incidents involving FTI. Once the incident has been addressed, the agency will conduct a post-incident review to ensure the incident response policies and procedures provide adequate guidance. Complete SPR section 9.11.5

Control Reference: 11.e Collection of Evidence

Control Specification:	Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented in support of potential legal action in accordance with the rules for evidence in the relevant jurisdiction(s).
Factor Type:	Organizational
Topics:	Documentation and Records Incident Response Requirements (Legal and Contractual) Services and Acquisitions

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	
Level 1 Regulatory Factors:	
Level 1 Implementation:	The organization shall collect, retain, and present evidence to support legal action (either civil or criminal). The evidence that is collected, retained, and presented shall be done in accordance with the laws of the relevant jurisdiction(s).
Level 1 Control Standard Mapping:	• HIPAA § 164.308(a)(6)(ii) • HIPAA § 164.408(c) • HIPAA § 164.414(b) • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework RS.AN-2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to PCI Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements; Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: Internal procedures shall be developed, documented and followed when collecting and presenting evidence for the purposes of disciplinary action handled within an organization. To achieve admissibility of the evidence, the organization shall ensure that their information systems comply with any published standard or code of practice for the production of admissible evidence. The weight of evidence provided shall comply with any applicable requirements. To achieve weight of evidence, the quality and completeness of the controls used to correctly and consistently protect the evidence (i.e. process control evidence) throughout the period that the evidence to be recovered was

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	stored and processed shall be demonstrated by a strong evidence trail established with the following conditions: i. for paper documents: the original is kept securely with a record of the individual who found the document, where the document was found, when the document was found and who witnessed the discovery; any investigation shall ensure that originals are not tampered with. ii. for information on computer media: mirror images or copies (depending on applicable requirements) of any removable media, information on hard disks or in memory shall be taken to ensure availability; the log of all actions during the copying process shall be kept and the process shall be witnessed; the original media and the log (if this is not possible, at least one mirror image or copy) shall be kept securely and untouched. Any forensics work shall only be performed on copies of the evidential material. The integrity of all evidential material shall be protected. Copying of evidential material shall be supervised by trustworthy personnel and information on when and where the copying process was executed, who performed the copying activities and which tools and programs have been utilized shall be logged. Organizations shall incorporate appropriate forensic handling procedures. Forensics can be outsourced or handled in-house. Any type of forensics shall require training, staff and processes for maintaining a proper chain of evidence.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 IR-4 (HIGH) • CSA IS-24 • IRS Pub 1075 v2014 9.3.8.4 • ISO/IEC 27002-2005 13.2.3 • ISO/IEC 27002:2013 16.1.7 • ISO 27799-2008 7.10.2.3 • MARS-E v1 IR-4 • NIST Cybersecurity Framework PR.IP-11 • NIST SP 800-53 R4 IR-4 • NRS 603A.215.1 • PCI DSS v3 A.1.4

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation:	No additional requirements

PCI-DSS Requirements

PCI Data:	A service provider shall protect each organization's hosted environment and data by enabling process to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Category: 12.0 - Business Continuity Management

Objective Name: 12.01 Information Security Aspects of Business Continuity Management

Control Objective:	To ensure that strategies and plans are in place to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Control Reference: 12.a Including Information Security in the Business Continuity Management Process

Control Specification:	A managed program and process shall be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.
Factor Type:	Organizational
Topics:	Contingency Planning Documentation and Records IT Organization and Management Roles and Responsibilities Media and Assets Personnel Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The program and process shall bring together the following key elements of business continuity management: i. identifying all the assets involved in critical business processes; ii. considering the purchase of suitable insurance which may form part of the overall business continuity process, as well as being part of operational risk management; iii. ensuring the safety of personnel and the protection of information assets and organizational property; and

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	iv. formulating and documenting business continuity plans addressing information security requirements in line with the agreed business continuity strategy (see 12.c).
Level 1 Control Standard Mapping:	• CSA RS-01 • HIPAA § 164.308(a)(7)(ii)(B) • HIPAA § 164.308(a)(7)(ii)(C) • HIPAA § 164.308(a)(7)(ii)(D) • HIPAA § 164.308(a)(7)(ii)(E) • HIPAA § 164.310(a)(2)(i) • HIPAA § 164.312(a)(2)(ii) • NIST Cybersecurity Framework ID.AM-5 • NIST Cybersecurity Framework PR.IP-11 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance; Requirements (High)Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements
Level 2 Implementation:	Level 1 plus: The program and process shall bring together the following key elements of business continuity management: i. identifying critical information system assets supporting organizational missions and functions; ii. understanding the risks the organization is facing in terms of likelihood and impact in time, including an identification and prioritization of critical business processes; iii. understanding the impact which interruptions caused by information security incidents are likely to have on the business (it is important that solutions are found that will handle incidents causing smaller impact, as well as serious incidents that could threaten the viability of the organization), and establishing the business objectives of

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	information assets; iv. implementing additional preventive detective controls for the critical assets identified to mitigate risks to the greatest extent possible; v. identifying financial, organizational, technical, and environmental resources to address the identified information security requirements; vi. testing and updating, at a minimum, a section of the plans and processes put in place at least annually; vii. ensuring that the management of business continuity is incorporated in the organization's processes and structure; and viii. assigning responsibility for the business continuity management process at an appropriate level within the organization.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CP-2 (HIGH) • CMSRs 2013v2 CP-2(8) (HIGH) • IRS Pub 1075 v2014 9.3.6.2 • ISO/IEC 27002-2005 14.1.1 • ISO/IEC 27002:2013 17.1.2 • ISO 27799-2008 7.11 • MARS-E v1 CP-2 • NIST Cybersecurity Framework ID.AM-6 • NIST Cybersecurity Framework ID.BE-5 • NIST Cybersecurity Framework PR.IP-9 • NIST Cybersecurity Framework DE.AE-4 • NIST SP 800-53 R4 CP-2 • NIST SP 800-53 R4 CP-2(8)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 12.b Business Continuity and Risk Assessment

Control Specification:	Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.
Factor Type:	Organizational

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Topics:	Contingency Planning IT Organization and Management Roles and Responsibilities Risk Management and Assessments

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to FISMA Compliance, Subject to CMS Minimum Security Requirements (High), Subject to MARS-E Requirements
Level 1 Implementation:	This process shall identify the critical business processes. Information security aspects of business continuity shall be based on identifying events (or sequence of events) that can cause interruptions to the organizations critical business processes (e.g., equipment failure, human errors, theft, fire, natural disasters and acts of terrorism). This shall be followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period. Based on the results of the risk assessment, a business continuity strategy shall be developed to identify the overall approach to business continuity. Once this strategy has been created, endorsement shall be provided by management, and a plan created and endorsed to implement this strategy.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 PM-8 (HIGH) • CSA RS-02 • MARS-E v1 PM-8 • NIST SP 800-53 R4 PM-8 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1) • HIPAA § 164.308(a)(1)(ii)(A) • HIPAA § 164.308(a)(7)(ii)(B) • NIST Cybersecurity Framework ID.BE-2 • NIST Cybersecurity Framework ID.BE-4 • NIST Cybersecurity Framework ID.RA-1 • NIST Cybersecurity Framework ID.RA-3 • NIST Cybersecurity Framework ID.RA-4 • NIST Cybersecurity Framework ID.RA-5

Level 2 Implementation Requirements

Level 2	BioTech Organizations: > $100,000 Spend on Research and Development Per

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Organizational Factors:	Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Implementation:	

Control Reference: 12.c Developing and Implementing Continuity Plans Including Information Security

Control Specification:	Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes. *Required for HITRUST Certification 2015
Factor Type:	Organizational
Topics:	Awareness and Training Contingency Planning Documentation and Records Physical and Facility Security Policies and Procedures

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance
Level 1 Implementation:	A formal, documented contingency planning policy (addressing purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance); and formal, documented procedures (to facilitate the implementation of the contingency planning policy and associated contingency planning controls) shall be developed, disseminated, and reviewed annually. The business continuity planning process shall include the following: i. implementation of the procedures to allow recovery and restoration of business operations and availability of information in required time-scales ii. particular attention shall be given to the assessment of internal and external business dependencies and the contracts in place; iii. documentation of agreed procedures and processes; and iv. testing and updating of at least a section of the plans. The planning process shall focus on the required business objectives (e.g., restoring of specific communication services to customers in an acceptable

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	amount of time). The procedures for obtaining necessary electronic covered information during an emergency shall be defined. The services and resources facilitating this shall be identified, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities. Such fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services. The organization shall coordinate contingency planning activities with incident handling activities. Developed business continuity plans shall: i. identify essential missions and business functions and associated contingency requirements; ii. provide recovery objectives, restoration priorities, and metrics; and iii. address contingency roles, responsibilities, assigned individuals with contact information; iv. address maintaining essential missions and business functions despite an information system disruption, compromise, or failure; v. address eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and vi. be reviewed and approved by designated officials within the organization; and vii. be protected from unauthorized disclosure and modification. Continuity and recovery plans shall be developed and documented to deal with system interruptions and failures caused by malicious code. Business continuity plans shall include recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements. Copies of the business continuity plans shall be distributed to the Information System Security Officer, System Owner, Contingency Plan Coordinator, System Administrator, and Database Administrator (or the organization's functional equivalents). If alternative temporary locations are used, the level of implemented security controls at these locations shall have logical and physical access controls that are equivalent to the primary site, consistent with the HITRUST CSF. The information system implements transaction recovery for systems that are transaction-based.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 CP-1 (HIGH) • CMSRs 2013v2 CP-2 (HIGH) • CMSRs 2013v2 CP-2(1) (HIGH) • CMSRs 2013v2 CP-2(2) (HIGH) • CMSRs 2013v2 CP-2(3) (HIGH)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• CMSRs 2013v2 CP-2(4) (HIGH) • CMSRs 2013v2 CP-2(5) (HIGH) • CMSRs 2013v2 CP-10(2) (HIGH) • CMSRs 2013v2 CP-10(4) (HIGH) • CSA RS-02 • HIPAA § 164.308(a)(7)(i) • HIPAA § 164.308(a)(7)(ii)(A) • HIPAA § 164.308(a)(7)(ii)(B) • HIPAA § 164.308(a)(7)(ii)(C) • HIPAA § 164.308(a)(7)(ii)(D) • HIPAA § 164.308(a)(7)(ii)(E) • HIPAA § 164.310(a)(2)(i) • HIPAA § 164.310(d)(2)(iv) • HIPAA § 164.312(c)(1) • HIPAA § 164.312(a)(2)(ii) • IRS Pub 1075 v2014 9.3.6.1 • IRS Pub 1075 v2014 9.3.6.2 • JCAHO IM.01.01.03, EP 2 • JCAHO IM.01.01.03, EP 4 • MARS-E v1 CP-1 • MARS-E v1 CP-2 • MARS-E v1 CP-2(1) • MARS-E v1 CP-2(2) • MARS-E v1 CP-10(2) • MARS-E v1 CP-10(3) • NIST Cybersecurity Framework ID.AM-5 • NIST Cybersecurity Framework ID.AM-6 • NIST Cybersecurity Framework ID.BE-4 • NIST Cybersecurity Framework ID.BE-5 • NIST Cybersecurity Framework PR.IP-9 • NIST Cybersecurity Framework RC.CO-3 • NIST Cybersecurity Framework RS.CO-4 • NIST Cybersecurity Framework RC.RP-1 • NIST SP 800-53 R4 CP-1 • NIST SP 800-53 R4 CP-2 • NIST SP 800-53 R4 CP-2(1) • NIST SP 800-53 R4 CP-2(3) • NIST SP 800-53 R4 CP-10(2) • NRS 603A.215.1 • PCI DSS v3 12.10.1 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to Joint Commission Accreditation, Subject to FTI Compliance
Level 2 Implementation:	Level 1 plus: The business continuity planning process shall include the following: i. identification and agreement of all responsibilities and business continuity procedures; ii. identification of the acceptable loss of information and services; iii. operational procedures to follow pending completion of response, recovery and restoration including: a. alternative storage and processing site possibilities; and b. emergency power and back-up telecommunications to the primary site. iv. appropriate education of staff in the agreed procedures and processes, including crisis management. Business continuity plans shall address organizational vulnerabilities and therefore may contain covered information that needs to be appropriately protected. Copies of business continuity plans shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. Management shall ensure copies of the business continuity plans are up-to-date and protected with the same level of physical and logical security as applied at the main site. Other material necessary to execute the continuity plans shall also be stored at the remote location. The organization shall identify alternative temporary locations for processing, and the necessary third party service agreements shall be established to allow for the transfer and resumption of information systems operations of critical business functions within a time-period (e.g., priority of service provisions) as defined by a risk assessment (see 12.b). The organization shall identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. The alternate location shall be at a sufficient distance to escape any damage from a disaster at the main site. The type of configuration for the alternate site shall be defined by the risk assessment (see 12.b). Acceptable solutions include:

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	i. cold sites - a facility with adequate space and infrastructure to support the system; ii. warm sites - partially equipped office spaces that contain some or all of the system hardware, software, telecommunications and power sources; iii. hot sites - office spaces configured with all of the necessary system hardware, supporting infrastructure and personnel; and/or iv. mobile sites - self-contained, transportable shells custom-fitted with IT and telecommunications equipment necessary to meet the system requirements. The organization shall identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. The organization develops alternate processing site agreements that contain Priority-of-Service provisions in accordance with the organization's availability requirements, including recovery time objectives (RTOs). The organization shall ensure that the alternate processing site provides information security measures equivalent to that of the primary site.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CP-4(4) (HIGH) • CMSRs 2013v2 CP-6 (HIGH) • CMSRs 2013v2 CP-6(1) (HIGH) • CMSRs 2013v2 CP-6(2) (HIGH) • CMSRs 2013v2 CP-6(3) (HIGH) • CMSRs 2013v2 CP-7 (HIGH) • CMSRs 2013v2 CP-7(1) (HIGH) • CMSRs 2013v2 CP-7(2) (HIGH) • CMSRs 2013v2 CP-7(3) (HIGH) • CMSRs 2013v2 CP-7(4) (HIGH) • CMSRs 2013v2 CP-9 (HIGH) • CMSRs 2013v2 CP-9(2) (HIGH) • IRS Pub 1075 v2014 9.3.6.5 • IRS Pub 1075 v2014 9.3.6.6 • IRS Pub 1075 v2014 9.3.6.8 • ISO/IEC 27002-2005 14.1.3 • ISO/IEC 27002:2013 17.1.2 • ISO 27799-2008 7.11 • JCAHO IM.01.01.03, EP 3 • MARS-E v1 CP-6 • MARS-E v1 CP-6(1) • MARS-E v1 CP-6(3) • MARS-E v1 CP-7 • MARS-E v1 CP-7(1) • MARS-E v1 CP-7(2) • MARS-E v1 CP-7(3) • MARS-E v1 CP-7(5)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• NIST Cybersecurity Framework PR.AT-1 • NIST Cybersecurity Framework PR.DS-1 • NIST Cybersecurity Framework PR.DS-4 • NIST Cybersecurity Framework PR.IP-7 • NIST Cybersecurity Framework RS.CO-1 • NIST SP 800-53 R4 CP-6 • NIST SP 800-53 R4 CP-6(1) • NIST SP 800-53 R4 CP-6(3) • NIST SP 800-53 R4 CP-7 • NIST SP 800-53 R4 CP-7(1) • NIST SP 800-53 R4 CP-7(2) • NIST SP 800-53 R4 CP-7(3) • NIST SP 800-53 R4 CP-9

Level 3 Implementation Requirements

Level 3 Organizational Factors:	BioTech Organizations: > $200,000,000 Spend on Research and Development Per Year, Third Party Processor: > 60,000,000 Records Processed Per Year, Physician Practice: > 180,000 Visits Per Year, Medical Facilities / Hospital: > 10,000 Licensed Beds, Health Plan / Insurance / PBM: > 7,500,000 Covered Lives, IT Service Providers (Vendors): > 2,500 Employees, Pharmacy Companies: > 70,000,000 Prescriptions Per Year, Health Information Exchange: >6,000,000 Transactions Per Year
Level 3 System Factors:	None
Level 3 Regulatory Factors:	Subject to FISMA Compliance, Subject to the CMS Minimum Security Requirements (High), Subject to MARS-E Requirements
Level 3 Implementation:	Level 2 plus: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within business defined time period when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites. The organization: i. Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements (including recovery time objectives); and ii. Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization shall provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure. Recovery of the information system after a failure or other contingency shall be done in a trusted, secure, and verifiable manner. Secure information system recovery and reconstitution shall include, but is not limited to: i. reset all system parameters (either default or organization-established), ii. reinstall patches, iii. reestablish configuration settings, iv. reinstall application and system software, and v. fully test the system.
Level 3 Control Standard Mapping:	• CMSRs 2013v2 CP-8 (HIGH) • CMSRs 2013v2 CP-8(1) (HIGH) • CMSRs 2013v2 CP-8(2) (HIGH) • CMSRs 2013v2 CP-8(3) (HIGH) • CMSRs 2013v2 CP-8(4) (HIGH) • CMSRs 2013v2 CP-10 (HIGH) • MARS-E v1 CP-8 • MARS-E v1 CP-8(1) • MARS-E v1 CP-8(2) • MARS-E v1 CP-10 • NIST SP 800-53 R4 CP-8 • NIST SP 800-53 R4 CP-8(1) • NIST SP 800-53 R4 CP-8(2) • NIST SP 800-53 R4 CP-10

CMS Contractor Requirements

CMS Contractors:	The business continuity plan shall: i. identify essential CMS missions and business functions and associated contingency requirements; ii. address maintaining essential CMS missions and business functions despite an information system disruption, compromise, or failure. The organization plans for the resumption of essential missions and business functions within the approved Maximum Tolerable Downtime (MTD) for the business functions. Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of system Recovery Time Objectives (RTOs) and business function Maximum Tolerable Downtimes (MTDs). Ensure alternate telecommunications Service Level Agreements (SLAs) are in

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

place to permit resumption of system Recovery Time Objectives (RTOs) and business function Maximum Tolerable Downtimes (MTDs).

The organization prepares the alternate processing site so that the site is ready to be used as the operational site supporting essential CMS missions and business functions.

The organization shall provide the capability to reimage information system components and support target recovery times from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.

The organization shall conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

The organization shall configure the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

The organization plans for the continuance of Primary Mission Essential Functions (PMEFs) with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

The organization shall use a sample of backup information in the restoration of selected information system functions as part of contingency plan testing (see 12.e, Level 2).

The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

Alternate telecommunications service providers that are sufficiently separated from the organization's primary service provider shall be identified and agreements established to ensure they are not susceptible to the same hazards.

The organization:

i. Requires primary and alternate telecommunications service providers to have contingency plans;
ii. Reviews provider contingency plans to ensure that the plans meet organizational contingency requirements; and
iii. Obtains evidence of contingency testing/training by providers within every three hundred sixty-five (365) days.

The organization plans for the resumption of all missions and business functions within the approved Maximum Tolerable Downtime (MTD) for the business functions.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

FTI Requirements

FTI Custodians:	The agency must identify alternative storage sites and initiate necessary agreements to permit the secure storage of information system and FTI backups and ensure the alternative storage sites provide information security safeguards that meet the minimum FTI protection and disclosure provisions of IRS 6103.

Health Insurance Exchange Requirements

Health Insurance Exchanges:	Ensure all equipment and supplies required for resuming system operations at the alternate processing site are available, or contracts are in place to support delivery to the site, to permit resumption of essential missions and business functions within one (1) week of contingency plan activation. Ensure alternate telecommunications service agreements are in place to permit resumption of information system operations for essential missions and business functions within one (1) week of contingency plan activation when primary telecommunications capabilities are unavailable. The organization provides compensating security controls for circumstances that inhibit recovery and reconstitution to a known state.

Control Reference: 12.d Business Continuity Planning Framework

Control Specification:	A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
Factor Type:	Organizational
Topics:	Contingency Planning IT Organization and Management Roles and Responsibilities Maintenance Policies and Procedures Services and Acquisitions

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory	Subject to FISMA Compliance, Subject to the CMS Minimum Security

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factors:	Requirements (High), Subject to MARS-E Requirements, Subject to FTI Requirements, Subject to Joint Commission Accreditation
Level 1 Implementation:	The organization shall create at a minimum one business continuity plan. The business continuity plan shall describe the approach for continuity, ensuring at a minimum the approach to maintain information or information asset availability and security. The plan shall also specify the escalation plan and the conditions for its activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, any existing emergency procedures (e.g., evacuation plans or fallback arrangements) shall be amended as appropriate. The plan shall have a specific owner. Emergency procedures, manual "fallback" procedures, and resumption plans shall be within the responsibility of the owner of the business resources or processes involved. Fallback arrangements for alternative technical services, such as information processing and communications facilities, shall usually be the responsibility of the service providers. The business continuity planning framework shall address the identified information security requirements, including the following: i. the conditions for activating the plans which describe the process to be followed (e.g., how to assess the situation, who is to be involved) before each plan is activated; ii. emergency procedures which describe the actions to be taken following an incident that jeopardizes business operations; iii. fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations, and to bring business processes back into operation in the required time-scales; iv. resumption procedures which describe the actions to be taken to return to normal business operations; v. a maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan; vi. awareness, education, and training activities which are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective; and vii. the critical assets and resources needed to be able to perform the emergency, fallback and resumption procedures.
Level 1 Control Standard Mapping:	• CMSRs 2013v2 CP-2 (HIGH) • CSA RS-03 • HIPAA § 164.308(a)(7)(ii)(B) • HIPAA § 164.308(a)(7)(ii)(C) • HIPAA § 164.308(a)(7)(ii)(E) • HIPAA § 164.310(a)(2)(i) • HIPAA § 164.312(a)(2)(ii) • IRS Pub 1075 v2014 9.3.6.2 • JCAHO IM.01.01.03, EP 1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• MARS-E v1 CP-2 • NIST SP 800-53 R4 CP-2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	Level 1 plus: Each business unit shall create at a minimum one business continuity plan. Procedures shall be included within the organization's change management program to ensure that business continuity matters are always addressed and timely as part of the change management process. A business continuity planning framework shall address the identified information security requirements and the following: i. temporary operational procedures to follow pending completion of recovery and restoration; and ii. the responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.
Level 2 Control Standard Mapping:	• ISO/IEC 27002-2005 14.1.4 • ISO/IEC 27002:2013 17.1.2 • ISO 27799-2008 7.11 • NIST Cybersecurity Framework ID.AM-5 • NIST Cybersecurity Framework ID.AM-6 • NIST Cybersecurity Framework ID.BE-5 • NIST Cybersecurity Framework PR.AT-1 • NIST Cybersecurity Framework DE.AE-5 • NIST Cybersecurity Framework RS.CO-1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 12.e Testing, Maintaining and Re-Assessing Business Continuity Plans

Control Specification:	Business continuity plans shall be tested and updated regularly, at a minimum annually, to ensure that they are up to date and effective.
Factor Type:	Organizational
Topics:	Awareness and Training Contingency Planning IT Organization and Management Roles and Responsibilities Personnel

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to Joint Commission Accreditation
Level 1 Implementation:	Business continuity plan tests shall ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked. The test schedule for business continuity plan(s) shall indicate how and when each element of the plan is tested. These techniques shall be applied on a 'programmatic' basis such that the tests build upon one another, and in a way that is relevant to the specific response and recovery plan. The results of tests shall be recorded and actions taken to improve the plans, where necessary. Updates will also consider lessons learned from implementation

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	of the business continuity plan(s). Responsibility shall be assigned for regular reviews of at least a part of the business continuity plan at a minimum, annually. The identification of changes in business arrangements not yet reflected in the business continuity plan shall be followed by an update of the plan. Changes where updating of business continuity plans shall be made are acquisition of new equipment, upgrading of systems and changes in: i. personnel; ii. location, facilities, and resources; iii. legislation; iv. processes, or new or withdrawn ones; v. risk (operational and financial).
Level 1 Control Standard Mapping:	• CSA RS-04 • HIPAA § 164.308(a)(7)(ii)(B) • HIPAA § 164.308(a)(7)(ii)(C) • HIPAA § 164.308(a)(7)(ii)(D) • HIPAA § 164.308(a)(7)(ii)(E) • HIPAA § 164.310(a)(2)(i) • HIPAA § 164.312(a)(2)(ii) • JCAHO IM.01.01.03, EP 5 • IRS Pub 1075 v2014 9.3.6.2 • NIST Cybersecurity Framework ID.AM-6 • NIST Cybersecurity Framework ID.GV-3 • NIST Cybersecurity Framework PR.IP-7 • NIST Cybersecurity Framework PR.IP-9 • NIST Cybersecurity Framework PR.IP-10 • NIST Cybersecurity Framework RS.CO-1 • NIST Cybersecurity Framework RC.IM-1 • NIST Cybersecurity Framework RC.IM-2 • NIST SP 800-53 R4 CP-2 • Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3 • Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3 • 1 TAC § 390.2(a)(1)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	BioTech Organizations: > $100,000 Spend on Research and Development Per Year, Third Party Processor: > 10,000,000 Records Processed Per Year, Physician Practice: > 60,000 Visits Per Year, Medical Facilities / Hospital: > 1,000 Licensed Beds, Health Plan / Insurance / PBM: > 1,000,000 Covered Lives, IT Service Providers (Vendors): > 500 Employees, Pharmacy Companies: > 10,000,000 Prescriptions Per Year, Health Information Exchange: >1,000,000 Transactions Per Year

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance, Subject to MARS-E Requirements, Subject to FTI Compliance
Level 2 Implementation:	Level 1 plus: Each element of the plan(s) shall be tested at least annually. A variety of techniques shall be used in order to provide assurance that the plan(s) will operate in real life including: i. table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions); ii. simulations (particularly for training people in their post-incident/crisis management roles); iii. technical recovery testing (ensuring information systems can be restored effectively) including: a. system parameters are set to secure values; b. security critical patches are reinstalled; c. security configuration settings are reset; d. system documentation and operating procedures are readily available; e. application system software is reinstalled and configured with secure settings; and f. information from the most recent secure back-up(s) is loaded; iv. testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site); v. tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment); vi. complete rehearsals (testing that the organization, personnel, equipment, facilities, and processes can cope with interruptions). The organization shall review test results and initiate corrective actions to ensure the continued effectiveness of the plan. Responsibility shall be assigned for regular formal reviews of each business continuity plan, which shall ensure that the updated plans are distributed and reinforced by yearly reviews of the complete plan. The organization shall coordinate business continuity plan testing and/or exercises with organizational elements responsible for related plans.
Level 2 Control Standard Mapping:	• CMSRs 2013v2 CP-2 (HIGH) • CMSRs 2013v2 CP-4 (HIGH) • CMSRs 2013v2 CP-4(1) (HIGH) • CMSRs 2013v2 CP-4(2) (HIGH) • CMSRs 2013v2 CP-4(4) (HIGH) • IRS Pub 1075 v2014 9.3.6.2 • IRS Pub 1075 v2014 9.3.6.4

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• IRS Pub 1075 v2014 9.4.2 (E.10) • ISO/IEC 27002-2005 14.1.5 • ISO/IEC 27002:2013 17.1.3 • ISO 27799-2008 7.11 • MARS-E v1 CP-2 • MARS-E v1 CP-4(1) • NIST SP 800-53 R4 CP-4 • NIST SP 800-53 R4 CP-4(1)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

CMS Contractor Requirements

CMS Contractors:	The organization shall test/exercise the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations. The organization shall include a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

FTI Requirements

FTI Custodians:	Both incremental and special purpose data backup procedures are required, combined with off-site storage protections and regular test-status restoration, to validate disaster recovery and business process continuity. Standards and guidelines for these processes are bound by agency policy and are tested and verified.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Category: 13.0 – Privacy Practices

Objective Name: 13.01 – Openness and Transparency

Control Objective:	To ensure openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.

Control Reference: 13.a Notice of Privacy Practices

Control Specification:	Individuals have a right to adequate notice of the uses and disclosures of PHI that may be made by the covered entity, and of the individual's rights and the entity's legal duties with respect to PHI.
Factor Type:	Organizational

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 Implementation:	The covered entity uses and discloses PHI in a manner consistent with its privacy notice. The covered entity provides individuals with an appropriate notice of the potential uses and disclosures of their PHI that contains required elements (e.g., header, descriptions of uses with at least one example, requirements for authorization). The covered entity must provide appropriate notice, in the manner and timeframe required (via mail, email, website posting) by federal and state law. If the covered entity provides a health plan, the covered entity provides notice or notices relevant to the individual (other than an inmate) no later than the compliance date or upon enrollment thereafter, within 60 days of a material revision, and no less than every three years. A covered entity may provide the notice of privacy practices to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn.
Level 1 Control	• 1 TAC § 390.2(a)(1)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Standard Mapping:	• HIPAA § 164.502(i) • HIPAA § 164.520(a) • HIPAA § 164.520(b) • HIPAA § 164.520(c) • HIPAA § 164.520(d) • HIPAA § 164.530(i)(4) • HIPAA § 164.530(j) • NIST SP 800-53 R4 AP-1 • NIST SP 800-53 R4 TR-1 • NIST SP 800-53 R4 TR-3 • NIST SP 800-53 R4 UL-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: When statutory language is written broadly and thus subject to interpretation, organizations shall ensure, in consultation with the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and legal counsel, that there is a close link between the general authorization and any specific collection of personally identifiable information (PII). Once the specific purposes have been identified, the purposes are clearly described in the related privacy compliance documentation, including but not limited to Privacy Impact Assessments (PIAs), System of Records Notices (SORNs), and Privacy Act Statements provided at the time of collection (e.g., on forms organizations use to collect PII). The organization provides real-time and/or layered notice when it collects PII. The organization: i. publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing PII; ii. keeps SORNs current; and iii. includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The organization publishes SORNs on its public website.
Level 2 Control Standard Mapping:	• NIST SP 800-53 R4 AP-2 • NIST SP 800-53 R4 TR-1(1) • NIST SP 800-53 R4 TR-2 • NIST SP 800-53 R4 TR-2(1)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Group Health Plans

Group Health Plans:	The health insurance issuer or HMO provides an individual—other than an inmate—enrolled in a group health plan a notice of privacy practices for that portion of the group health plan through which the individual receives benefits. At a minimum of once every three years, the health plan must notify individuals then covered by the plan, of the availability of the notice and how to obtain the notice. Notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents. Notice must be given to individuals who are new enrollees at the time of enrollment, and within 60 days of a material revision to the notice.

Control Reference: 13.b Rights to Protection and Confidentiality

Control Specification:	Individuals shall have the right to request restriction of uses and disclosures of their PHI.
Factor Type:	Organizational

Level 1 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 Implementation:	A covered entity must permit an individual, or their legally-authorized representative, to request that the covered entity restrict uses or disclosures of the individual's PHI to carry out treatment, payment, or health care operations. A covered entity is not required to agree to a restriction. A covered entity that agrees to a restriction on use or disclosure must document the restriction in accordance with HIPAA § 164.530(j). The business associate, and its subcontractors, must agree to the same restrictions and conditions that apply to the covered entity with respect to such information. The covered entity agrees to- and complies with-, requests by individuals for restrictions on disclosure of PHI to a health plan for a health care item or service for which someone other than the health plan pays in full. The covered entity terminates agreements to restrictions if the individual agrees to or requests the termination in writing, an oral agreement is documented, or the covered entity informs the individual, and termination is effective only for PHI created or received thereafter. The covered entity provides for individual complaints concerning the covered entity's privacy policies and procedures or its compliance with such policies and procedures. The covered entity ensures that individuals who exercise any of their lawful rights, including the filing of a complaint, are not subject to intimidation, threats, discrimination, or any other retaliatory action.
Level 1 Control Standard Mapping:	• 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(4)(B)(i) • 1 TAC § 390.2(a)(4)(B)(ii) • 1 TAC § 390.2(a)(4)(B)(iii) • 1 TAC § 390.2(a)(4)(B)(v) • 1 TAC § 390.2(a)(4)(B)(xiv) • 1 TAC § 390.2(a)(4)(B)(xv) • 1 TAC § 390.2(a)(4)(B)(xvi) • 1 TAC § 390.2(a)(4)(C)(i) • 1 TAC § 390.2(a)(4)(C)(ii) • • HIPAA § 164.502(g) • HIPAA § 164.522(a) • HIPAA § 164.522(a)(3)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• HIPAA § 164.530(j) • HIPAA § 164.530(d) • HIPAA § 164.530(g) • NIST SP 800-53 R4 IP-4

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: Organizational complaint management processes include tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed within a reasonable timeframe, which is explicitly defined by the organization.
Level 2 Control Standard Mapping:	• NIST SP 800-53 R4 IP-4(1)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Texas Covered Entities

Texas Covered Entities:	Hospitals, ambulatory surgical centers, nursing and other facilities in which the patient is resident, outpatient facilities such as those for end stage renal disease, special care facilities such as those for AIDs patients, psychiatric (mental) facilities, and intermediate care facilities such as those for the elderly or persons with an intellectual disability or related conditions, shall ensure their statement of patient rights addresses the right of the patient,

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	within the limits of federal and state law, to personal privacy and confidentiality of personal information and clinical records. Organizations shall ensure that a minor child as defined in Texas Civil Practice Code § 129.001 or non-parent of a minor child may consent to medical, dental, psychological, counseling and surgical treatment for the child by a licensed physician or dentist for those circumstances specified in Texas Family Code §§ 32.003 and 32.004. Organizations shall also ensure a parent, foster parent, guardian, or managing conservator of a minor child with special healthcare needs or an adult client with special needs retains the rights and duties specified in Texas Administrative Code § 38.5. Organizations shall ensure that a parent of a minor child retains the rights and duties specified in Texas Family Code §§ 151.001, 153.073, 153.074 and 153.132 pursuant to the exceptions provided by §§ 32.003 and 32.004.

Control Reference: 13.c Authorization Required

Control Specification:	Valid authorizations for the use or disclosure of PHI shall be obtained, and such use or disclosure shall be consistent with such authorization.
Factor Type:	Organizational

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 Implementation:	The covered entity does not use or disclose PHI without a valid authorization, when such authorization is required. A valid authorization is required for the use or disclosure of psychotherapy notes or for marketing purposes. When authorization is required, the covered entity ensures the authorizations are valid by including required core elements (reference 45 CFR 164.508(c)), and the covered entity shall allow an individual to revoke such authorization in writing at any time. The covered entity shall not create compound authorizations, except when combining authorizations for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with a consent to participate in research. However, a covered entity may combine authorizations specifically for the use or disclosure of psychotherapy notes. When combining any of the above authorizations, the covered entity must ensure there is no condition on the provision of treatment, payment,

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	enrollment in a health plan, or eligibility for benefits on the provision of an authorization except as allowed for research, underwriting and risk determinations, or disclosure of PHI to a third party, but in no case for the use of psychotherapy notes.
Level 1 Control Standard Mapping:	• 1 TAC § 390.2(a)(4)(C)(iii) • 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(4)(A)(viii) • 1 TAC § 390.2(a)(4)(A)(xv) • 1 TAC § 390.2(a)(4)(B)(i) • 1 TAC § 390.2(a)(4)(B)(ii) • 1 TAC § 390.2(a)(4)(B)(xviii)(III) • 1 TAC § 390.2(a)(4)(C)(i) • HIPAA § 164.508(a) • HIPAA § 164.508(b) • HIPAA § 164.508(c) • HIPAA § 164.530(j) • NIST SP 800-53 R4 IP-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: The organization implements mechanisms to support itemized or tiered consent for specific uses of data.
Level 2 Control Standard Mapping:	• NIST SP 800-53 R4 IP-1(1)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation:	No additional requirements

Texas Covered Entities

Texas Covered Entities:	Persons or organizations required to report immunization information to the state for registry purposes or authorized to receive information from the registry shall not disclose the individually identifiable information of an individual to any other person without the written or electronic consent of the individual or the individual's legally authorized representative, except as provided by Texas Occupations Code § 159 or TX Insurance Code § 602.053, and subject to the penalties outlined in THSC § 161.009. Persons and organizations shall not request information from the immunization registry without providing the written consent of the individual or, if a child, the parent, managing conservator or legal guardian, or except as provided by the TX Occupations Code § 159, or the TX Insurance Code § 28B.04. Persons and organizations shall ensure registry information is not inadvertently released due to a request for discovery, subpoena, or other means of legal compulsion for release to any person or entity, except as provided by THSC 161 § Subchapter A. Persons and organizations (providers) shall identify and treat government benefits / federal assistance information (records), such as those relating to 7 CFR § 272 (SNAP), 45 CFR § 205.50 (TANF) and 42 CFR § 431.300 (Medicaid) as confidential and not public records, and such information (records) shall be disclosed only upon written authorization of the recipients, except as noted in the respective program's parent regulation(s) or as otherwise required or authorized by other federal or state law. Except as authorized by THSC § 241.153, a hospital or an agent or employee of a hospital may not disclose health care information about a patient to any person other than the patient or the patient's legally authorized representative without the written authorization of the patient or the patient's legally authorized representative. Except as provided in 40 TAC §19.407(3), a resident patient may approve or refuse the release of personal and clinical records to any individual outside of the facility. Organizations shall ensure that consent for the release of confidential information related to a minor child must be in writing and signed by the patient, the parent or legal guardian of the patient, an attorney ad litem appointed for the patient, or a personal representative of the patient if the patient is deceased per Texas Occupations Code § 159.005.

Control Reference: 13.d Opportunity Required

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Specification:	Individuals shall be informed in advance of the use or disclosure of PHI and shall have the opportunity to agree to or prohibit or restrict the use or disclosure when required.
Factor Type:	Organizational

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 Implementation:	The covered entity informs individuals in advance of an allowed use or disclosure and provides an opportunity to agree to or prohibit or restrict the use or disclosure, either orally or in writing. If an individual does not object, the covered entity limits the PHI contained in a directory of individuals at its facility to the individual's name, location, general condition, and religious affiliation and only uses or discloses such information for directory purposes to members of the clergy or, except for religious affiliation, to other persons who ask for the individual by name. The covered entity informs individuals of the PHI it may include in a directory, and to whom it may disclose such information, and provide the individual an opportunity to restrict or prohibit some or all of the disclosures. The covered entity provides directory information for allowed uses, only in cases where the individual has not objected to such use, or when the opportunity to object cannot be practicably provided because of incapacity or an emergency treatment circumstance. If the covered entity discloses PHI to a family member, or other relative, or a close personal friend of the individual, or any other person identified by the individual, or to assist and locate such a person, the disclosure is limited to that PHI directly relevant to the person's involvement with the individual's care or payment related to such care, or otherwise limited to the requirements for limited uses and disclosures when the individual is not present, for disaster relieve purposes, or for a deceased individual. If an individual is present, or has the authority, the covered entity obtains the individual's consent or authorization, provides the individual an opportunity to object, or reasonably infers from the circumstances that the individual does not object to disclosure of PHI. When an individual is not present or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of incapacity or

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	emergency, the covered entity ensures that it only allows uses or provides disclosures of PHI to a person that is directly relevant to that person's involvement with the individual's health care. The covered entity limits disclosure of PHI to a public or private entity authorized by law or by its charter, to assist in disaster relief efforts or emergency response. If the individual is deceased, a covered entity only discloses to a family member, or other persons identified in this control (13.d) who were involved in the individual's care or payment for health care prior to the individual's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any known prior expressed preferences.
Level 1 Control Standard Mapping:	• 1 TAC § 390.2(a)(1) • HIPAA § 164.510(a) • HIPAA § 164.510(b) • NIST SP 800-53 R4 IP-1

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 13.e Authorization or Opportunity Not Required

Control Specification:	PHI may only be used or disclosed without written authorization of the individual or the opportunity for the individual to agree or object only when such use or disclosure is authorized by applicable laws or regulations.
Factor Type:	Organizational

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 Implementation:	The covered entity limits the use or disclosure of PHI to the extent that such use or disclosure is authorized by law. The covered entity complies with the regulatory criteria for permitted uses and disclosures of PHI for public health activities for purposes including preventing or controlling disease; reporting incidents of child abuse or neglect; relating to the jurisdiction of the Food and Drug Administration; intervention or investigation of communicable diseases; work-related illness or injury; or to disclose proof of immunization. The covered entity discloses PHI about an individual whom the entity reasonably believes to be a victim of abuse, neglect, or domestic violence to government authorities authorized by law to receive such reports only to the extent necessary and required by law, and notifies the individual when required by law. The covered entity discloses PHI to a health oversight agency only for those oversight activities authorized by law. The covered entity ensures that satisfactory assurances are obtained before providing the appropriate disclosures of PHI pursuant to court orders, subpoenas, or discovery requests for judicial and administrative proceedings The covered entity only discloses PHI to law enforcement for valid law enforcement purposes when specifically defined criteria are met. The covered entity discloses PHI to law enforcement for identification and location purposes subject to specifically defined criteria, including whether or not notice or consent is provided. The covered entity discloses PHI related to victims of a crime to law enforcement subject to specifically defined criteria.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The covered entity discloses PHI related to an individual who has died to law enforcement if the covered entity has a suspicion that such death may have resulted from criminal conduct. The covered entity discloses PHI related to a crime on premises or in an emergency to law enforcement if the covered entity believes in good faith criminal conduct occurred on the premises. The covered entity limits disclosure of PHI to a coroner or medical examiner--or a covered entity acting in the capacity of a coroner or medical examiner--to that required to identify a deceased person, determine a cause of death, or other duties as authorized by law. The covered entity limits disclosure of PHI to funeral directors, consistent with applicable law, to the minimum necessary to carry out their duties with respect to the decedent. The covered entity limits uses or disclosures of PHI to legitimate organ procurement organizations for the purpose of facilitating organ, eye or tissue donation and transplantation. The covered entity uses or discloses PHI for research only if approved by a valid IRB or privacy board and receives appropriate representations from the research regarding the appropriate uses and disclosures necessary for research purposes. Documentation for a use or disclosure permitted for research based on approval of an alteration or waiver shall contain a signed, dated statement from the IRB or privacy board that confirms the necessary conditions for use or disclosure. A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose PHI to the extent allowed if the covered entity, in good faith, believes the use or disclosure is reasonable or necessary for safety or law enforcement. The covered entity uses or discloses the PHI of Armed Forces personnel for activities deemed necessary by appropriate military command authorities only if the authority has published notice in the Federal Register, with appropriate military command authorities, and the purposes for which the PHI may be used or disclosed are identified. The covered entity discloses PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities. The covered entity discloses PHI to authorized Federal officials for the

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	provision of protective services to the President or other authorized officials or for the conduct of authorized investigations. A covered entity that is a component of the Department of State uses PHI only to make determinations regarding the medical suitability of an individual to officials in the Department of State who need access to such information for required security clearance, to determine worldwide availability or availability for mandatory service abroad, or for a family to accompany a Foreign Service member abroad. The covered entity uses or discloses PHI of an inmate to a law enforcement official having lawful custody of the inmate if the correctional institution or such law enforcement official represents such PHI is necessary. The covered entity only discloses PHI as authorized and to the extent necessary to comply with laws relating to workers' compensation or similar programs.
Level 1 Control Standard Mapping:	• 1 TAC § 390.2(a)(4)(A)(I) • 1 TAC § 390.2(a)(1) • HIPAA § 164.512(a) • HIPAA § 164.512(b) • HIPAA § 164.512(c) • HIPAA § 164.512(d) • HIPAA § 164.512(e) • HIPAA § 164.512(f) • HIPAA § 164.512(g) • HIPAA § 164.512(h) • HIPAA § 164.512(i) • HIPAA § 164.512(j) • HIPAA § 164.512(k) • HIPAA § 164.512(l) • NIST SP 800-53 R4 UL-1 • NIST SP 800-53 R4 UL-2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Federal Requirements

Federal Agencies and Contractors:	A health plan that is a government program providing public benefits may disclose PHI relating to eligibility for or enrollment in the health plan to another agency administering a government program providing public benefits if the sharing is required or expressly authorized by statute or regulation. A covered entity that is a government agency administering a government program providing public benefits may disclose PHI relating to the program to another covered entity that is a government agency administering a government program providing public benefits if they serve similar populations and the disclosure is necessary to coordinate the functions of such programs.

Texas Covered Entities

Texas Covered Entities:	Cancer data may be provided to the Texas Cancer Registry without patient authorization or consent in accordance with 25 TAC § 91.3(e).

Objective Name: 13.02 – Individual Choice and Participation

Control Objective:	To ensure individuals are provided a reasonable opportunity and capability to make informed decisions about the collection, use and disclosure of their individually identifiable health information.

Control Reference: 13.f Access to Individual Information

Control Specification:	Individuals have a right of access to inspect and obtain a copy of limited PHI about themselves contained in a Designated Record Set for as long as that

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	information is maintained.
Factor Type:	Organizational

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	With limited exceptions, the covered entity provides individuals the right of access to review and obtain a copy of certain PHI contained in a Designated Record Set for as long as that record set is maintained, and provides such access in a timely manner (30 days with no more than one 30 day extension), for no more than a reasonable, cost-based fee (if any), or, if the covered entity does not maintain the PHI but knows where it's located, the covered entity informs the individual where to direct the request. The covered entity provides the individual access to the PHI in the designated record set in a written or electronic form and format requested by the individual or otherwise agreed to by the covered entity and the individual. Summaries of the PHI requested are only provided in lieu of the designated record set if the individual agrees in advance to the summary and any fees imposed for providing such summary. The covered entity only provides access to another person designated by the individual if the individual requests such access in writing, signed by the individual, and the request clearly identifies the designated person and where the copy of the PHI should be sent. The covered entity denies an individual access to their PHI without providing an opportunity to review for psychotherapy notes, information compiled in anticipation of legal proceedings or subject to or exempt from the Clinical Laboratory Improvements Amendments of 1988; the covered entity is a correctional facility; the individual is involved in research in progress; the information is contained in records subject to the Privacy Act; or the information was obtained from an entity other than a health care provider on the promise of confidentiality. Should a licensed health care professional determine that access would endanger the life or physical safety of, or otherwise cause substantial harm to, the individual or another person, access to the individuals PHI shall be denied.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The covered entity provides timely (30 days plus no more than a 30 day extension), written denial to an individual's request for access in plain language that addresses the basis for denial, a statement of the individual's rights for review of the denial (e.g., review of the denial by a licensed health care professional), and a description of procedures for complaints to the entity and the Secretary of Health and Human Services.
Level 1 Control Standard Mapping:	• 1 TAC § 390.2(a)(1) • HIPAA § 164.524(a) • HIPAA § 164.524(b) • HIPAA § 164.524(c) • HIPAA § 164.524(d) • HIPAA § 164.530(j)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: The organization: i. Publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; ii. Publishes access procedures in System of Records Notices (SORNs); and iii. Adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests.
Level 2 Control Standard Mapping:	• NIST SP 800-53 R4 IP-2

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation:	No additional requirements

Control Reference: 13.g Accounting of Disclosures

Control Specification:	Individuals have a right to receive an Accounting of Disclosures for certain PHI.
Factor Type:	Organizational

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The covered entity provides individuals the right to receive an accounting of disclosures of certain PHI made by the covered entity in the six years prior to the date on which the accounting is requested, except for specific disclosures addressed in CSF controls 13.c (authorizations provided), 13.d (facility directory and relevant persons), 13.e (correction institutions and national security or intelligence purposes), 13.i (required disclosures), 13.j (permitted disclosures), and 13.l (limited data sets). The covered entity's accounting of disclosures includes, for the six years prior to the request, the date, a name and address of the entity provided the PHI, a description of the PHI disclosed, and the purpose for which the information was disclosed; and, if for research, the name of the research activity, the period of time the PHI was disclosed, the contact information of the research sponsor (name, address and phone number), and a statement that the PHI may or may not have been disclosed for a particular research activity. When requested by the individual, the covered entity provides assistance to the individual in contacting the research sponsor and researcher for an accounting. The covered entity acts upon an individual's request for an accounting no later than 60 days after receipt of the request (with a one-time 30 day extension with proper notice to the requestor), free of charge for the first request within any 12 month period and, if informed in advance, for a reasonable cost-based fee for subsequent requests within the period. The covered entity must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	official for the time specified by such agency or official, if such agency or official provides the covered entity with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.
Level 1 Control Standard Mapping:	• 1 TAC § 390.2(a)(1) • HIPAA § 164.528(a) • HIPAA § 164.528(b) • HIPAA § 164.528(c) • HIPAA § 164.530(j)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: The Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) periodically consults with managers of organization systems of record to ensure that the required accountings of disclosures of records are being properly maintained and provided to persons named in those records consistent with the dictates of the Privacy Act.
Level 2 Control Standard Mapping:	• NIST SP 800-53 R4 AR-8

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Control Reference: 13.h Correction of Records

Control Specification:	Individuals have a right to have certain PHI amended for as long as the information is maintained.
Factor Type:	Organizational

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The covered entity ensures individuals have the right to amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set. The covered entity denies an individual's request for amendment only if it determines the PHI or record was not created by the covered entity (unless the originator no longer exists), is not part of the designated record set, is not available for inspection per CSF control 13.f, or is otherwise accurate and complete. The covered entity acts on an individual's request for amendment within 60 days of the request, with no more than one 30 day extension. If the covered entity requires a written request with a rationale for the amendment, the covered entity makes these requirements known in advance. If the requested amendment is accepted in whole or in part, the covered entity makes the amendment, informs the individual the amendment was made in a timely manner, and makes reasonable efforts to notify relevant persons with whom the amendment must be shared in a reasonable timeframe. If a requested amendment is denied in whole or in part, the covered entity must provide the individual with a written denial; permit the individual to submit a statement of disagreement; prepare a written rebuttal if the individual submits a statement of disagreement; maintain denials, disagreements and rebuttals as organizational records; and provide relevant information regarding any disagreements in future disclosures of the

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	individual's PHI. The covered entity corrects an individual's PHI if informed by another covered entity of an amendment.
Level 1 Control Standard Mapping:	• 1 TAC § 390.2(a)(1) • HIPAA § 164.526(a) • HIPAA § 164.526(b) • HIPAA § 164.526(c) • HIPAA § 164.526(d) • HIPAA § 164.526(e) • HIPAA § 164.526(f) • NIST SP 800-53 R4 DI-1 • NIST SP 800-53 R4 IP-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: The organization requests that the individual or individual's authorized representative: i. validate PII during the collection process, and ii. periodically revalidate that PII collected is still accurate at an organization-defined frequency but no less than annually. The organization establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act. The organization publishes Computer Matching Agreements on its public website.
Level 2 Control Standard Mapping:	• NIST SP 800-53 R4 DI-1(1) • NIST SP 800-53 R4 DI-1(2) • NIST SP 800-53 R4 DI-2 • NIST SP 800-53 R4 DI-2(1)

Level 3 Implementation Requirements

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Group Health Plans

Group Health Plans:	The group health plan limits exceptions to the general requirements for amendments to PHI to health benefits provided other than solely through an insurance contract with a health insurance issuer or HMO and PHI that it does not create or receive, except for summary health information or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan. Amended plan documents are subject to the organization's retention policy.

Control Reference: 13.i Required Uses and Disclosures

Control Specification:	PHI shall be used or disclosed when required by applicable laws and regulations.
Factor Type:	Organizational

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	In certain instances, a covered entity may use or disclose PHI without the written authorization of the individual or the opportunity for the individual to agree or object. A covered entity may use or disclose PHI to the extent that such use or disclosure is required by law and the use or disclosure complies with and is

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	limited to the relevant requirements of such law. The covered entity shall disclose PHI to an individual when requested or required under federal or state law, or when required by the Secretary of Health and Human Services to investigate or determine the covered entity's compliance with the HIPAA Privacy Rule. The business associate shall disclose PHI when required by the Secretary of Health and Human Services to investigate or determine the business associate's compliance with the HIPAA Privacy Rule and to the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations as described in CSF control 13.f with respect to an individual's request for an electronic copy of PHI.
Level 1 Control Standard Mapping:	• 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(4)(A)(iii) • 1 TAC § 390.2(a)(4)(A)(xii) • 1 TAC § 390.2(a)(4)(A)(xiv) • 1 TAC § 390.2(a)(4)(B)(x) • • HIPAA § 164.502(a)(2) • HIPAA § 164.502(a)(4) • NIST SP 800-53 R4 UL-2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: Organizations ensure that they use PII only for legally authorized purposes and in a manner compatible with uses identified in the Privacy Act and/or in public notices, to include monitoring and auditing organizational use of PII. With guidance from the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and where appropriate, legal counsel, organizations formally evaluate any proposed new uses of PII to assess whether they fall within the scope of the organizational authorities.
Level 2 Control Standard Mapping:	• NIST SP 800-53 R4 UL-1

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Texas Covered Entities

Texas Covered Entities:	Healthcare entities receiving medical records from the Social Security Administration shall ensure that no part of the medical record is withheld from the individual or, in the case where the medical record pertains to a minor child, from the parent or guardian pursuant to 42 U.S.C. §1306, 20 CFR Part 401.55(c)(2), as referenced by 20 CFR Part 401.100(d). Laboratories shall ensure the confidentiality of patient information during all stages of the testing process that are under the laboratory's control and release test results only to authorized persons and, if applicable, the individual responsible for using the test results and the laboratory that initially requested the test. Laboratories shall have an adequate manual or electronic system(s) in place to ensure test results and other patient-specific information is accurately and reliably transmitted from the point of data entry (whether interfaced or entered manually) to the final report's destination, in a timely manner. The entity that performed the genetic test shall disclose the test results to the individual or a physician designated by the individual upon written request. Persons and organizations (providers) shall treat family planning information as defined by 25 TAC § 56.11 as confidential and not public records, and shall be disclosed only upon written authorization of the clients (patients), except for reports of child abuse as required by Texas Family Code § 261 or as required or authorized by other federal or state law.

Control Reference: 13.j Permitted Uses and Disclosures

Control Specification:	PHI may be used or disclosed when permitted by applicable laws and regulations.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Factor Type:	Organizational

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Organizations shall ensure patient information with special handling requirements, e.g., HIV, mental health and substance abuse-related records (see 07.e), is not disclosed except to individuals, organizations or agencies expressly allowed by applicable federal and state law. The covered entity limits permitted uses or disclosures of PHI to the individual; for treatment, payment or healthcare operations; incident to a use or disclosure otherwise permitted or required; or otherwise pursuant to a valid authorization or agreement. A business associate only uses or discloses PHI as permitted or required by its business associate contract or other arrangement and does not use or disclose PHI in a manner that would violate requirements for the protection of such information, if done by the covered entity, except for the purposes specified in CSF control 13.h if such uses or disclosures are permitted by its contract or other arrangement. The covered entity complies with restrictions on use and disclosure of PHI for which it has agreed. A covered entity or business associate may disclose PHI to a business associate and may allow a business associate to create, receive, maintain, or transmit PHI on its behalf, if the covered entity or business associate obtains satisfactory, written assurance (e.g., a written contract, agreement or arrangement that satisfies the requirements of this control) that the business associate will appropriately safeguard the information. The covered entity expressly permits disclosures of PHI by whistleblowers and specifies the appropriate conditions under which whistleblowers may disclose PHI. The covered entity permits certain disclosures of PHI by workforce members who are victims of a crime to law enforcement and specifies the conditions under which they may disclose PHI.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	The covered entity or business associate understands when it has not obtained satisfactory assurances or met the standards for business associate contracts and takes appropriate action if it knew of a pattern or activity or practice of the business associate that constituted a material breach or violation of its obligations. The covered entity uses and discloses PHI for treatment, payment or health care operations appropriately and not in a manner inconsistent with uses or disclosures that require authorization or are otherwise prohibited. If consent is obtained from an individual to carry out treatment, payment or health care operations the covered entity does not use or disclose PHI in other circumstances that require authorization or when another condition must be met for such use or disclosure. The covered entity only discloses PHI for specific, allowed treatment, payment or health care operations, including quality assessments, competency or qualification reviews, health care fraud and abuse detection or compliance, and patient safety activities. The covered entity only uses or discloses specific, limited types of PHI under specific, defined conditions to a business associate or an institutionally-related foundation for the purpose of raising funds for its own benefit. The covered entity restricts uses and/or disclosures of PHI used for underwriting purposes for any other purpose except as may be required by law. The covered entity formally verifies (e.g., with appropriate documentation) the identity and authority of persons (e.g., public officials) requesting PHI.
Level 1 Control Standard Mapping:	• 1 TAC § 390.2(a)(1) • 1 TAC § 390.2(a)(4)(A)(i) • 1 TAC § 390.2(a)(4)(A)(ii) • 1 TAC § 390.2(a)(4)(A)(iii) • 1 TAC § 390.2(a)(4)(A)(ix) • 1 TAC § 390.2(a)(4)(A)(v) • 1 TAC § 390.2(a)(4)(A)(x) • 1 TAC § 390.2(a)(4)(A)(xi) • 1 TAC § 390.2(a)(4)(A)(xiii) • 1 TAC § 390.2(a)(4)(B)(iii) • 1 TAC § 390.2(a)(4)(B)(xvii) • 1 TAC § 390.2(a)(4)(C)(iii) • 1 TAC § 390.2(a)(1) • NIST SP 800-53 R4 UL-1 • NIST SP 800-53 R4 UL-2

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Texas Covered Entities

Texas Covered Entities:	Organizations shall ensure reports, records, and other documents containing sensitive personal information lawfully obtained by state agencies are not subject to subpoena and may not otherwise be released or made public except as authorized by law. Genetic information is considered sensitive personal information (also PHI as defined by HIPAA) and is confidential and privileged regardless of the source of the information. Persons and organizations, including licensing authorities, shall ensure that genetic information about an individual may not be disclosed, or compelled to be disclosed by subpoena or otherwise, unless the disclosure is to the individual, or otherwise authorized by the individual as provided by TX Insurance Code § 546.104, a physician or other individual designated or authorized by the individual as provided by TX Labor Code § 21.403 or other applicable federal or state law. Persons and organizations shall ensure that records of the identity, personal history or background information of a survivor of sexual assault, or

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	information concerning the victimization of a survivor, created by or provided to an advocate or maintained by a sexual assault program is confidential and may not be disclosed except as provided by Tex. Gov. Code § 420 Subchapter D. Persons and organizations shall ensure that the section of a birth certificate entitled "For Medical and Health Use Only" is not considered part of the legal birth certificate and is not released or made public on subpoena or otherwise, except that release may be made for statistical purposes only so that no person, patient, or facility is identified, or to medical personnel of a health care entity, as that term is defined in Subtitle B, Title 3, TX Occupations Code, or appropriate state or federal agencies for statistical research, except as provided in § 192.002. Persons and organizations shall ensure that reports, records, and information relating to cases or suspected cases of diseases or health conditions—regardless of the source—are confidential, are not made public, and are not released or made public on subpoena or otherwise except as provided by THSC § 81.046 and other applicable federal or state law. Persons and organizations shall ensure that individual morbidity reports are confidential, are not made public, and are not released or made public except as allowed under federal or state law. Persons and organizations shall ensure the confidentiality of reports of abuse, neglect, or exploitation of minor, elderly and disabled persons including those with an intellectual disability or related condition, ICF/IID), or information used or developed in an investigation or in providing services as a result of an investigation, and that disclosures of such information are limited to those defined in TX Human Resources Code §§ 48.101 and 48.154 and TX Family Code §§ 261.201 thru 261.203, and THSC § 252.126. Persons and organizations shall treat occupational health case reports as defined by 25 TAC § 99.1 as confidential and not public records, and shall be accessed only by authorized persons, except when such information is de-identified for statistical and epidemiological studies, which may be made public. Persons and organizations shall treat records associated with a state investigation of alleged abuse or neglect of a chemical dependency counselor or treatment center as confidential per THSC § 464.010(e) and not public records, and shall only be disclosed as authorized by THSC §§ 464.010(e) and 464.011. Organizations shall ensure the disclosures of client Medicaid information comply with TX Human Resources Code §§ 12.003 and 21.012 and TX Government Code § 552.10 in addition to the federal requirements outlined in 42 USC, §1396a(a)(7) and 42 CFR §§431.301 thru 431.306.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Objective Name: 13.03 - Correction

Control Objective:	To ensure individuals are provided with a timely means to dispute the accuracy of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.

Control Reference: 13.k Prohibited or Restricted Uses and Disclosures

Control Specification:	PHI shall not be used or disclosed when prohibited or otherwise restricted by applicable laws and regulations.
Factor Type:	Organizational

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Unless the entity is an issuer of long-term care policies, the health plan may not use or disclose PHI that is genetic information for underwriting purposes. The covered entity or business associate shall not sell PHI.
Level 1 Control Standard Mapping:	• 1 TAC § 390.2(a)(4)(B)(iii) • 1 TAC § 390.2(a)(4)(B)(xiv) • 1 TAC § 390.2(a)(1) • HIPAA § 164.502(a)(5) • NIST SP 800-53 R4 UL-1 • NIST SP 800-53 R4 UL-2

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Texas Covered Entities

Texas Covered Entities:	Records relating to the deaths of residents with an intellectual disability or related condition are also confidential and not subject to release or disclosure under the provisions of TX Government Code § 552. End stage renal facilities shall ensure information concerning quality of care provided to or compiled by the Department of State Health Services or medical review board and a recommendation of the medical review board are confidential. The information or recommendation may not be made available for public inspection, is not subject to disclosure under TX Government Code, Chapter 552, and is not subject to discovery, subpoena, or other compulsory legal process.

Control Reference: 13.l Minimum Necessary Use

Control Specification:	The use or disclosure of PHI shall be limited to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request, including de-identification and limited data sets
Factor Type:	Organizational

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Level 1 Regulatory Factors:	None
Level 1 Implementation:	The covered entity or business associate makes reasonable efforts to limit requests for PHI to, or from, another covered entity or business associate to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. Exceptions include, but are not limited to, treatment, requests by the individual, or uses or disclosures pursuant to a valid authorization, required by law, or required for compliance with other requirements, such as disclosures made to the Secretary of Health and Human Services. A covered entity must make reasonable efforts to limit the access of persons or classes of persons to those with a legitimate need to access to PHI. The covered entity limits the PHI disclosed to the minimum amount reasonably necessary to achieve the purpose of the disclosure. The covered entity only creates and uses information that is not individually identifiable (i.e., de-identified) when a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified is not disclosed. If the de-identified information is subsequently re-identified, the covered entity only uses or discloses such re-identified information as permitted or required for PHI. The covered entity understands that health information is not identifiable (i.e., de-identified) only when there is no reasonable basis to believe that the information can be used to identify an individual and meets federal requirements for de-identified data. When de-identifying PHI, the covered entity removes all eighteen (18) data elements required by the HIPAA Administrative Simplification's Privacy Rule and has no knowledge the resulting data set could be re-identified, or an appropriate person applies generally accepting scientific principles and methods for rendering information not individually identifiable and determines the risk of re-identification is appropriately small. The covered entity may enter into a data use agreement with a recipient before allowing the use or disclosure of a limited data set and ensures the data provided meets the requirements for a limited data set. A covered entity may use or disclose a limited data set only for the purposes of research, public health, or health care operations.
Level 1 Control Standard Mapping:	• 1 TAC § 390.2(a)(1) • HIPAA § 164.502(b) • HIPAA § 164.502(d) • HIPAA § 164.514(a) • HIPAA § 164.514(b) • HIPAA § 164.514(c) • HIPAA § 164.514(d)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	• HIPAA § 164.514(e) • NIST SP 800-53 R4 DM-1 • NIST SP 800-53 R4 DM-3

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	Subject to FISMA Compliance
Level 2 Implementation:	Level 1 plus: The organization, where feasible and within the limits of technology, locates and removes/redacts specified PII and/or uses anonymization and de-identification techniques to permit use of the retained information while reducing its sensitivity and reducing the risk resulting from disclosure. The organization, where feasible, uses techniques (e.g., as described in NIST SP 800-122) to minimize the risk to privacy of using PII for research, testing, or training.
Level 2 Control Standard Mapping:	• NIST SP 800-53 R4 DM-1(1) • NIST SP 800-53 R4 DM-3(1)

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Control Reference: 13.m Confidential Communications

Control Specification:	Individuals shall be afforded the right to request and the covered entity must accommodate reasonable requests to receive communications of PHI by

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	alternative means or at alternative locations.
Factor Type:	Organizational

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	Persons and organizations shall ensure that communications between a patient and a healthcare professional are made available, upon request. A covered entity may require the individual to make a request for a confidential communication in writing. Communication between a healthcare provider and a patient, and records of the identity, evaluation, or treatment of a patient, that are made or created in the course of providing healthcare services to the patient shall be considered confidential and privileged and may not be disclosed except as provided by federal or state law. A patient's pharmacy records are similarly confidential, and a pharmacist may only release a confidential record to the patient or other individual or entity permitted by federal or state law. Communication between certified emergency medical services personnel or a physician providing medical supervision and a patient, and records relating to the identity, evaluation, or treatment of a patient that are made or created in the course of providing emergency medical services to the patient, shall be considered confidential and privileged and may not be disclosed except as provided by federal or state law. The covered entity must permit individuals who represent they are in danger to request and must accommodate reasonable requests by individuals to receive communications of PHI from the covered entity by alternative means or at alternative locations. As appropriate, the covered entity only conditions requests for confidential communications on how payment, if any, will be handled and the specification of an alternative address or other method of contact; however, in no case may the organization require an explanation as to the basis of the individual's request.
Level 1 Control	• 1 TAC § 390.2(a)(1)

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Standard Mapping:	• 1 TAC § 390.2(a)(4)(A)(vi) • 1 TAC § 390.2(a)(4)(A)(vii) • 1 TAC § 390.2(a)(4)(B)(ix) • 1 TAC § 390.2(a)(4)(B)(vi) • 1 TAC § 390.2(a)(4)(B)(vii) • 1 TAC § 390.2(a)(4)(B)(viii) • 1 TAC § 390.2(a)(4)(B)(xi) • 1 TAC § 390.2(a)(4)(B)(xii) • HIPAA § 164.502(h) • HIPAA § 164.522(b)

Level 2 Implementation Requirements

Level 2 Organizational Factors:	None
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Texas Covered Entities

Texas Covered Entities:	Persons and organizations shall ensure that communications between a patient and a professional for the diagnosis, evaluation, or treatment of any mental or emotional condition or disorder, including alcoholism or drug addiction, and records of the identity, diagnosis, evaluation, or treatment of a patient that are created or maintained by a professional, are only disclosed in select instances as provided by THSC §§ 611.004 or 611.0045, or 42 CFR

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

	Part 2.

Control Reference: 13.n Organizational Requirements

Control Specification:	An individual's privacy and security shall be assured through appropriate contracts, monitoring and other means and methods to report and mitigate non-adherence and breaches.
Factor Type:	Organizational

Level 1 Implementation Requirements

Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	None
Level 1 Implementation:	The covered entity ensures each of its business associates have a valid agreement that addresses the proper management/oversight of the business associate and specifies applicable requirements (e.g., around use, further disclosure, and the implementation of reasonable and appropriate safeguards). If the covered entity has multiple functions that would make the entity any combination of a health care provider, a health plan, and a health care clearinghouse, it ensures the use and disclosure of PHI is only for the purpose related to the appropriate function being performed. In an arrangement between business associate and a subcontractor who handles PHI for the business associate, the contractual requirements apply in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.
Level 1 Control Standard Mapping:	• 1 TAC § 390.2(a)(1) • HIPAA § 164.504(e) • HIPAA § 164.504(f) • HIPAA § 164.504(g) • NIST SP 800-53 R4 AR-3 • NIST SP 800-53 R4 UL-2

Level 2 Implementation Requirements

Level 2	None

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

Organizational Factors:	
Level 2 System Factors:	None
Level 2 Regulatory Factors:	None
Level 2 Implementation:	No additional requirements

Level 3 Implementation Requirements

Level 3 Organizational Factors:	None
Level 3 System Factors:	None
Level 3 Regulatory Factors:	None
Level 3 Implementation:	No additional requirements

Group Health Plan Requirements

Group Health Plans:	The group health plan documents appropriately restrict the use and disclosure of PHI by the plan sponsor. The group health plan, or a health insurance issuer or HMO with respect to the group plan, limits disclosures to the plan sponsor of information on whether an individual is participating in the plan, or is enrolled in or disenrolled from a health insurance issuer or HMO offered by the plan. The group health plan documents are amended as required to incorporate provisions to establish permitted and required uses and disclosures, and disclose PHI to the plan sponsor only upon receipt of certification that the documents have been amended for specific, limited reasons, e.g., that no use or further disclosure other than that permitted or required will be made. Plan documents ensure adequate separation between the group health plan and the plan sponsor by describing employees or classes of employees to whom PHI may be disclosed, restricting access and use by such persons or classes of persons to administrative functions the plan sponsor performs, and providing an effective mechanism for resolving issues of noncompliance with the plan document provisions.

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement

© 2015 HITRUST Alliance
Viewing and use of this document subject to the terms of the HITRUST CSF Licensing Agreement