HITRUST

Introduction to the HITRUST CSF

Version 9.1

February 2018

Contents

Executive Summary

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 by addressing specific challenges such as concern over current breaches, numerous and sometimes inconsistent requirements and standards, compliance issues, and the growing risk and liability associated with information security in the healthcare industry. By collaborating with healthcare, business technology and information security leaders, HITRUST developed a common framework that any and all organizations can use to create, access, store, or exchange Protected Health Information (PHI) safely and securely.

Organization of the HITRUST CSF

The HITRUST CSF is structured on International Organization of Standards (ISO) and International Electrotechnical Commission (IEC) standards 27001:2005 and 27002:2005 and incorporates other healthcare information security-related regulations, standards and frameworks to provide comprehensive and prescriptive coverage, including but not limited to:

- American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria
- Catalog of Minimum Acceptable Risk Standards for Exchanges (MARS-E) – Exchange Reference Architecture (ERA) Supplement v2
- Center for Internet Security (CIS) Critical Security Controls v6
- Department of Homeland Security (DHS) Cyber Resilience Review (CRR)
- European Union General Data Protection Regulation (EU GDPR)
- Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook – Information Security, September 2016
- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA) Omnibus Final Rule
- IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information (New)
- ISO/IEC 27001:2013, Information Technology—Security Techniques—Information Security Management Systems Requirements
- ISO/IEC 27002:2013, Information Technology—Security Techniques—Code of Practice for Information Security Controls
- ISO/IEC 27799:2008 Health Informatics (guidance for information security management for healthcare organizations using ISO/IEC 27002:2005)
- National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)
- New York State Department of Financial Services (Title 23 NYCRR Part 500)
- NIST Framework for Improving Critical Infrastructure Cybersecurity v1
- Control Objectives for Information and related Technology (COBIT) v4.1

- Payment Card Industry (PCI) Data Security Standard v3.2
- Federal privacy requirements (e.g., HHS)
- State security requirements (e.g., Nevada, Massachusetts, and Texas)
- Experiences and best practices of HITRUST participants

The HITRUST CSF is organized by 14 Control Categories, which contain 46 Control Objectives and 149 Control Specifications based on ISO/IEC 27001:2005 and 27002:2005. Each Control Specification consists of as many as three implementation levels applied to healthcare organizations according to specific organizational, system and regulatory factors.

Certain industry segments have specific requirements that do not apply or would not be considered reasonable and appropriate to other segments across the industry. As a result, the HITRUST CSF contains specific categories that provide additional requirements for these segments. Examples include CMS Contractors, Health Information Exchanges, Health Insurance Exchanges, PCI Data, and FTI Custodians.

HITRUST also provides detailed assessment guidance and cross-references to the many authoritative sources incorporated into the framework, including a detailed *Risk Analysis Guide for HITRUST Organizations & Assessors*.

Although comprehensive and prescriptive, the HITRUST CSF is quite flexible. With the diverse nature of healthcare and today's information systems, there may be situations in which implementing specific controls may not be reasonable and appropriate. HITRUST defined a formal process by which organizations may propose and, if approved, implement alternate controls to mitigate risk associated with a particular HITRUST CSF requirement.

HITRUST also developed and makes available an integrated online tool, MyCSF, that organizations may use to effectively and efficiently assess high risk areas and/or apply the HITRUST CSF risk factors to create a tailored set of control specifications and support control assessment and risk management activities.

Practical Action Plan for Implementing the HITRUST CSF

The HITRUST CSF is applicable to healthcare organizations of varying size and complexity due to incorporation of all major healthcare information security-related requirements and practices. In addition to the principle control categories contained in the ISO/IEC framework, the HITRUST CSF also includes specific categories for an "Information Security Management System" (ISMS) and risk management practices that help ensure organizational and system controls are properly specified and implemented.

To help ensure the success of an information security program and implementation of the HITRUST CSF, organizations should:

- Have the visible support and commitment of management before attempting to implement the HITRUST CSF
- Partition their organization into auditable business units

- Apply the HITRUST CSF to covered information such as PHI, regardless of the form
- Apply HITRUST CSF controls to all information systems irrelevant of, but appropriate to, their classification or function
- Have a good understanding of their information security requirements
- Educate and train employees at all levels
- Provide adequate resources for information security management
- Implement measurement systems to evaluate performance of information security management activities and controls

Introduction

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 HITRUST 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 HITRUST CSF and sound risk mitigation practices through the HITRUST 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 (see Appendix 1) to provide organizations of varying sizes and risk profiles with prescriptive implementation requirements. In doing so, the HITRUST CSF:

- Establishes a single benchmark for organizations to facilitate internal and external measurements that incorporate 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
- 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 are located under the *Downloads* section on the HITRUST Alliance Website:

- HITRUST CSF License Agreement
- Content Spotlight
- Publicly Available Downloads
  - MyCSF
  - HITRUST CSF, RMF & Related Documents
  - HITRUST CSF Assessors
  - HITRUST Cyber Threat Briefings
  - HITRUST CSF Assurance & Related Programs
- Frequently Asked Questions
- Industry Insights

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

- HITRUST Glossary of Terms and Acronyms
- HITRUST CSF Standards and Regulations Cross-Reference *(Accessed Through CSF Download)*
- HITRUST CSF Assurance Program Requirements
- HITRUST CSF Assessment Methodology
- HITRUST CSF Assessor Requirements
- HITRUST Risk Analysis Guide for HITRUST Organizations and Assessors
- HITRUST Risk Management Framework Frequently Asked Questions
- Healthcare Sector Cybersecurity Framework Implementation Guide

Organization of the HITRUST 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 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 HITRUST CSF is no more than what already applies to healthcare organizations. The HITRUST CSF was built to simplify these issues by providing direction for security tailored to the needs of the organization. The HITRUST 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 control objectives and control specifications based on the ISO/IEC 27001:2005 and ISO/IEC 27002:2005 standards. 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 leading practices of the HITRUST community are then integrated and normalized into specific requirements for each control. The result is an industry-level overlay of the NIST SP 800-53 moderate-impact minimum security control baseline that is extensively tailored for the healthcare community. The specific frameworks, standards and regulations applicable to each control are referenced as 'authoritative sources.'

Control Categories

The CSF contains 14 security Control Categories comprised of 46 Control Objectives and 149 Control Specifications. The CSF Control Categories, accompanied with the number of objectives and specifications for each category, 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, define, and manage the processes and resources that are necessary for the implementation of the rest of the HITRUST CSF.

Each Control Category contains the following:

- **Control Reference:** Control number and title.
- **Control Objective:** A statement of the desired result or purpose to be achieved by one or more controls within a HITRUST CSF Control Category.

Each control contains the following:

- **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.
- **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 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 HITRUST CSF, available as Illustrative Procedures in MyCSF, to provide clarity to both assessor organizations and those adopting the HITRUST CSF (e.g., by compliance or internal audit) when validating the security controls implemented by the organization against the requirements of the HITRUST CSF. This guidance includes examination of documentation, interviewing of personnel, and testing of technical implementation. Although illustrative, these procedures should be the starting point when performing an assessment and developing a test plan.

- **Standard Mapping:** The cross-reference between each Implementation Requirement Level and the requirements and controls of other common standards and regulations. While the document version of the HITRUST CSF release continues to consolidate mappings to its authoritative sources at the implementation level, mappings are now also provided for each industry segment. Mappings between individual HITRUST CSF implementation requirements and the HITRUST CSF authoritative sources are available in *MyCSF*.

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.

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[1] are defined based on the total inherent risk posed by the amount of sensitive information an organization holds and/or processes, or alternatively an annual number of records or the relative size of the organization based on a relevant estimator (e.g., number of beds, covered lives or transactions per year).

- Volume of business
  - Payer: Total or Annual Record Count / Number of Covered Lives
  - Hospital / Inpatient Facility: Total or Annual Record Count / Number of Admissions Per Year / Number of Licensed Beds
  - Pharmacy / Pharmacy Benefit Management: Total or Annual Record Count / Number of Prescriptions Per Year
  - Physician Practice: Total or Annual Record Count / Number of Patient Encounters Per Year / Number of Physicians
  - Health Information Exchange: Total or Annual Record Count / Number of Transactions Per Year
  - Service Provider (IT): Total or Annual Record Count / Data Volume

1. *Organizational risk factors were updated with the 2016 HITRUST CSF v8 release. For more information, refer to the HITRUST Risk Factors whitepaper available on the HITRUST Alliance website.*

- Service Provider (Non-IT): Total or Annual Record Count / Volume of Data Exchanged 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:

- Subject to PCI Compliance
- Subject to FISMA Compliance
- Subject to FTC Red Flags Rules
- Subject to the State of California Civil Code § 1798.81.5(a)(1)
- 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
- Subject to EHNAC Accreditation
- Subject to FFIEC IT Examination Requirements for Information Security
- Subject to FedRAMP Certification
- Subject to the EU GDPR
- Subject to 23 NYCRR 500

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

In general, for a system to increase from a Level 1 Implementation Requirement to Level 2 based on a system risk factor, the system must be processing covered information (e.g., 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 covered information, that system is only required to meet the Level 1 Implementation Requirements. However, if the entity has another system that DOES process covered information 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 total record count but must also be FISMA compliant (implementing and adhering to the controls of NIST), the organization must implement the Level 3 requirements of the HITRUST 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 HITRUST CSF requirements. Consequently, organizations may need to employ alternate security controls to mitigate risk or compensate for a system control failure. HITRUST developed an alternate control process to provide the means for organizations to meet HITRUST CSF requirements by deploying alternate controls as a substitute for a HITRUST CSF control specification. An alternate control is defined as a compensating control that has been submitted and approved for general use by the HITRUST Alternate Controls Committee. Alternate controls are generally employed by an organization in lieu of a management, operational or technical security control for the Level 1, 2 or 3 Implementation Requirements described in the HITRUST 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 HITRUST 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 (only for the purpose of HITRUST CSF certification); and
4. The organization assesses and formally accepts the risk associated with employing the alternate control for the information system.

Evolution of the HITRUST 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 HITRUST CSF stays relevant and current to the needs of healthcare organizations based on the demands of the industry.

The HITRUST CSF is designed to be easily adapted based on changes to the healthcare environment to address and incorporate new standards and regulations. HITRUST has done extensive work in the prior releases to harmonize NIST, CMS and the Minimum Acceptable Risk Safeguards for Exchanges (MARS-E) requirements, and better align and eliminate redundant requirements within the framework. HITRUST will continue streamlining the HITRUST CSF based on continued analysis of the framework's implementation requirements and recommendations from the HITRUST Community.

And, while HITRUST will continue integrating and normalizing relevant frameworks, standards, best practices and regulatory requirements, as needed, to ensure the CSF remains relevant to healthcare, HITRUST will also adapt the CSF structure and content to ensure it can be easily consumed by non-healthcare organizations.

With the growing threat to security and privacy, regardless of industry, HITRUST is seeing an increase in international adoption of the HITRUST CSF outside of the healthcare and public health sector. Recognizing the demand for increased cybersecurity, HITRUST is taking steps towards making the framework more agnostic, further enabling global adoption across a variety of industries.

CSF Assurance and MyCSF

CSF Assurance and MyCSF The HITRUST 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.

MyCSF allows an organization or HITRUST CSF Assessor to efficiently assess the high-risk areas of an environment, and/or apply the HITRUST CSF Risk Factors and Implementation Requirements to create a custom set of requirements tailored to an environment. This fully integrated, optimized, and powerful tool marries the content and

methodologies of the HITRUST CSF and CSF Assurance program. MyCSF makes it easier and more cost-effective for an organization to manage information risk and meet international, federal and state regulations concerning privacy and security. The MyCSF tool provides global organizations of all sizes with a purposefully designed, and engineered SaaS solution for performing risk assessments, corrective action plan management, enhanced benchmarking and dashboards, and integration with major GRC platforms and the HITRUST Assessment XChange®. MyCSF is a solution that will support an organization's evolving assessment needs that align with managing risk in the changing cyber threat, information risk and global regulatory landscape. 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.

By having a subscription to MyCSF, organizations both large and small will have complete access to the HITRUST CSF and 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.

Please visit the *HITRUST website* for more information on MyCSF.

Implementing the CSF

Industry experience and professional leading 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 HITRUST CSF. Management's active involvement and support are essential for success and, at minimum, should include written and oral statements of commitment to the importance of information security and recognition of its benefits. Management's clear understanding of purpose and their commitment to adopting the HITRUST CSF will help manage expectations and minimize problems around implementation efforts.

Scope

The HITRUST 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). However, an organization may wish to scope the organizational elements and/or systems subject to a HITRUST CSF assessment for specific business reasons.

Organization: The HITRUST CSF Assurance Program 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 HITRUST CSF Validated or HITRUST 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 HITRUST CSF, including application software components, databases, operating systems, interfaces, tools, and servers. When implementing the HITRUST CSF, it is appropriate to aggregate assets into one observation if the management, function, and environment allow the assets to be logically grouped.

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

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 HITRUST CSF addresses all areas of InfoSec governance and control as it relates to the healthcare industry. The HITRUST 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 2018 HITRUST CSF v9.1, thirty-seven (37) 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*
- American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria: *Security, Confidentiality and Availability*
- California Civil Code § 1798.81.5(b) (mapped to CIS CSC v6): *CA Attorney General Interpretation of "Reasonable Security Procedures"*
- Center for Internet Security (CIS) Critical Security Controls (CSC) v6: *Critical Security Controls for Effective Cyber Defense*
- 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 (with associated mappings to COBIT 5): Deliver and Support Section 5 – Ensure Systems Security
- Department of Homeland Security (DHS) Critical Resilience Review (CRR)
- EU General Data Protection Regulation (GDPR)
- Federal Register 21 CFR Part 11: *Electronic Records; Electronic Signatures*
- 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 Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook – Information Security, September, 2016
- Federal Register 21 CFR Part 11: *Electronic Records; Electronic Signatures*
- Federal Risk and Authorization Management Program (FedRAMP)
- Health Information Trust Alliance (HITRUST) De-Identification (De-ID) Framework: *De-identification Controls Assessment (DCA)*
- 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: *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 v2.0: *Catalog of Minimum Acceptable Risk Controls for Exchanges – Exchange Reference Architecture Supplement*
- New York State Department of Financial Services – Title 23 NYCRR Part 500
- 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*
- Office of Civil Rights (OCR) Audit Protocol April 2016 – HIPAA Security Rule
- Payment Card Industry (PCI) Data Security Standard Version 3.2: *Information Management (IM) Standards, Elements of Performance, and Scoring*
- Precision Medicine Initiative Data Security Policy Principles and Framework v1.0: *Achieving the Principles through a Precision Medicine Initiative Data Security Policy Framework*
- Texas Health and Safety Code § 181 – State of Texas: *Texas Medical Records Privacy Act*
- Title 1 Texas Administrative Code § 390.2 – State of Texas: *Standards Relating to the Electronic Exchange of Health Information*

Questions and Comments on the CSF

HITRUST encourages organizations to provide their comments to ensure the HITRUST 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 HITRUST CSF can do so by sending their comments via email to *info@hitrustalliance.net*.

About HITRUST

Founded in 2007, HITRUST Alliance is a not-for-profit organization whose mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from both the public and private sectors, HITRUST develops, maintains and provides broad access to its widely adopted common risk and compliance management and de-identification frameworks; related assessment and assurance methodologies; and initiatives advancing cyber sharing, analysis and resilience.

HITRUST actively participates in many efforts in government advocacy, community building and cybersecurity education. For more information, visit *www.HITRUSTAlliance.net*.

HITRUST®

855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net