HITRUST
Health Information Trust Alliance

Introduction to the HITRUST Common Security Framework

2014 – Version 6.0

HITRUST
Health Information Trust Alliance

Table of Contents

Executive Summary 3
Introduction 6
Organization of the CSF 8
- Key Components 8
- Control Categories 9
- Implementation Requirement Levels 10
- Segment Specific Requirements 11
- Risk Factors 11
- Alternate Controls 13
- Evolution of the CSF 13
- CSF Assurance Kit 14

Implementing the CSF 16
- Management Commitment 16
- Scope 16
- Organization 16
- Systems 16
- Implementation 17
- Critical Success Factors 17

Appendix 1 – Primary Reference Material 19

Executive Summary

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 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 Security Framework (CSF) than any and all organizations can use to create, access, store, or exchange Protected Health Information (PHI) safely and securely.

Organization of the CSF

The CSF is based on the 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

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- 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)
- Control Objectives for Information and related Technology (COBIT)
- Payment Card Industry (PCI) Data Security Standard
- State requirements (e.g., Nevada, Massachusetts, and Texas)
- Experiences and best practices of HITRUST participants

The CSF is organized by 13 Control Categories, which contain 42 Control Objectives and 135 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

CSF contains specific categories that provide additional requirements for these segments. Examples include 'CMS Contractors' and 'Health Information Exchanges.'

HITRUST also provides detailed assessment guidance and cross-references to the many authoritative sources incorporated into the framework, including detailed guidance on risk analysis for HITRUST organizations and CSF certified assessors published in the third quarter of 2013.

Although comprehensive and prescriptive, the 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 CSF requirement.

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

Practical Action Plan for Implementing the CSF

The CSF is applicable to healthcare organizations of varying size and complexity due to incorporation of all major healthcare information security-related requirements and best practices.

In addition to the principle control categories contained in the ISO/IEC framework, the CSF also includes specific categories for risk management. The CSF incorporates the concept of an "Information Security Management System" or ISMS that ensures processes are implemented in an organization to ensure organizational and system controls are properly implemented.

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

- Have the visible support and commitment of management before attempting to implement the CSF
- Partition their organization into auditable business units
- Apply the CSF to covered information such as PHI in all its aspects, regardless of the form the information takes
- Apply CSF controls to all information system irrelevant of 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 a measurement system to evaluate performance of information security management activities and controls

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 environment
- 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. 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 (see Appendix 1) 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 measurement 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
- 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 documents located under the Downloads section on HITRUST Central should be referenced for additional program background and using the CSF:

- HITRUST CSF Executive Summary
- 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

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 Cybersecurity Framework, 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.

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, PCI, COBIT, HITECH, 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 13 security Control Categories comprised of 42 Control Objectives and 135 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)

[1] Although not formally a part of CSF 2014 (v6), HITRUST has proposed a new Control Category, 13.0 Privacy Practices, to support Texas certification of the HIPAA Privacy Rule. Formal incorporation of privacy requirements into the CSF will occur once the HITRUST Board of Directors approves of the Privacy Working Group's recommendations. However, some of the supporting privacy requirements, which map to the existing 13 Control Categories, are included in this release

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 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.

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 (e.g., internal audit) when validating the security controls implemented by the organization against the requirements of the CSF. 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.

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 2014 are segment specific requirements for Texas covered entities and Federal Tax Information (FTI) custodians.

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.

Organization 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:

- Subject to PCI Compliance
- Subject to FISMA Compliance
- Subject to FTC Red Flags Rules
- Subject to HITECH Breach Notification Requirements
- 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)

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. The System Factors are:

- 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 an 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.

Factor Logic: 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 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 two 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 recommendations from the HITRUST Community, and plans to add the following sources in 2014 in two interim releases (versions 6.1 and 6.2):

- PCI DSS v3.0 (changes from v2.0)
- NIST Cybersecurity Framework v1.0
- ISO/IEC 27001:2013 and 27002:2013 (changes from 2005 releases)
- MARS-E Harmonized Security and Privacy Framework – Exchange Reference Architecture Supplement v1
- NIST HSR Toolkit (harmonization) (held over from 2013 pending updates from the 2013 release of NIST SP 900-53 r4 (final))
- OCR Audit Protocol (harmonization) (held over from 2013 pending release of new version)
- Recommendations from the HITRUST Privacy WG (including NIST SP 800-53 App J, HIPAA and GAPP) (pending completion of its work and formal Board approval)

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 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.

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 Protected Health Information (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.

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.

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 forum 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.

About HITRUST Central

The CSF in PDF format can be accessed through HITRUST Central – the industry's first managed online community for healthcare information security professionals. HITRUST Central is a resource for individuals who seek to enhance their organization's knowledge of information security and interact and collaborate with their peers. HITRUST Central boasts resources such as user forums, blogs, downloads, and education for all qualified subscribers.

Appendix 1 – 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 2014 CSF, eighteen (18) 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 2010 v1.5
  CMS Minimum Security Requirements for High Impact Data
- COBIT 4.1 and 5
  Deliver and Support Section 5 – Ensure Systems Security
- Encryption / Destruction Guidance – Federal Register 45 CSF Parts 160 and 164
  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 Sections 308, 310, 312, 314 and 316
  Health Insurance Reform: Security Standards
- ISO/IEC 27001:2005
  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 27799:2008
  Health informatics — Information security management in health using ISO/IEC 27002
- HITECH Act – Federal Register 45 CFR Parts 160 and 164

Breach Notification for Unsecured Protected Health Information; Interim Final Rule

- Joint Commission (formerly the Joint Commission on the Accreditation of Healthcare Organizations, JCAHO)
- NIST Special Publication 800-53 Revision 4 (Final)
  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 2.0
  Information Management (IM) Standards, Elements of Performance, and Scoring
- Texas Gen. Laws § 181 – State of Texas (aka "TX HB 300")
  Texas Medical Records Privacy Act