Information systems and data exchanges are considered fundamental for their potential to allow organizations to meet these objectives; however, the adoption of these technologies is highly regulated and introduces risks that require additional oversight and vigilance by the industry.

Healthcare organizations face multiple challenges relating to information security:

- Redundant and inconsistent requirements and standards.
- Confusion surrounding implementation and acceptable minimum controls.
- Inefficiencies associated with varying interpretations of control objectives and safeguards.
- Increasing scrutiny from regulators, auditors, underwriters, customers and business partners.
- Growing risk and liability, including data breaches, regulatory violations and extortion.

The Health Information Trust Alliance (HITRUST) believes that despite these challenges information security is critical to the broad adoption, utilization and confidence in health information systems, medical technologies and electronic exchanges. HITRUST, in collaboration with healthcare, business, technology and information security leaders, works to identify issues and obstacles to protecting information and develops approaches to standardize, streamline and simplify security in a manner that is applicable to all organizations in the healthcare industry.

The product of this collaboration is the HITRUST Common Security Framework (CSF), a certifiable framework that all healthcare organizations that create, access, store or exchange electronic health and other sensitive information can implement. By adopting the CSF, organizations can better protect their electronic information assets and build greater trust and efficiencies in the electronic flow of information within the healthcare system.
The Common Security Framework

The most widely-adopted security framework in the U.S. healthcare industry and an invaluable tool for healthcare security professionals, the CSF provides organizations with the needed structure, detail and clarity relating to information security that is tailored to the healthcare industry. It includes a prescriptive set of controls and supporting requirements that clearly define how organizations meet the objectives of the framework. According to type, size and complexity of the organization and its systems, the controls scale through multiple levels of implementation requirements that are based on risk-contributing factors.

The HITRUST CSF also addresses the challenges of the industry by leveraging and cross-referencing existing standards and regulations. This avoids introducing redundancy and ambiguity into the industry and helps simplify an organization’s compliance efforts. The CSF normalizes these sources in such a way that organizations can quickly understand their compliance status across a wide range of standards and authoritative sources.

By implementing the CSF, organizations will have a common security baseline and a method for communicating validated security controls to all of their constituents.

Organization of the CSF

The HITRUST CSF is a comprehensive tool developed to aid organizations that create, store, access or exchange electronic health and other sensitive information. The CSF is comprised of two components — Information Security Implementation Manual, and Standards and Regulations Mapping.

Information Security Implementation Manual

The Information Security Implementation Manual is a certifiable, best-practice-based specification that scales according to the type, size and complexity of an organization’s environment to provide prescriptive implementation guidance. It includes both recommended security governance practices (e.g., organization, policies, etc.) and sound security control practices (e.g., people, process, technology) to ensure the effective and efficient management of information security.

Control Framework

The Implementation Manual contains 13 security control categories comprised of 42 control objectives and 135 control specifications. The categories included in the Manual are:

- Information Security Management Program
- Access Control
- Human Resources Security
- Risk Management
- Security Policy
- Organization of Information Security
- Compliance
- Asset Management
- Physical and Environmental Security
- Communications and Operations Management
- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity Management

Enhancements to the CSF Version 6.0

HITRUST provides regular updates to the CSF to ensure it remains relevant to the organizations that rely upon it to address evolving security requirements and maintain regulatory compliance. Recent updates include new guidance pertaining to:

- State of Texas Standards
- NIST 800 Series Harmonization
- Updated CMS Contractor Requirements
- Updated Illustrative Procedures and Administrative Guidance
By implementing the CSF, organizations will have a common security baseline and method for communicating validated security controls to all of their constituents.

**Alternate Controls**

With the diverse nature of today's information systems, organizations may find it difficult or not practical to meet the CSF's requirements. Because of this, the CSF supports a concept of approved Alternate Controls as a risk mitigation or compensation strategy for a system control failure. HITRUST has defined an alternate control process that provides for the streamlined proposal, approval and implementation of Alternate Controls across all organizations. This allows the entire industry to continually improve its security and compliance stance. An Alternate Control is defined as a management, operational or technical control (i.e., safeguard or countermeasure) that can be employed by an organization in lieu of the level 1, 2 or 3 implementation requirements defined in the CSF that provides equivalent or comparable protection for an organization's information system.

**Standards and Regulations Mapping**

The Standards and Regulations Mapping tool reconciles the HITRUST CSF with multiple common and accepted standards and regulations applicable to healthcare organizations.

The tool maps each control specification and implementation requirement so that one can clearly understand the alignment between HITRUST's requirements and those of other standards, thus aiding compliance efforts. In addition, the Mapping identifies any gaps not addressed by other sets of requirements that are covered by the HITRUST CSF. The tool gives organizations a 360° perspective of their information security landscape. Covered standards and regulations include:

- ISO/IEC 27001:2005
- ISO/IEC 27002:2005
- COBIT 5
- HIPAA
- NIST SP 800-53 Revision 4
- NIST SP 800-66
- PCI DSS version 2.0
- 16 CFR Part 681
- FTC Red Flags Rule
- HITECH Act
- 21 CFR Part 11
- JCAHO IM
- 201 CMR 17.00 (State of Mass.)
- NRS 603A (State of Nev.)
- CSA Cloud Controls Matrix v1
- CMS ARS
- TX HB 300
- CAQH CORE
Implementing the CSF

Implementation of the HITRUST CSF will vary by organization in both time commitment and level of effort. This can be due to several factors, including:

- Complexity of the individual organization’s information systems environment.
- Maturity of the current security processes and controls.
- Number of resources available to the organization.

Despite these variations, all organizations can follow the same process in preparing for and performing an assessment of their existing infrastructure against the CSF. This consistent process allows organizations to feel secure in the success of their CSF implementations and confident that other organizations have performed equal due diligence to achieve compliance with the CSF.

Access your copy of the CSF

A subscription to MyCSF is available for an annual fee based on organization type and provides access for five individuals in the purchasing organization to access MyCSF View, MyCSF Assessment and MyCSF Benchmarking. The annual subscription price for MyCSF is $7,500 for qualified organizations and $10,000 for all other organizations (i.e., professional services and technology organizations). To learn more about a subscription to MyCSF, download the MyCSF datasheet.

For more information about HITRUST, the HITRUST CSF and other HITRUST offerings and programs, visit HITRUSTalliance.net.

About HITRUST

The Health Information Trust Alliance (HITRUST) was born out of the belief that information security should be a core pillar or, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST, in collaboration with healthcare, business, technology and information security leaders, has established the Common Security Framework (CSF), a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal health and financial information. Beyond the establishment of the CSF, HITRUST is also driving the adoption of and widespread confidence in the framework and sound risk management practices through awareness, education, advocacy and other outreach activities.

* A qualified organization is any organization employing a function or activity involving the use or disclosure of individually identifiable health information, provided that said organization does not provide security products or services. Additionally, any federal, state, or local agency or department may qualify. HITRUST has the right to verify eligibility.