The HITRUST CSF

A Revolutionary Way to Protect Electronic Health Information
Organizations in the healthcare industry are under immense pressure to improve quality, reduce complexity, increase efficiency and better manage medical expenses.

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 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 HITRUST CSF

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 other 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.

Enhancements to the CSF Version 7.0

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:

- HIPAA Privacy Rule
- NIST SP 800-53 r4, Appendix J, Privacy Control Catalog
- Catalog of Minimum Acceptable Risk Controls for Exchanges—Exchange Reference Supplement v1
- CMS Information Systems Acceptable Risk Safeguards, Appendix A, CMS High Impact Level Data, v2

Organization of the CSF

The HITRUST CSF is a comprehensive framework 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 Requirements and a Standards and Regulations Mapping.
Information Security Implementation Requirements

The CSF’s Information Security Implementation Requirements provide certifiable, best-practice-based specifications that scale 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 CSF contains 14 security control categories comprised of 45 control objectives and 149 control specifications. The CSF Control Categories, along with the number of Objectives and Specifications, are:

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

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 helps reconcile 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:

- 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 (with associated mappings to COBIT 5): Deliver and Support Section 5 – Ensure Systems Security
- 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
- 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)
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.
Assessing Against the CSF

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.

HITRUST CSF Assessment Activities

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Project Startup</td>
</tr>
<tr>
<td>2</td>
<td>Define Organizational Scope</td>
</tr>
<tr>
<td>3</td>
<td>Define System Scope</td>
</tr>
<tr>
<td>4</td>
<td>Examine Documentation &amp; Practices</td>
</tr>
<tr>
<td>5</td>
<td>Conduct Interviews</td>
</tr>
<tr>
<td>6</td>
<td>Perform/Review Technical Testing</td>
</tr>
<tr>
<td>7</td>
<td>Alternate Control Identification and Selection</td>
</tr>
<tr>
<td>8</td>
<td>Reporting</td>
</tr>
<tr>
<td>9</td>
<td>Remediation Tracking</td>
</tr>
</tbody>
</table>

Inputs:
- Resource requirements
- Project management tools
- Available resources
- Organization chart
- Business unit contact information
- Asset inventory list
- Information classification
- Policies and procedures
- Prior assessment reports
- Auditing and monitoring records and logs
- Observable practices
- Management
- System owners
- Key stakeholders
- Detailed configuration settings
- Vulnerability scans
- Penetration tests
- Noncompliant CSF controls
- Analysis of results with observations

Outputs:
- Staffed project
- Project management processes
- Identified key stakeholders including site coordinator
- Identified business unit information entered into tool
- Identified system owners
- Identified information system information entered into tool
- Identified high risk areas (storage, processing or transmission of ePHI)
- Policies, procedures and supporting documents for each bus. unit system
- Documented findings, if any
- Inherent compliance score
- Documented findings, if any
- Inherent compliance score
- Documented findings, if any
- Inherent compliance score
- Data entered into MyCSF assessment
- Remediation plan
- Residual compliance score
- Final report
- Remediation plan
- Management response
- Remediation of highest risk areas of noncompliance
- Residual compliance score
Access your Copy of the CSF

MyCSF is a full-featured, user-friendly, fully-integrated and managed tool that streamlines the entire information compliance and risk management process, from policy creation, approval and publication to risk assessment and remediation as well as incident and exception management. The optimized and powerful tool marries the content and methodologies of the CSF and CSF Assurance Program with the technology and capabilities of a governance, risk and compliance (GRC) tool.

Offered as a service, MyCSF provides healthcare organizations of all types and sizes a fully integrated, web-based solution for accessing the HITRUST CSF. In addition, it incorporates content and features for managing policies, performing assessments, streamlining remediation activities, reporting and tracking compliance and servicing exceptions and incidents.

There are two ways to access MyCSF; purchase a self/validated assessment report or purchase a subscription.

**Self/Validated Assessment Reports:** This access, known as “assess only” is limited to 90 days and grants an organization access to perform an assessment and receive their report. After 90 days, an organization no longer has access and the information is no longer available. Any subsequent assessments will then be performed from scratch.

**MyCSF Subscription:** With a subscription to MyCSF, organizations receive complete access to the CSF and authoritative sources, as well as the expanded benefit of having 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 to report on their progress. Subscriptions vary in relation to users, assessments and functionality. To learn more about a subscription to MyCSF, contact sales@hitrustalliance.net to best determine which configuration will best meet your needs.

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 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.