



The HITRUST Common Security Framework:

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 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

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 4.0

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:

- NIST Special Publication 800-53 Revision 3
- Centers for Medicare and Medicaid Services (CMS) Information Security Acceptable Risk Safeguards (ARS)
- CMS Minimum Security Requirements version 1.0 (CMSR v1.0)
- Payment Card Industry Data Security Standard (PCI-DSS) v2.0
- Input from HITRUST Health Information Exchange and Mobile Device Working Groups
- Industry recommendations and loss data trend analysis

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. HTRUST 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.

The tool maps each control specification and implementation requirement so that one can clearly understand the alignment between HTRUST'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 HTRUST 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
- ISO/IEC 27799:2008
- COBIT 4.1
- HIPAA
- NIST SP 800-53 Revision 3
- 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

Standards and Regulations Mapping

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

HITRUST
CSF Controls - 01 Password Management System

Control Reference: 01 / Password Management System
Control Description: System for managing passwords shall be introduced and shall ensure quality passwords.
Control Objective: 01-01 Access Control
 01-01-01 Operating System Access Control

Level 1 Implementation Requirement

Level 1 Operational Factors: None

Level 1 Regulatory Factors: Processing PWD, No - AND - Accountable for the control: No
 Number of Days: 300
 Escalation: Yes
 Third Party: Yes
 Publicly Available: No

Level 1 System Factors: None

Level 1 Implementation: Refer to Sections 1 and 11 for a full list of password controls. In addition, a password management system shall be implemented to:

1. require the user of individual user IDs and passwords to maintain accountability;
2. ensure that user IDs and passwords are never presented and include a workstation procedure to allow for rapid account lockout;
3. be updated to change temporary passwords at the first log on (see 1.3);
4. be used only once to be secure when logging on;
5. ensure change window is not available before existing systems on the network including password, single sign-on management protocol (SSMPP), connectivity setup and the alteration of unnecessary accounts.

Level 1 Control Audit Procedure:

Control: 1. The policy and procedures for password management to ensure the initiation and enforcement of passwords is defined and controlled.

Interview: 1. Semi-structured interview to ensure IDs are linked to individual responsibility and control of access.
 2. Document evidence collected to ensure temporary passwords must be changed at the first log on.

Test: 1. The operating systems on critical systems to ensure that passwords are:

Confidential Page 3 3/1/2009
 This document is the HTRUST CSF and CSF Controls. It is the property of HTRUST, LLC. It may be used, modified or reproduced in whole or in part, without the express written permission of HTRUST, LLC.

HITRUST

Not displayed on the screen when being printed

Level 1 Control Standard Mapping: • HIPAA 164.308 (a)(2)(ii)

Control ID	Control Type	Control Description
01-01-01-01	Compensating	Systems shall use algorithms and other based access controls (operational or operating management systems (e.g., fire, antibodies, access control lists, security state, threat-control security team, database sub-external) to control access to data.

Level 2 Implementation Requirement

Level 2 Operational Factors: None

Level 2 Regulatory Factors: Subject to POC Compliance
 Processing PWD, Yes - AND - Accountable for the control: Yes
 Number of Days: 300
 Escalation: Yes
 Third Party Support: Yes
 Publicly Available: Yes

Level 2 System Factors: None

Level 2 Implementation: Refer to Sections 1 and 11 for a full list of password controls. The password management system shall:

1. store and transmit passwords in protected (e.g. encrypted or hashed) form;
2. store passwords from separately from application systems data;
3. ensure a record of security incidents (SI);
4. update password changes (see 01-01-01-01).

Level 2 Control Audit Procedure:

Control: 1. Semi-structured interview responsible for information security to verify that similar mapped details are always changed before installing a system or on the network.

Confidential Page 3 3/1/2009
 This document is the HTRUST CSF and CSF Controls. It is the property of HTRUST, LLC. It may be used, modified or reproduced in whole or in part, without the express written permission of HTRUST, LLC.

HITRUST

Test: 1. The operating systems on critical systems using host IDs or accounts to validate that the selection of passwords is consistent with the requirement in place (e.g. strong passwords used for servers).
 2. The operational systems on the systems to ensure that any version-specific operational systems have been changed.

Level 2 Control Standard Mapping:

Control ID	Control Type	Control Description
01-01-01-01-01	Compensating	Systems shall use cryptography to encrypt data exchanged to authenticate user access.

Level 2 Operational Factors: None

Level 2 Regulatory Factors: None

Level 2 System Factors: No additional requirements

Level 2 Control Audit Procedure: None

Level 3 Alternate Controls

Control Name	Control ID	Control Type	Control Description
No records identified.			

Confidential Page 3 3/1/2009
 This document is the HTRUST CSF and CSF Controls. It is the property of HTRUST, LLC. It may be used, modified or reproduced in whole or in part, without the express written permission of HTRUST, LLC.

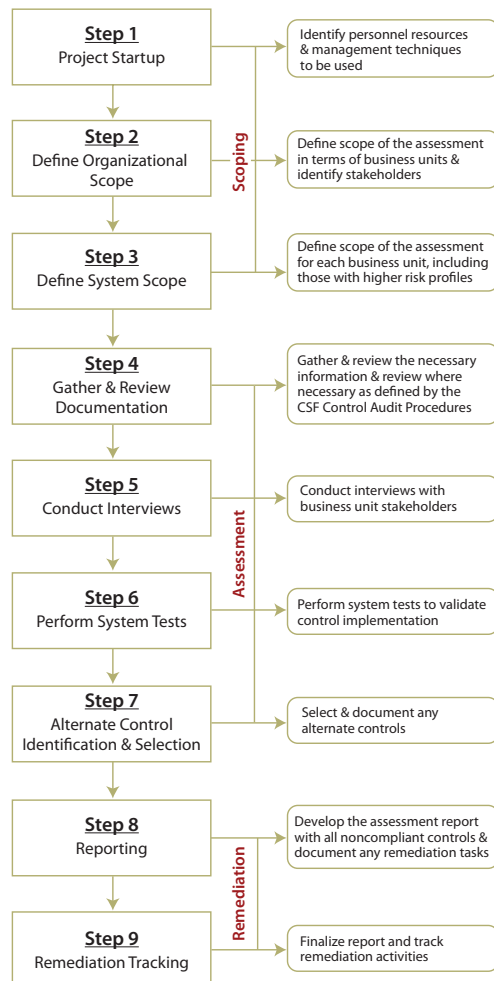
Implementing the CSF

Implementation of the HTRUST 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.

HTRUST CSF Implementation and Assessment Activities



Access your copy of the CSF

The HTRUST CSF is available by subscribing to HTRUST Central, the online community for healthcare information security professionals.

Individuals can register for one of two annual subscription options – Standard and Professional. A Standard subscription, which includes access to the core CSF, is available at no charge to individuals from qualified organizations* and Professional subscriptions are available for an annual fee based on organization type. The Professional subscription provides access for five individuals in the purchasing organization to access HTRUST Central and the online, interactive version of the CSF, authoritative sources and the CSF Assurance Toolkit. The annual price of the Professional version is \$5,500 for qualified organizations and \$10,000** for all other organizations (i.e., professional services and technology organizations).

To learn more about the subscription levels, visit www.hitrustalliance.net/csf/hitrust_central_information, or to register, visit **HTRUST Central**.

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

About HTRUST

The Health Information Trust Alliance (HTRUST) 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. HTRUST, 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, HTRUST 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 technology or security products or services**. Additionally, any federal, state, or local agency or department may qualify for a Standard subscription. HTRUST has the right to verify eligibility.

** Includes one seat in HTRUST Training for Practitioners