HIPAA HITRUST Compliance Certificate

**GOOGLE: HIPAA HITRUST Compliance Certificate**
OR https://blog.rsisecurity.com/hitrust-compliance-what-you-need-to-know/


# HITRUST COMPLIANCE: WHAT YOU NEED TO KNOW

## What is HITRUST

The Healthcare Information Trust Alliance (HITRUST) is an independent organization that partners with government and information security professionals working to create programs that safeguard sensitive information. According to the HITRUST website, HITRUST "develops, maintains and provides broad access to its widely-adopted common risk and compliance management frameworks, related assessment and assurance methodologies."

Individual business needs vary depending on the amount and type of patient data. As the compliance landscape becomes more complex, understanding HIPAA, HITECH, or CMS requirements is a difficult task. HITRUST issues the Certified Security Framework (CSF) certification to businesses that can successfully meet the rigorous requirements. This framework covers compliance requirements for industry standards. HITRUST compliance shows that the vendor has met the requirements for managing and protecting sensitive patient data.

## Why HITRUST

The healthcare industry handles copious amounts of data which is extremely sensitive in nature. As technology continues to improve in gathering and storing more data, challenges arise of keeping that data secure. Some of the challenges might include:

- Poor management techniques resulting in uniformed employees
- Increased public fear of data breaches or loss of sensitive information
- Augmented scrutiny from business partners, clients, or external auditors
- Inability to implement basic security controls largely in part due to rapidly changing security protocol environments
- Redundant or unclear information security regulations for diverse healthcare organizations

To tackle these challenges, the HITRUST Alliance created a framework that effectively encapsulates and minimizes the confusion surrounding compliance requirements.

## Certified Security Framework Certification

According to the HITRUST website, the CSF certification serves to encapsulate the necessary "regulations and standards into a single overarching security framework." As mentioned before, with a complex compliance landscape, the benefit of seeking CSF certification means that the vendor can "tailor the security control baselines based on a variety of factors including organization type, size, systems, and regulatory requirements."

In other words, what this certification does is give a solid foundation upon which vendors can then build strong security protocols matching their needs. This certification provides a comprehensive set of baseline security measures meeting the standards of industry controls such as ISO, NIST, PCI, and HIPAA.

Think of this certification as a TSA Pre-Check at the airport. If you adhere to the rules and regulations outlined by the TSA, you can quickly pass by the security checks unlike the other passengers who must run through a complete check each time they choose to fly. Through obtaining a CSF certification, you meet the standard requirements for a wide range of industry controls like those listed above.

## Industry Controls

For more information on these important compliance practices, please refer to RSI Security articles on these industry controls under How to Improve your Security with NIST, PCI DSS Assessment, HIPAA Compliance Checklist.

The HITRUST Alliance outlines on its website that CSF Certification:

- Includes, harmonizes, and cross-references existing, globally recognized standards, regulations and business requirements, including ISO, NIST, PCI, HIPAA, and State laws
- Scales controls according to type, size, and complexity of an organization
- Provides prescriptive requirements to ensure clarity
- Follows a risk-based approach offering multiple levels of implementation requirements determined by specific risk thresholds
- Allows for the adoption of alternate controls when necessary
- Evolves according to user input and changing conditions in the industry and regulatory environment on an annual basis
- Provides an industry-wide approach for managing Business Associate compliance

## Risk Factors

Each vendor has different requirements for HITRUST compliance depending on the specifications of their business. The following risk factors are those outlined by the HITRUST Alliance (HITRUST Executive Report) and are separated into organizational factors, regulatory factors, and system factors.

## Organizational Factors

These factors are dependent upon the complexity and size of the organization.
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

These factors are contingent upon the applicable compliance requirements for an organization. You may need to meet a variety of these compliance requirements. Vendors may be:

- 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

Systems factors are attributes within a security system that increase the chance of a data breach or mismanagement of said data. The following attributes factor into increased risks for data management:

- Stores, processes, or transmits PHI (Protected Health Information)
- Accessible from the Internet
- Accessible by a third party
- Exchanges data with a third party/business party
- Publicly accessible
- Mobile devices are used
- Connects with or exchanges data with a HIE (Health Information Exchange)
- Number of Interfaces to other systems
- Number of users
- Number of transactions per day

## Alternate Controls

Admittedly, you may be a vendor that cannot match all the controls as dictated by a CSF auditor. HITRUST Alliance has come up with an arrangement for those who may need to employ a substitution of their standard security measures. The

Alliance has defined an alternate control 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.”
These alternate controls may only be employed by an organization under specific conditions which are:

1. The organization selects the alternate control(s) from the CSF, or if an alternate appropriate 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
4. The organization assesses and formally accepts the risk associated with employing the alternate control for the information system

Or to put it more simply, your organization may employ a different security control, but the HITRUST Alliance does not recommend it due to the inherent risks of dynamic threats. The goal of HITRUST is to get your organization up to standard. Nevertheless, HITRUST compliance does allow a personalized approach that can ease the vendor’s fears about the high standards.

## Steps to Become HITRUST CSF Certified

The first thing to note is that the HITRUST Alliance does allow vendors to perform self-assessments. You can first perform a self-audit by accessing the HITRUST Alliance’s portal called MyCSF. MyCSF Portal This tool can help you determine problematic gaps within your security protocols. You may also opt to be assessed by a CSF auditor who will perform a full spectrum risk assessment. After you have determined the required risk management strategy, be sure to set an implementation timeline and steps to bring your organization up to speed. This includes meeting the basic requirements of ISO (International Organization for Standardization) before seeking a CSF certificate.
According to the HITRUST executive report , there are several factors that vendors should be aware of to best meet CSF requirements:

- 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 the performance of information security management activities and controls

## Cost

HITRUST compliance can be an expensive certification to obtain, but there are many benefits to having this certification. HITRUST Validated Assessment fees range from $40,000 to $250,000 per year depending on the risk factors as detailed above. These high costs come from the vast amount of control categories that are assessed by an auditor.

One way to potentially increase benefit for your organization is to combine a HITRUST CSF certification with a SOC 2 (System and Organizational Control) report. You can read more about SOC 2 compliance in our article SOC 2 Compliance Requirements.

You should note that with a regular SOC 2 report, you are only required to meet the necessary security standards outlined in the five trust service principles. The rigorous nature of HITRUST compliancerequires that businesses also test two additional trust service principles of availability and confidentiality.

## CSF Certification Process

Due to the nature of the sensitivity of the patient data, HITRUST audits are long and extremely thorough. Over several months, the alliance conducts multiple rounds of security audits testing for vulnerabilities.

Image source: https://hitrustalliance.net/the-hitrust-approach/

The vendor is given ample opportunity to adapt their security protocols as dictated by the reports of the initial audits from the reviewer. After multiple

iterations of testing vulnerabilities and reconfiguring security measures, the vendor is awarded a CSF certification.

## Control Categories

The CSF certification process has specific control categories designed to test for best security practices. The executive CSF report HITRUST Executive Report outlines that there are "13 security Control Categories comprised of 42 Control Objectives and 135 Control Specifications." These categories include:

1. Information Security Management Program
2. Access Control
3. Human Resources Security
4. Risk Management
5. Security Policy
6. Organization of Information Security
7. Compliance
8. Asset management
9. Physical and Environmental Security
10. Communications and Operations Management
11. Information Systems Acquisition, Development, and Maintenance
12. Information Security Incident Management
13. Business Continuity Management

All these control categories and subsequent control objectives and specifications are equally important and should be carefully addressed in the self-assessment process. HITRUST compliance may seem an overwhelming process but is tailored to best serve the needs of vendor's handling such sensitive patient data.

## HITRUST Compliance Timeline

According to the HITRUST FAQs page, the length of time required to become HITRUST CSF certified varies depending on the initial readiness level of the company. The amount of remediation needed to fully implement all the requirements for the scope of the audit also affect the time for certification. "In general, it can take up to 3-4 months to complete the assessment and obtain certification once an organization is ready."

This FAQ page is a great resource for approaching concerns with HITRUST compliance. It is organized to help you determine what is expected of you as a vendor and what threats you may face.

This process is specifically suited to best meet the needs of each organization. Should you still have questions or concerns after reading this guide and the reports by the HITRUST Alliance, call us for a free consultation with one of our experts who will help prepare you for a HITRUST CSF audit.
Each certification is valid for two years. At the end of the two-years, any vendor looking for recertification must go again through the entire assessment and validation process. This ensures that the vendor maintains the most up-to-date security measures and technology.

## HITRUST Compliance Advantages

There are several advantages to obtaining and maintaining HITRUST compliance. For instance, due to the nature of the HITRUST two-year certification period before requiring reassessment, you can confidently know that you are meeting excellent security criteria.
This certification also proves to companies with who you do business that you can more than adequately manage and protect sensitive data. Finally, HITRUST CSF certification is an overarching framework that guarantees healthcare vendors will sufficiently meet a wide range of industry standards.
Health IT Outcomes cites that because the requirements of HIPAA and HITECH are incorporated into the HITRUST framework, 83% of hospitals and healthcare providers have become HITRUST compliant. Since the standard of excellence is so high for companies to be certified, many healthcare payers are requiring vendors to become CSF certified. More than 90 healthcare payers request their vendors to seek certification.
At RSI Security, we offer top of the line service on making sure companies meet the HITRUST compliance certification requirements, contact us now.