HITRUST Compliance

Protecting sensitive information must be an absolute priority for all organizations. Between ever-evolving security threats and increasingly complex government regulations, it's difficult to stay on top of the necessary security measures to keep information safe while remaining compliant. HITRUST sets the standard for healthcare information security for any entity that handles PHI or other sensitive data.

What Is HITRUST?

HITRUST is a private organization made up of providers (hospitals, physician practices, etc.) and payers (insurance companies) that created a certifiable common security framework for healthcare technology security: HITRUST CSF.

The HITRUST CSF is a detailed map of specific security measures to take in order to meet compliance requirements.

Its sophisticated, evolving set of control requirements protects against the various security, privacy, and regulatory challenges facing healthcare entities, as well as those in other industries, in order to help them comply with healthcare (HIPAA, HITECH), government (NIST, FTC), third-party (GDPR, PCI, COBIT), and state-specific standards, regulations, and business requirements. It also provides tools for governance and risk management.

Why HITRUST?

Achieving HITRUST CSF Certification can make you a more attractive option for consumers because it displays a deep commitment to protecting patients' and customers' sensitive data.

It safeguards against the government fines, criminal charges and reputational damages that can result from noncompliance.

Many of the large payers are requiring entities they contract with to be HITRUST-Certified.

If you implement the HITRUST CSF, you can leverage testing results in your reporting for multiple compliance efforts.

Who Needs HITRUST?

Organizations that handle sensitive information, such as covered entities in the healthcare industry, looking to bolster security and improve risk management.

The business associates of covered entities

The HITECH Act extended HIPAA requirements to organizations that conduct business with healthcare entities and handle sensitive health information. Health information exchanges, CPA firms, and medical transcriptionists are a few examples.

Why KraftCPAs?

KraftCPAs has earned the designation of HITRUST CSF Assessor. Our team of HITRUST-Certified CSF Practitioners (CCSFPs) has been extensively trained in HITRUST and the CSF requirements.

They also participate in ongoing annual training and recertification every three years. Thus, we can efficiently and effectively perform services to address the multitude of security, privacy, and regulatory challenges facing your organization.

KraftCPAs and affiliates also work extensively with clients in the healthcare industry; healthcare is our largest industry concentration in terms of revenue and dedicated staff.

KraftCPAs
PLLC

HITRUST Compliance

CONTACT
615-242-7353 ext. 190
risk@kraftcpas.com
kraftcpas.com/HITRUST

HITRUST CSF Certification

The path to CSF certification is neither quick nor easy, but our CCSFPs are trained to help you every step of the way. The process consists of three components:

GAP Analysis

We will review your current control environment in order to identify gaps between current controls and the minimum HITRUST requirements.

Readiness Assessment Consulting/Facilitation

After you purchase the HITRUST Readiness Report and/or a subscription to the CSF GRC Tool, we can assist you in completing the information and questions in the Readiness Assessment. This process will allow us to identify your customized population of HITRUST requirements based on your individualized risk factors (e.g., size, transactions, cloud services, etc.) and identify controls to meet those risk factors.

This process results in a report which can be provided to third parties to show that you're committed to meeting the requirements of HITRUST. This report is not validated by HITRUST and does not result in certification, but it is a step in the right direction because it provides the starting point for us to test your HITRUST requirements, as explained in the next section.

Assessment for Validation/Certification

Once you've identified the HITRUST control requirements and implementation level, you will enter your controls for the related HITRUST requirements in the CSF tool. As your assessor, we will perform an independent assessment and testing of those controls to determine compliance with HITRUST requirements and submit the results to HITRUST on your behalf. HITRUST will review the assessment and determine compliance with the HITRUST CSF. The process can result in:

HITRUST Validation (and CAP Report)
Once reviewed by HITRUST, you will receive a validated report. If some areas do not meet the compliance threshold, you will be required by HITRUST to prepare and submit a corrective action plan (CAP) report. We are able to assist with validating the remediation of the items noted in the CAP report.

HITRUST Certification (and CAP Report, if necessary)
If HITRUST deems that you are in compliance with the CSF requirements, you will receive a certification letter with your validated report. HITRUST certification is good for two years, as long as you complete an interim review and there are no breaches or significant changes in scope during that time. (Certified organizations can also be required to prepare and submit a CAP report.)

HITRUST Corrective Action Plan Reports

If the assessment results in scores below HITRUST's compliance threshold on particular areas, HITRUST requires that you prepare a CAP report to address the gaps. As your assessor, we will evaluate the effectiveness of the CAP and provide recommendations or feedback as needed. We can assist you with articulation and prioritization of your plan. If you achieve certification, we will continue to monitor your remediation progress in the interim review.

Gina Pruitt

Scott Nalley

KraftCPAs PLLC

HITRUST RightStart Program™

Implementing a risk management and compliance program is often challenging for start-up companies due to costs and the strain on internal resources. HITRUST started a program to help start-up companies begin using the HITRUST CSF so that they can build a solid foundation around privacy and security. The program includes training and use of the MyCSF platform, making it easier and less costly to implement. We can help you determine if you qualify for the program, and we can assist you with the implementation.

SOC 2 + HITRUST

As our HITRUST-Certified Practitioners are also CPAs, our team can satisfy both HITRUST and SOC 2 reporting needs for your organization. HITRUST and the American Institute of CPAs have collaborated to make HITRUST CSF and SOC 2 reporting complementary. The reports we can assist with include:

Gap Analysis: A review of your current control environment that identifies gaps between current controls, SOC criteria, and the minimum HITRUST requirements

SOC 2 Only: A service auditor's report detailing how your organization protects the security, availability, and confidentiality of user data

SOC 2 + HITRUST CSF: A SOC 2 report that also expresses an opinion on whether your controls meet the HITRUST CSF requirements

SOC 2 + HITRUST CSF + CSF Certification: One combined report for organizations that have received a SOC 2 + HITRUST CSF report and also received the HITRUST CSF Certification

HITRUST
Authorized CSF Assessor

KraftCPAs is a HITRUST Authorized CSF Assesor firm. Developed in collaboration with healthcare and information security professionals, the HITRUST CSF is the most widely-adopted security framework in the U.S. healthcare industry.

© KraftCPAs PLLC Feb. 2020