ClearDATA
SECURE • HEALTHCARE • CLOUD

Overcome Healthcare Security and Compliance Challenges

ClearDATA and HITRUST

What is HITRUST?

The Health Information Trust Alliance (HITRUST) was born out of the belief that information security and privacy should be a core pillar of, 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 HITRUST 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 HITRUST 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.

An integral component to achieving the HITRUST goal of advancing the healthcare industry's protection of health information is the establishment of a practical mechanism for validating an organization's compliance with the HITRUST CSF. According to HITRUST Alliance, HITRUST CSF is the most widely adopted security framework in the healthcare industry[1].

The HITRUST CSF is an overarching security framework that incorporates and leverages the existing security requirements placed upon healthcare organizations, including federal (e.g., HIPAA and HITECH), state, third party (e.g., PCI and COBIT), and other government agencies (e.g., NIST and FTC). The HITRUST CSF – healthcare's model implementation of the NIST

Framework for Improving Critical Infrastructure Cybersecurity – is already being widely adopted by leading healthcare payers, providers, and state exchanges as their security framework.

HITRUST has developed the HITRUST CSF Assurance program, which encompasses the common requirements, methodology and tools that enable both healthcare organizations and their business partners to take a consistent and incremental approach to managing compliance. This program is the mechanism that allows healthcare organizations and their business partners to assess and report against multiple sets of requirements. Unlike other programs in healthcare and in other industries, the oversight, vetting, and governance provided by HITRUST affords greater assurances and security across the industry.

ClearDATA Advantage

The HITRUST CSF is divided into nineteen different domains, including end point protection, mobile device security, and access control. HITRUST certifies IT offerings against these controls. HITRUST also adapts requirements for certification to the risks of an organization based on organizational, system, and regulatory factors.

A public cloud serves many industries; therefore, their HITRUST certification will usually be limited to the cloud's scope of services – that is the IaaS, PaaS or in some cases even SaaS. In contrast, ClearDATA exclusively serves healthcare organizations and the solution providers that support healthcare. ClearDATA's scope of assessment is much more expansive, encompassing a broader scope of series, including policies and procedures specific to its PHI environments under AWS, Azure and soon Google public clouds.

In addition to HITRUST, ClearDATA's responsive platform is backed by the most comprehensive Business Associate Agreement (BAA) in the industry, providing contractual commitment for risk mitigation and ongoing security. As healthcare security and compliance experts, ClearDATA provides a BAA that ensures full and purposeful coverage, negating the need for a separate BAA from public cloud providers. ClearDATA's BAA covers not only foundation layers (i.e. compute, storage, database) and services but also supports operating systems, network, firewall, and public ClearDATA platform layers.

ClearDATA HITRUST Inheritance Program

The HITRUST CSF Inheritance Program[2] enables hosting, cloud, and service providers to make assessment scores available for inheritance to ClearDATA customers.

This program simplifies the process and reduces the effort for hosting and service organizations. By working with a participating managed service provider such as ClearDATA, customers can reduce the required testing and associated costs for inherited controls in a fully automated manner.

Why HITRUST Inheritance?

Healthcare organizations can leverage ClearDATA with HITRUST to simplify their own CSF Assessments in order to manage the daunting task of securing their sensitive data (PHI).

What domains may a customer inherit from ClearDATA HITRUST report?

9 of 19 HITRUST domains are potentially inheritable by customers running on ClearDATA's platform. They are:

- Information Protection Program
- Configuration Management
- Vulnerability Management
- Network Protection
- Transmission Protection
- Audit Logging
- Business Continuity & Disaster Recovery
- Physical & Environmental Security
- Data Protection & Privacy

NOTE: *ClearDATA will determine which controls can be inherited based upon each customer's unique situation.*

How does inheritance impact the audit process?

During the evidence gathering process, a ClearDATA customer would typically upload artifacts to the myCSF portal for each control, demonstrating their compliance with the control requirements. Inheritance allows the organization to instead select a partner with whom the organization had a previously established relationship (like ClearDATA) from which to inherit that control. Once an organization requests to inherit one or more of the ClearDATA controls, the request is reviewed by ClearDATA's Chief Privacy and Security Officer. If the request is applicable to the solution provided to their organization by ClearDATA, then approval is given.

1 https://hitrustalliance.net/
2 https://hitrustalliance.net/documents/mycsf/mycsf_information/CSFInheritanceDatasheet.pdf