HITRUST Shared Responsibility: The ISV’s Role vs. Ours

PROJECT HOSTS™
Security Compliant Clouds

www.projecthosts.com

info@projecthosts.com

Introduction

The healthcare industry is in a tight spot when it comes to information security and compliance. Because of the sensitive nature of medical care, healthcare organizations are held to incredibly strict data protection standards and regulations, not to mention the rising expectations of the patients whose privacy they're sworn to protect.

At the same time, providers are eager to improve medical care and streamline operations through the use of cloud computing. Given that cloud service offerings (CSO) have the potential to generate hundreds of billions of dollars in revenue for healthcare companies, it's no wonder that the sector is leaping headfirst into the cloud.[1]

But before organizations can reap the rewards of their cloud investments, they must vet the security of the independent software vendors (ISVs) whose products they choose to deploy. Simultaneously, they need to maintain a robust cybersecurity program of their own.

So, what are the ISV's responsibilities? Which are those of the healthcare provider? In this white paper, we'll address these questions and demystify the complexities of healthcare compliance and shared responsibility.

[1] https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/clouds-trillion-dollar-prize-is-up-for-grabs

Understanding HITRUST compliance

Few organizations handle as much sensitive information on a daily basis as those within the healthcare industry. In this sector — where personal health information (PHI) and personally identifiable information (PII) are abundant — data security and patient privacy are mission critical.

For this reason, malicious actors and cybercriminals often target healthcare organizations. In fact, healthcare breaches affected 45 million people in 2021 — an all-time high.[2] That's more than triple the amount of people whose records leaked just three years prior.

In fact, healthcare breaches affected 45 million people in 2021 — an all-time high.[2] That's more than triple the amount of people whose records leaked just three years prior.

Whereas some hackers are motivated by financial gain, others merely aim to disrupt one of the nation's most critical infrastructures. No matter the driving force, data breaches and leaks are a violation of the Health Insurance Portability and Accountability Act (HIPAA) — the primary U.S. legislation created to protect PHI.

Although HIPAA includes many cybersecurity requirements and best practices, its specifications are highly nuanced. Organizations who lack a certain degree of size and skill may be ill-equipped to implement these security measures, leaving major gaps in their cybersecurity posture.

[2] https://www.criticalinsight.com/resources/news/article/critical-insight-finds-35-percent-increase-in-attacks-on-health-plans-in-2021-end-of-year-healthcare-data-breach-report

The HITRUST Common Security Framework

Recognizing the need for an integrated approach to cybersecurity, the Health Information Trust (HITRUST) Alliance was formed. As a nonprofit, its mission is to help organizations better manage data, information risk and compliance.[3] In a sense, HITRUST is designed to fill the void that HIPAA regulations don't address.

HIPAA-covered entities consist of all organizations that process PHI, including ISVs who sell cloud service offerings to the healthcare sector. HITRUST aims to simplify compliance and unite covered entities under a single cybersecurity standard known as the HITRUST CSF (Common Security Framework). The CSF acts as a roadmap to cloud security and HIPAA compliance, and is a certifiable standard that's modeled off of several globally recognized frameworks.

HITRUST CSF holds healthcare providers and their ISVs to a more rigorous standard than HIPAA. Because it's a certifiable program, HITRUST can provide assurance that cloud products have been tested against the most stringent cybersecurity controls in the industry and assessed by an objective third party.

However, several challenges complicate certification:

- It takes years to implement, assess and certify HITRUST's incredibly strict framework. At the same time, it costs hundreds of thousands of dollars to work through the assessment, which needs to be repeated every two years.
- HITRUST CSF includes hundreds of security controls that need to be regularly managed to maintain compliance.
- When organizations deploy an ISV's managed solution, they're often confused about which party is responsible for certain controls. Many healthcare providers don't realize that cloud security isn't fully managed by the vendor. And if controls are left unmanaged, both parties are exposed to risk.

> *Because it's a certifiable program, HITRUST can provide assurance that cloud products have been tested against the most stringent cybersecurity controls in the industry and assessed by an objective third party.*

[3] https://hitrustalliance.net/

A closer look at shared responsibility

Most cloud services are delivered using a shared responsibility model. When healthcare organizations move applications, data and workloads into the cloud, they normally agree to this arrangement.

Under a shared responsibility model, the end user's company (i.e. the healthcare provider) maintains accountability for certain aspects of cybersecurity, while the ISV takes care of the rest. For this model to work, both parties must clearly define their roles and responsibilities. If there's confusion as to who is meant to manage certain security functions, vulnerabilities may arise and leave critical gaps uncovered.

To mitigate this challenge and clarify expectations, HITRUST created its Shared Responsibility and Inheritance Program.[4] The initiative introduces two solutions that ISVs and healthcare companies can use to better define their responsibilities while also saving time and money performing HITRUST assessments.

HITRUST Control Inheritance

HITRUST Control Inheritance allows you to use prior HITRUST Validated or Certified assessment scores. In other words, an organization can leverage a partner's previous results when conducting its own CSF assessment, thereby inheriting its controls. This solution simplifies the assurance process while also saving time, money and other valuable resources.

By automatically inheriting controls from a previously certified provider, the program reduces the need to perform duplicative and redundant testing. Better yet, it makes it easier for organizations to effectively manage ongoing assurances and prove they're proactively protecting sensitive health information. With Control Inheritance, companies gain the transparency they need to effectively understand, inherit and maintain their security responsibilities.

[4] https://hitrustalliance.net/content/uploads/HITRUST-Shared-Responsibility-and-Inheritance-Program.pdf

The HITRUST Shared Responsibility Matrix

The second of HITRUST's two solutions is a no-cost, out-of-the-box template called the Shared Responsibility Matrix (SRM). The purpose of this template is to help cloud vendors communicate their security and privacy assurances so that customers can better understand their own responsibilities. By taking ownership of cloud security functions and clearly defining roles, organizations and ISVs can streamline the assurance process when inheriting controls from their providers.

The SRM is designed in collaboration with leading cloud service providers, including Amazon Web Services, Google Cloud and Microsoft Azure. The matrix includes over 2,000 controls that range from access and privilege management to segregation networks. Each control is assigned one of three designations: full responsibility, partial responsibility or no responsibility.

Benefits of Shared Responsibility

HITRUST's Shared Responsibility and Control Inheritance program takes the guesswork out of interpreting the complex ecosystem of healthcare cloud security and compliance. **At the same time, the initiative also:**

- Stimulates effective communication between healthcare organizations and cloud vendors that enables both parties to stay on the same page and manage cybersecurity more effectively.
- Reduces time and effort spent pursuing risk management and compliance objectives thanks to HITRUST's "assess once, inherit many" capabilities.
- Clarifies shared responsibilities through a standardized structure that reinforces control ownership in a complex cloud environment.
- Saves valuable resources that would otherwise be used to verify assurances, implement controls and maintain compliance.

> *The SRM is designed in collaboration with leading cloud service providers, including Amazon Web Services, Google Cloud and Microsoft Azure.*

Project Hosts for HITRUST compliance: Your role and ours

When it comes to deploying cloud solutions, healthcare organizations can lean on the assurances provided by HITRUST-certified products. But if you're an ISV hoping to enter the healthcare sector, acquiring HITRUST certification is easier said than done.

That's where Project Hosts can help. As a HITRUST CSF-certified cloud service provider, Project Hosts makes it easy to inherit compliance and reap the benefits of the Shared Responsibility program using our pre-audited platform: the General Support System (GSS).

When ISVs partner with Project Hosts and connect their applications to the GSS, they instantly offload up to 95% of their requisite security controls to us. With thousands of controls that need to be implemented and maintained, that's a massive weight off their shoulders.

Below is a non-exhaustive list of the security functions that Project Hosts manages on your behalf:

- Access control and authentication.
- Implementing and monitoring firewalls.
- Auditing/reviewing logs and alerts.
- Monitoring systems for availability and performance.
- Monthly vulnerability scanning.
- Configuration and monitoring.
- Patch and vulnerability management.
- Malware and intrusion prevention.
- Dedicated incident response and analysis.
- Contingency and disaster recovery.

Project Hosts takes ownership of everything outside of the software level. The remaining 5% of controls are the responsibility of the ISV partner. These include basic controls such as identifying and authorizing users, enforcing rules of behavior, remediating vulnerabilities and training on security awareness. By outsourcing all infrastructure components, ISVs can focus on developing their applications, meeting customer expectations and scaling operations.

Compliance-as-a-service

Inheriting compliance from Project Hosts is a great way to accelerate the HITRUST certification process. By offloading the majority of controls, assessors only need to examine the few that the ISV still manages. The result? HITRUST certification in as little as two or three months.

Project Hosts also offers two compliance by certification services:

Do it yourself:
If ISVs choose to initiate the HITRUST certification process on their own, Project Hosts can ease their burden by sharing our policies and procedures in addition to collecting evidence of control implementation.

We do it for you:
We engage with an assessor on the ISV's behalf and prepare the organization for the HITRUST audit.

Best of all, any ISV whose application runs on our platform gains the benefit of our security teams, who continuously monitor performance, prevent intrusion and patch the cloud environment. With the support of our team, ISVs can maintain ongoing compliance and focus on driving value across their organization.

Kick-start compliance with Project Hosts

When it comes to HITRUST compliance and cloud security, you don't need a service provider — you need a partner. That's why our expert engineers work alongside your team to take the pain out of HITRUST assessment, certification and maintenance.

With Project Hosts, you can concentrate your energy on the continued success of your business while we take care of compliance. Together, we not only kick-start your HITRUST journey, but help you make it across the finish line.

For more information, reach out to our team today.

Sources

1. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/clouds-trillion-dollar-prize-is-up-for-grabs
2. https://www.criticalinsight.com/resources/news/article/critical-insight-finds-35-percent-increase-in-attacks-on-health-plans-in-2021-end-of-year-healthcare-data-breach-report
3. https://hitrustalliance.net/
4. https://hitrustalliance.net/content/uploads/HITRUST-Shared-Responsibility-and-Inheritance-Program.pdf