Protecting Patient Information with HIPAA- and HITRUST-Compliant Cloud Services

Introduction

In the last few decades, technology has changed the face of every single industry, but few have been impacted like healthcare.

The biggest impact came when advanced technology—specifically, off-premise databases and hosted applications–created greater access to sensitive patient information for doctors, hospitals, and other healthcare staff. Along with this increased access came the need for heightened security standards that would ensure that everyone involved with this data was properly protecting patient details.

Enter the Health Insurance Portability and Accountability Act (HIPAA) in 1996 and the Health Information Technology for Economic and Clinical Health (HITECH) in 2009. These regulations placed new requirements on the healthcare industry, and also changed the way healthcare institutions interacted with and utilized the services of their IT solutions providers.

Who is Impacted by HIPAA and HITECH?

Prior to these standards, healthcare providers were responsible for the security of electronic protected health information (ePHI), and in many cases, doctors' offices, hospital, and other organization used on-premise servers to store, access, and maintain this information. With the emergence of the cloud and other hosted environments, however, security standards were needed to ensure the protection of ePHI both inside and outside of healthcare providers' network infrastructures.

While investigating these security standards, governing bodies discovered that threats to ePHI existed not only with healthcare providers themselves, but with the third-party service providers actually hosting the data. This is what prompted officials in the U.S. Department of Health and Human Services and the Office of Civil Rights to create HIPAA and HITECH. This expanded the responsibility for protection beyond the healthcare provider themselves and on to the solution providers supporting their hosted environments.

ANY ORGANIZATION inside or outside of the healthcare industry that in any way deals with ePHI is beholden to the security requirements of HIPAA and HITECH. This includes any service provider that accesses, stores, transmits or otherwise utilizes or facilitates the sensitive ePHI of patients.

What Does this Mean for Healthcare Providers' Relationships with Their Service Providers?

One of the largest changes to take place with HIPAA and HITECH was the requirement for a signed Business Associate Agreement (BAA) between the healthcare provider and their solution vendor. Within this document, the technology service provider, or business associate, enters into an agreement with the healthcare provider, or covered entity, noting that they will "appropriately safeguard protected health information," according to the Department of Health and Human Services.

What's more, if a service provider outsources any healthcare-related solutions, this third-party vendor must also sign a subcontractor BAA validating that they will comply with the regulations included in HIPAA and HITECH.

What Does a HIPAA-Compliant Service Provider Look Like?

In addition to the BAA and subcontractor agreements, there are several important safeguards, processes, and policies that a HIPAA- and HITECH-compliant managed service provider should have in place.

Documented Administrative Processes

Much of compliance within the technology industry deals with very specific policies and processes. It's critical that these items are well–documented by the service provider in a detailed manner. In particular, healthcare providers should ensure that the security breach notification process is documented. This will outline what happens if a breach takes place, including how quickly the covered entity is notified, how they are made aware of the instance, and how the breach is rectified.

Disaster Recovery and Business Continuity

In addition to breach notification, the service provider should also outline their processes for disaster recovery and business continuity. In the event of an outage, the healthcare provider must still be able to continue its critical operations. The hosted solution vendor should support this, while also ensuring that no sensitive data is lost.

Robust Data Encryption

HIPAA requires that ePHI is encrypted at all times, including when being stored or transmitted by the service provider. Solution vendors should have AES 256 encryption in place to prevent any unauthorized access and guarantee security for the sensitive healthcare data they are responsible for.

Physical and Technical Safeguards

HIPAA and HITECH require the presence of security at the administrative, physical and technical levels, helping to ensure end-to-end protection of ePHI. As noted, everyone involved with sensitive healthcare–related data has specific responsibilities under HIPAA and HITECH. Healthcare providers should also have compliant security processes in place on their side. An experienced service provider can explain how their policies and processes connect with those in place at the healthcare institution to support unified compliance.

A Step Further: Third-Party Attestation

While these industry standards don't require third-party auditing for service providers as part of compliance, many expert solution providers take this extra step to help guarantee their adherence with HIPAA and validate their processes. This attestation letter demonstrates that not only has the service provider self–assessed their policies and safeguards, but that those security measures and supporting activities have also been checked and validated by a HIPAA and HITRUST auditing expert. In this way, healthcare institutions can be sure that their sensitive patient information is in the best, most experienced, and most secure hands with its hosted solution partner.

What is HITRUST?

Founded in 2007, the Health Information Trust Alliance, or HITRUST, is a not-for-profit organization whose mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. Before the HITRUST certification was established, HIPAA laws were the go-to framework for properly handling electronic medical data; however, there has never been a governing body that polices compliance to proactively secure against breaches. Organizations can claim compliancy through self-assessment, but with the HITRUST certification, companies are verified as compliant by a neutral third party.

The HITRUST certification bolsters HIPAA regulations, but also brings additional clarity and guidance for the security controls an enterprise puts in place to ensure better protection of their data and systems. Since many healthcare organizations utilize a number of third-party vendors, it can sometimes be hard to control and consolidate these security compliance efforts.

The HITRUST certification bolsters HIPAA regulations, but also brings additional clarity and guidance for the security controls an enterprise puts in place to ensure better protection of their data and systems. Since many healthcare organizations utilize a number of third-party vendors, it can sometimes be hard to control and consolidate these security compliance efforts.

What Does a HITRUST-Compliant Service Provider Look Like?

Healthcare organizations that work with HITRUST-certified vendors can expect an increased value in the relationship–there is less risk of a breach; therefore, there is less risk of incurring the costs associated with a breach.

To determine whether or not organizations can become HITRUST certified, 19 categories are evaluated, each with 131-500+ different control requirements that are dependent on size, complexity, and regulatory factors. Furthermore, there are five levels of maturity upon which each control requirement is assessed:

- Policy
- Process
- Implemented
- Measured
- Managed

To earn this certification, an organization must meet all of the minimum requirements and achieve a passing score for each of the control domains.

Healthcare organizations aren't the only company types that should pay attention to the HITRUST certification. Due to the rigorous auditing process vendors must go through to attain this designation, the HITRUST certification means better protection and processes across the board–something all businesses can benefit from.

HIPAA/HITECH

HITRUST CSF Certified

▶ **Does your infrastructure hold up to compliancy best practices?**
Request a free risk assessment by calling 1-866-680-7556.

About Hostway|HOSTING
Hostway|HOSTING is leading the industry in secure, digital transformation solutions, featuring full-stack services across the entire lifecycle to help IT leaders harness data. As the world's most trusted managed cloud services provider, Hostway|HOSTING delivers experienced and secure migration services, complex managed cloud infrastructure, and application solutions for mission-critical software. Our team of engineers in North America, Europe, and Asia deliver reliable and scalable managed cloud and hybrid cloud solutions to thousands of customers across fourteen geographically diverse data centers around the world—all while ensuring strict compliance to PCI, HITRUST, HIPAA, FERPA, and GDPR guidelines. The Hostway|HOSTING mission is simple—to provide the best customer experience from the industry's best team. Visit www.hostway.com or www.HOSTING.com for more information.

HOSTWAY | HOSTING