HOSTWAY®

PROTECTING PATIENT INFORMATION WITH HIPAA–COMPLIANT HOSTING

Peter Marsh
Director of IT Security

INTRODUCTION

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

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 health care 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 health care industry, and also changed the way health care institutions interacted with and utilized the services of their IT solutions providers.

WHO IS IMPACTED BY HIPAA AND HITECH?

Prior to these standards, health care providers were responsible for the security of electronic protected health information (ePHI), and in many cases, doctors' offices, hospitals and other organizations 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 health care providers' network infrastructures.

ANY ORGANIZATION INSIDE OR OUTSIDE OF THE HEALTH CARE INDUSTRY THAT IN ANY WAY DEALS WITH EPHI IS BEHOLDEN TO THE SECURITY REQUIREMENTS OF HIPAA AND HITECH.

While investigating these security standards, governing bodies discovered that threats to ePHI existed not only with health care 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 health care provider themselves and on to the solution providers supporting their hosted environments.

Any organization inside or outside of the health care 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 HEALTH CARE 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 health care provider and their solution vendor. Within this document, the technology service provider, or business associate, enters into an agreement with the health care 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 health care–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?

There are several important safeguards, processes and policies that a HIPAA– and HITECH–compliant hosted service provider should have in place in addition to the BAA and subcontractor agreements. Health care providers should make sure that their hosted solution vendor has the following in place to ensure their compliance:

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, health care 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 health care 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 health care 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 health care–related data has specific responsibilities under HIPAA and HITECH. So health care 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 health care 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 auditing expert. In this way, health care institutions can be sure that their sensitive patient information is in the best, most experienced and most secure hands with its hosted solution partner.

COMPLIANT SOLUTIONS FROM HOSTWAY

Hostway, an industry–leading provider of hosted and cloud solutions, is proactive about its HIPAA compliance, providing secure hosting options specifically designed to support the needs of health care providers. Hostway leverages Microsoft Azure to support its dedicated compliant solutions, including dedicated servers, dedicated firewalls, dedicated Hyper V virtualized environments and Office 365 email solutions.

To find out more about how Hostway can provide solutions for your HIPAA and HITECH compliance needs contact now.


HOSTWAY