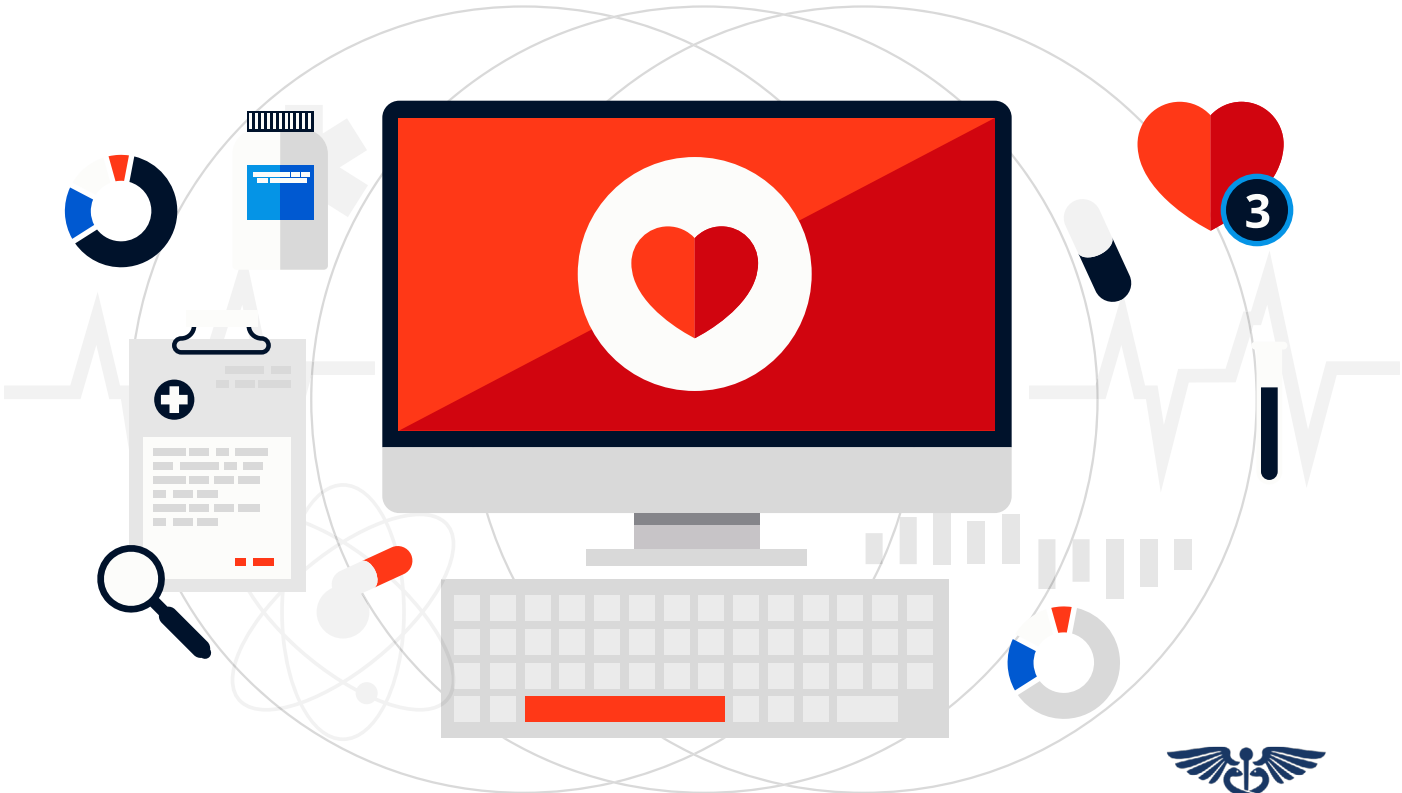
HOSTWAY®
THE TRUSTED CLOUD

The simplified guide to HIPAA compliance



HIPAA COMPLIANCE

Introduction

HIPAA, the Health Insurance Portability and Accountability Act, sets the legal requirements for protecting sensitive patient data. It's also an act with teeth.

In the last few years HIPAA data breach settlements have ranged from $1 million to $4.8 million with a significant number also falling within these two figures.

Any company that deals with protected health information (usually shortened to PHI) must ensure it has the appropriate security measures in place to ensure HIPAA compliance.

Compliance doesn't just apply to healthcare organizations. It also extends to service providers and sub-contractors that have access to health information.

If your data is hosted by a service provider the company must be HIPAA-compliant.

For hosting providers, HIPAA specifies a detailed series of administrative, physical and technical requirements to meet the requisite security criteria.

This guide provides you with a high level overview of the HIPAA compliance issues you need to consider and what to look for in a cloud hosting provider as part of your overall HIPAA compliance strategy.

Core considerations

The essence of HIPAA for any company working with electronic medical records is privacy and security.

The HIPAA Privacy Rule and Security Rule require organizations to provide safeguards to protect ePHI. This applies to hosting companies too.

Specifically, the requirements are:

- Ensure the confidentiality, integrity and availability of all relevant data that is created, received, maintained or transmitted
- Identify and protect against threats to the security or integrity of the information
- Protect against impermissible use or disclosure of data
- Ensure compliance by an organization's workforce

This can be boiled down to ensuring data confidentiality, safeguarding data so it is not altered or destroyed, data risk management and making sure employees are security aware.

However, HIPAA doesn't advocate a 'one size fits all' approach rather it recognizes that not all organizations are equal and each will implement solutions appropriate to their business, size and resources.

As such, measures aren't dictated. But that said each organization must:

- Evaluate the likelihood and impact of potential risks
- Implement appropriate security measures
- Document the chosen security measures
- Maintain continuous, reasonable and appropriate security protections

Value of a HIPAA-compliant hosting company

By using a HIPAA-compliant hosting company you can largely address privacy and security requirements by leveraging the following benefits:

Private hosted Environment

Your data is not stored in a shared environment with other's systems or apps, especially those that aren't subject to HIPAA requirements. Further, each technology stack within the cloud provider's environment will be HIPAA-compliant.

Increased security

A dedicated hosting platform keeps your data separate and more secure than a shared or public hosting environment. Deploying and managing data on dedicated hardware helps you avoid the risk of security breaches from a shared environment.

Location

You know where your servers are located and the dedicated hosting environment keeps your data together to ensure security and privacy.

HIPAA specialists

A HIPAA-compliant hosting provider must meet or exceed the same requirements that healthcare organizations do. As such you have a team of HIPAA certified security compliance experts who can help make sure you achieve and maintain compliance.

Requirements for HIPAA-compliant hosting providers

HIPAA stipulates that hosting providers must meet administrative, physical and technical requirements. As such a dedicated HIPAA hosting provider must address a number of points in their data centers to ensure compliance. When choosing a hosting company you need to be assured that they address each of the following points.

Physical safeguards

This requires that authorized access safeguards are put in place so only those who need to access data can do so. It requires a well thought out policy about use and access, for instance, restricting who can use workstations that hold data and usage of removable electronic media such as USB sticks. Policy should also cover how data is transferred, removed, stored and disposed of.

Technical safeguards

In essence this is the use of tools that govern access to data and is widely known as access control. It includes using unique user IDs, an emergency access procedure, automatic log off, the use of virtual private networks and data encryption and decryption.

Audit reports

Audit reports provide detailed insight into who has accessed data, when and where it was accessed and what specific data was accessed. In short, audit reports provide a record and route of all activity across different types of hardware and software. It's especially important in helping identify the source of a security violation.

Technical policies

This covers measures put in place to confirm that data hasn't been altered or destroyed. Importantly it covers disaster recovery and offsite data backups. In the event of some form of emergency or mishap such as a power outage, storage systems crash, fire or flood it's essential that all data can be recovered quickly, accurately and intact.

Network transmissions

Data will travel between your organization and the hosting company. This data must be protected whether it's transmitted via email, over a private network or the internet. Typically this means high levels of data encryption to protect against unauthorized access to data.

Questions to ask a hosting provider

A dedicated HIPAA-compliant hosting provider will be able to answer the following questions with ease. If not you should reconsider your choices.

Have you been independently audited?

A hosting provider needs to be fully compliant with the latest OCR HIPAA Audit Protocol across all of its technology stacks.

What IT services do you use to meet required security standards?

You should receive an answer that provides detailed insight into the tools that are used. These will include things like a private firewall, VPN for remote access, SSL certificates for data encryption, two-factor authentication, offsite backups and a private hosted environment.

What are your documented policies and procedures?

A hosting provider should have policies that lay down required responses in the event of a data breach, for instance, notifying you within a stipulated time period.

Do you have a business associate agreement?

If you use a hosting company you must have a business associate agreement (BAA) signed with that organization. This delineates the role the hosting company and its responsibilities. A HIPAA BAA is a legal contract and a compliance requirement.

Are your employees trained?

HIPAA requires all employees to be trained in good security practices. This includes policies, physical security, auditing, the use of secure passwords, data protection and more. This requirement also applies to BAA partners such as hosting companies.