The Simplified Guide to HIPAA Compliance

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 electronic protected health information (ePHI) 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 managed cloud service 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 managed cloud services 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 managed cloud service providers, too.

Specifically, the requirements are to:

- 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. Instead, it recognizes that not all organizations are equal and that 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 Cloud Services Company

You can largely address privacy and security requirements by using a HIPAA-compliant cloud services company and leveraging the following benefits:
PRIVATE ENVIRONMENT
Your data is not stored in a shared environment with others’ 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 platform keeps your data separate and more secure than a shared or public cloud 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 environment keeps your data together to ensure security and privacy.

HIPAA SPECIALISTS
A HIPAA-compliant provider must meet or exceed the same requirements that healthcare organizations do. Due to this requirement, the provider should provide you with a team of HIPAA-certified security compliance experts who can help make sure you achieve and maintain compliance.

Requirements for HIPAA-Compliant Providers
HIPAA stipulates that providers must meet administrative, physical, and technical requirements.

As such, a dedicated HIPAA cloud services provider must address a number of points in their datacenters to ensure compliance. When choosing a partner, 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. This 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 includes measures put in place to confirm that data hasn’t been altered or destroyed, plus 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 managed cloud services provider. 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 Provider

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

**Have you been independently audited?**
A 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, such as a private firewall, VPN for remote access, SSL certificates for data hosted environment.

**What are your documented policies and procedures?**
A provider should have policies that outline 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 (BAA)?**
If you use a managed cloud services company, you must have a signed BAA on file from that organization. This delineates the role of the company and makes its responsibilities clear. 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 managed cloud services companies.

---

**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](http://www.hostway.com) or [www.HOSTING.com](http://www.HOSTING.com) for more information.