HIPAA Guide for Small Business

Liquid Web™

HIPAA Challenges

If you're a small business in the healthcare market, or a company that serves small businesses in healthcare, chances are that you are struggling to understand how healthcare legislation like the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) impact your business. You are probably also struggling to learn what you need to do in order to ensure that you are compliant with the law. That's not an easy task, especially when more and more businesses like yours are relying on hosting companies to deliver the technology that their business needs to effectively operate and compete. And that's where we can help.

In order to make this process easier for you, we've put together this HIPAA guide for small businesses. In it you'll learn about the relevant laws that impact your healthcare-related business and common HIPAA terminology.

3 Healthcare Laws That Impact Your Business

If your company stores or processes electronic protected health information (ePHI), then your business is primarily impacted by three pieces of healthcare legislation: HIPAA, HITECH, and the HIPAA Omnibus Rule.

HIPAA

The Healthcare Insurance Portability and Accountability Act (HIPAA) is legislation that was signed into law by President Bill Clinton in 1996. It had four primary goals:

- To provide workers who change or quit jobs with continuous healthcare coverage.
- To reduce the administrative burdens and cost of healthcare by establishing standards for the electronic transmission of administrative and financial transactions.
- To combat abuse, fraud and waste in health insurance and healthcare delivery.
- And to improve access to long-term care services and health insurance.

HIPAA is comprised of five sections, which are typically referred to as *titles*. When people refer to *HIPAA compliance*, they mean adhering to Title II of HIPAA, which is often referred to as the *Administrative Simplification Provisions*.

When it comes to working with hosting companies or any other technology partner, the most important component of the Administrative Simplification Provisions is the *HIPAA Security Rule*. This establishes a national set of security standards for protecting important patient health information that is being housed or transferred in electronic form.

All healthcare related businesses (commonly referred to as *covered entities*) and their technology partners who process ePHI on their behalf (commonly referred to as *business associates*) must follow these rules in order to attain HIPAA compliance.

HITECH Act

The Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law in 2009 by President Obama. It added additional requirements to HIPAA by adding several provisions that strengthen the civil and criminal enforcement of the HIPAA rules. It establishes four categories of violations and corresponding tiers of penalty amounts, and caps the maximum penalty amount to $1.5M for all violations of an identical provision.

HIPAA Omnibus Rule

The HIPAA Omnibus Rule was published by the Department of Health and Human Services (HHS) in January 2013. These final regulations modifying HIPAA were designed in part to expand the requirements for HIPAA to business associates (i.e. contractors and subcontractors like hosting companies that process ePHI on behalf of covered entities).

The HIPAA Security Rule

The HIPAA Security Rule establishes national standards for the protection of electronic protected health information (ePHI). It's made up of three types of safeguards that every covered entity must implement in order to to ensure the confidentiality, integrity, and security of electronic protected health information.

Administrative Safeguards

Administrative Safeguards are policies and procedures that you define, document, and implement that describe how you will secure ePHI, who within your workforce has access to ePHI, and what employees are allowed to do with ePHI. It also requires your organization to periodically review your security measures and to have written business contracts with any third-parties (i.e. Business Associates) that have access to ePHI data that you manage.

What to Expect from Your Hosting Provider

Hosting providers are considered a special type of Business Associate called a Cloud Service Provider (CSP). As such, any hosting provider that you work with should be able to provide you with a Business Associate Agreement that describes their responsibilities when it comes to helping you secure ePHI. In addition, hosting providers can also help by:

- Ensuring only authorized employees have access to systems that you host with them.
- Keeping track of who accesses hosted systems and what they access.
- Providing and updating antivirus and malware software to protect your hosted systems.
- Helping you backup and recover ePHI in the case of a catastrophic event.
- Offering vulnerability scans of hosted systems to help you periodically review your security measures.

Physical Safeguards

Physical safeguards are physical measures, policies, and procedures that you implement to protect systems, buildings, and equipment from hazards and unauthorized intrusion. You need to consider all physical access to ePHI, from your office, to employee's homes, to even a separate physical storage center.

What to Expect from Your Hosting Providers

Hosting providers can't help you physically secure your office or your employee's homes, but they are responsible for making sure that their facilities have the necessary physical safeguards to help protect any ePHI that you store with them. These includes:

- Securing the data centers where your systems are hosted with physical safeguards like locks for all entry points, biometric scanners, and video surveillance.
- Securing the cabinets where the servers that run your systems are stored with locks.
- Documenting which of their employees have physical access to your systems and what they are authorized to do.
- Helping you backup and recover ePHI in the case of a catastrophic event.

The HIPAA Security Rule (continued)

Technical Safeguards

Technical Safeguards are technology, policies, and procedures that protect ePHI and control access to it. You are required to use any security measures that allow you to reasonably and appropriately protect ePHI. In addition, you must determine which security measures and specific technologies are reasonable and appropriate for your type of business.

What to Expect from Your Hosting Provider

This is one area where hosting providers excel at helping businesses like yours. The best providers offer a range of technology designed to secure ePHI that you store with them, including:

- Access control solutions that limit who has access to hosted systems and what they can do.
- Log management solutions that track who has accessed hosted systems and any actions that they took.
- File integrity solutions that track any changes to files running on hosted systems.
- Data encryption solutions that prevent unauthorized access to ePHI that is stored on hosted systems.
- Network encryption solutions that prevent unauthorized access to ePHI as it travels across networks.

> ***"No hosting provider can make you HIPAA compliant, but the very best hosting providers understand that HIPAA compliance requires deep partnership to ensure that each party is doing their part."***

Joe Oesterling, CTO, Liquid Web

HIPAA Glossary of Terms

Covered Entity. One of three different types of entities in the healthcare ecosystem:

- **A healthcare provider**, which includes doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies, but only if they transmit any information in electronic form in connection with a transaction for which HHS has adopted a standard.
- **A health plan**, which includes health insurance companies, HMOs, company health plans, and government programs that pay for health care like Medicare, Medicaid, and military and veteran health care programs.
- **A health care clearinghouse**, which includes entities that process nonstandard health information they receive from another entity into a standard electronic format.

Business Associate (BA). A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. This includes vendors or subcontractors like hosting companies, data processing firms, software companies, auditors, accountants, and medical transcription service providers.

Protected Health Information (PHI). Any information in a medical record that can be used to identify an individual, and that was created, used, or disclosed in the course of providing a healthcare service, such as a diagnosis or treatment.

In order for health data to be considered PHI and regulated by HIPAA it needs to be two things:

- Personally identifiable to the patient
- Used or disclosed to a covered entity during the course of care

Electronic Protected Health Information (ePHI). Any protected health information (PHI) that is covered under HIPAA security regulations and is produced, saved, transferred, or received in an electronic form.

Business Associate Agreement. A contract between a covered entity and a business associate (BA). The contract protects PHI in accordance with HIPAA guidelines by specifying each party's responsibility when it comes to PHI and the permitted and required PHI uses for the BA.

Cloud Service Provider (CSP). A type of business associate that offers online access to shared computing resources (e.g., networks, servers, storage, applications) with varying levels of functionality depending on the users' requirements. These range from mere data storage to complete software solutions (e.g., an electronic medical record system), platforms to simplify the ability of application developers to create new products, and entire computing infrastructure for software programmers to deploy and test programs.

Liquid Web HIPAA Compliant Hosting

Liquid Web delivers secure, robust, and high-performance infrastructure designed to power a full range of HIPAA workloads. It's also designed and fully managed for you by our team of infrastructure and security experts, so that you can acheive HIPAA compliance faster and more confidently than you ever imagined.

Physical Security

From biometric scanners to video surveillance to locked cabinets and more, our facilities are hardened to ensure that your ePHI is protected from physical threats.

Network Security

Firewalls, VPN with triple DES or AES encryption, Intrusion Detection, and round-the-clock network monitoring as just some of ways we protect your ePHI while in transit.

Backup Management

Our fully managed, robust backup solution captures your valuable ePHI on a continuous basis to ensure that's its always available, even in the face of a catastrophic event.

Security Services

Tap into advanced security capabilities like hardened servers, brute force detection and evasion, DOS prevention/protection and more for additional peace of mind.

HIPAA/HITECH COMPLIANT HOSTING

Contact us today at 800-580-4985 to learn how Liquid Web can help you deliver highly performant and secure hosting for your HIPAA projects.

About Liquid Web

Liquid Web powers content, commerce and potential for SMB entrepreneurs and the designers, developers and digital agencies who create for them. An industry leader in managed hosting and cloud services, Liquid Web is known for its high-performance services and exceptional customer support.

With over 30,000 customers spanning 150 countries, Liquid Web owns and manages its own core data centers and provides a wide portfolio of offerings spanning from bare metal servers and fully managing hosting to Managed WordPress and Managed WooCommerce Hosting. The Most Helpful Humans In Hosting™, Liquid Web earns the industry's highest customer loyalty* and has been recognized among INC Magazine's 5,000 Fastest Growing Companies for eleven years.

*2017 NPS score of 66%.

Liquid Web™

www.LiquidWeb.com
800.580.4985