calyptix® SECURITY

HIPAA for IT Providers

The most important rules to know

intro

The healthcare industry is a bonanza for IT service companies. Thousands of medical professionals struggle to manage and secure their networks. And the volume of medical technology keeps rising.

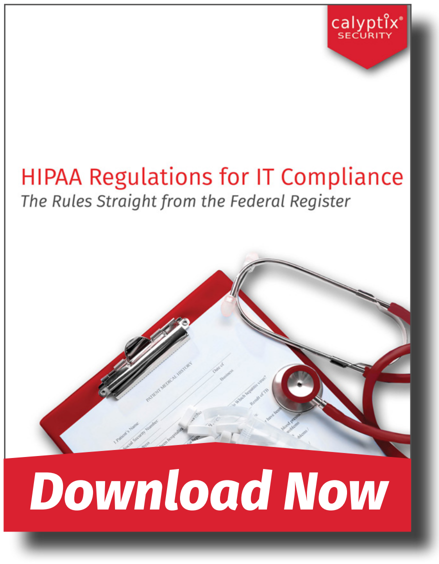
But one thing stands in the way of IT professionals who want to cash in on this bounty: HIPAA.

The Health Insurance Portability and Accountability Act is a sweeping set of regulations that affects all corners of the healthcare industry. From the way healthcare transactions are recorded, to protections for patient data, HIPAA has rules for it all.

This report provides the background information that IT professionals must know to grapple with HIPAA. You'll see who has to follow the rules, what the rules require, and the parts of HIPAA that matter most to IT.

This report does not include the exact text of the regulations. For that, download the companion report:

HIPAA Regulations for IT Compliance:
The Rules Straight from the Federal Register


HIPAA Regulations for IT Compliance

The Rules Straight from the Federal Register

Key Concepts

What does "HIPAA" mean?

The term "HIPAA" can refer to two things. The first is an act passed by the U.S. Congress in 1996 called the Health Insurance Portability and Accountability Act. The act had five major sections, one of which created a set of regulations to protect healthcare data.

The more common use of "HIPAA" is to refer to the regulations themselves. Although the rules have been updated by later laws, such as the HITECH Act of 2009, everyone still calls them "HIPAA."

The regulations are listed in the U.S. Code of Federal Regulations under the following sections:

Code of Federal Regulations - TITLE 45

- Part 160 – General Administrative Requirements
- Part 162 – Administrative Requirements
- Part 164 – Security and Privacy

What does HIPAA do?

HIPAA affects healthcare organizations in many ways. For example, some rules require the use of unique identifiers for health plans and employers. Others affect healthcare transactions. The most significant rules for IT professionals require the protection of electronic protected health data (ePHI).

What are PHI and ePHI?

"Protected health information" is defined in HIPAA as any type of personally identifiable health information. It is a major asset that all covered entities and business associates must protect under HIPAA. PHI is typically information about a patient, such as a person's blood type or their upcoming appointments. A medical bill, doctor's notes, and even a record that merely lists someone as a patient – it's all protected under HIPAA.

ePHI is the electronic form of PHI. It includes any personally identifiable health information that is transmitted or stored electronically. The HIPAA regulations for network security focus on the protection of ePHI, which makes them the most important rules for IT professionals.

Who must comply with HIPAA?

The groups that must comply with HIPAA are organized into three groups:

Covered Entity - A "covered entity" is a person or group that is required to follow HIPAA. Nearly every organization in the healthcare industry falls into this category. This is the group most affected by HIPAA. This includes health plans, healthcare clearing houses, and healthcare providers such as doctors, dentists, and hospitals.

Business Associate - A "business associate" is any person or group who handles health data on behalf of a covered entity. Anyone who creates, receives, maintains, or transmits ePHI for a doctor's office, medical billing office, or another covered entity is considered that entity's business associate.

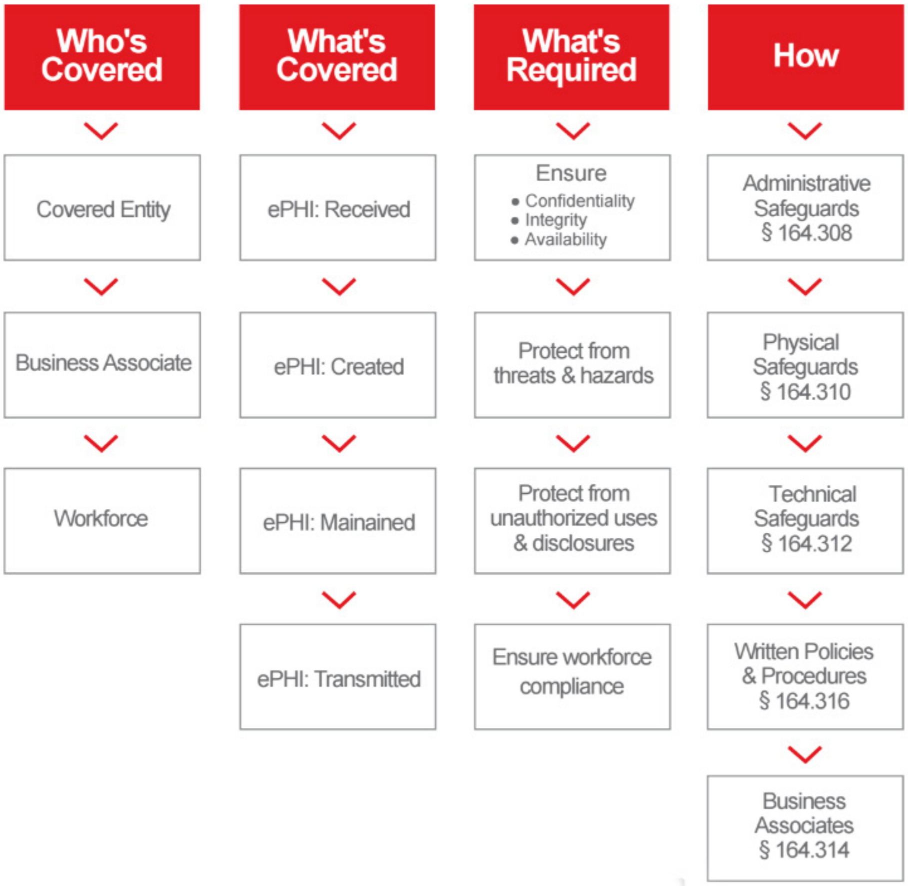
Business associates are required to enter agreements with the covered entities they serve. The agreements typically stipulate that the associate must follow HIPAA's guidelines to protect all ePHI they handle. IT service providers, including MSPs and VARs, who have clients in the healthcare market are almost always considered business associates. This requires them to follow HIPAA guidelines when working with healthcare clients.

Workforce - This final group includes employees, volunteers, trainees, and other people who work for a covered entity or business associate. Whether or not a person is paid, if their conduct is under direct control of a covered entity or business associate, then they fall into this group.

What parts of HIPAA affect IT professionals?

The portion of HIPAA most relevant to IT is known as the Security Rule. It outlines how electronic protected health information (ePHI) must be handled and protected. The following chapter of this report explains the Security Rule further.

Security Rule



Who's Covered	What's Covered	What's Required	How
Covered Entity	ePHI: Received	Ensure • Confidentiality • Integrity • Availability	Administrative Safeguards § 164.308
Business Associate	ePHI: Created	Protect from threats & hazards	Physical Safeguards § 164.310
Workforce	ePHI: Mainained	Protect from unauthorized uses & disclosures	Technical Safeguards § 164.312
	ePHI: Transmitted	Ensure workforce compliance	Written Policies & Procedures § 164.316
			Business Associates § 164.314

The HIPAA regulations contain more than 65,000 words. The phrase "Security Rule" is not among them. Nonetheless, the phrase refers to a subset of the regulations that set broad standards for the protection of ePHI (the sections are listed below).

IT professionals with clients in the healthcare industry must be intimately familiar with the regulations in the Security Rule to serve those clients effectively and stay within the bounds of compliance.

What does the Security Rule require?

All covered entities and business associates must do the following, as outline by the Security Rule in HIPAA:

- Ensure the confidentiality, integrity, and availability of ePHI
- Protect ePHI from hazards and threats
- Protect ePHI from unauthorized use and disclosure
- Ensure workforce compliance

For business associates, this of course applies only to the ePHI they handle. For example, if an IT business stores patient data on a remote server for a healthcare client, and that is the only service provided to that client, then the IT business is responsible to protect that data only. It is not responsible to protect all the client's ePHI.

Security Rule

How must ePHI be protected?

The Security Rule outlines how to meet the requirements to protect ePHI. This information is organized into six sections which are described below.

Each section is shown with its reference number for Title 45 of the Code of Federal Regulations.

Security standards: General rules – §164.306

This section sets broad standards to protect ePHI, such as one requirement to "protect ePHI from hazards and threats." All covered entities and business associates must meet the standards. How they do this is addressed in the following sections.

Administrative safeguards – §164.308

This section lists requirements for the planning and management of the privacy and security activities of a covered entity. For example, the entity must perform a risk assessment and enact policies and procedures for controlling access to ePHI.

Physical safeguards – §164.310

Physical access to machines that handle ePHI must also be controlled. For example, provisions in this section specify that a covered entity must maintain a record of the location of all hardware and electronic media and who is responsible for it.

Technical safeguards – §164.312

Requirements for the control and monitoring of access to ePHI are in this section. For example, providers must assign a unique identifier to each network user. Another requirement is that the system must automatically log-off users after a predetermined amount of idle time.

Business associate agreements – §164.314

The relationship between a covered entity and its business associates must follow certain guidelines. Specifically, covered entities must enter into a "business associate agreement" with each associate.

The required terms of these agreements are detailed in this section. For example, the associate must agree to be subject to the rules of the agreement and comply with its terms.

Additionally, the subcontractors of a business associate that handle ePHI are also subject to these rules. Subcontractors for MSPs and VARs might include backup recovery services, hosted email providers, and other similar services.

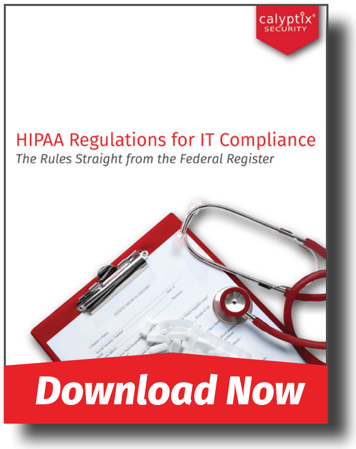
Written policies and procedures – §164.316

Rules in this section specify that covered entities must document the policies and procedures they will follow to maintain compliance and protect ePHI. They must also document how the organization will meet the requirements for the administrative, technical, and physical safeguards outlined in other sections.

The documents must be retained for at least six years. They must be made available to anyone required to follow their procedures, and they must be periodically reviewed and updated.

This report does not include the exact text of the regulations. For that, download the companion report:

HIPAA Regulations for IT Compliance:
The Rules Straight from the Federal Register


calyptix SECURITY
HIPAA Regulations for IT Compliance
The Rules Straight from the Federal Register
Download Now

Conclusion

HIPAA is a sales opportunity

IT service providers have responded to HIPAA in different ways. Some see it as a burden and a barrier to entering the large and growing healthcare market. Many others see it as an opportunity to find new business and increase sales to current clients.

Small firms need you

HIPAA affects organizations of all sizes. Smaller firms often struggle more than large firms to grapple with the rules. Much of this comes down to resources.

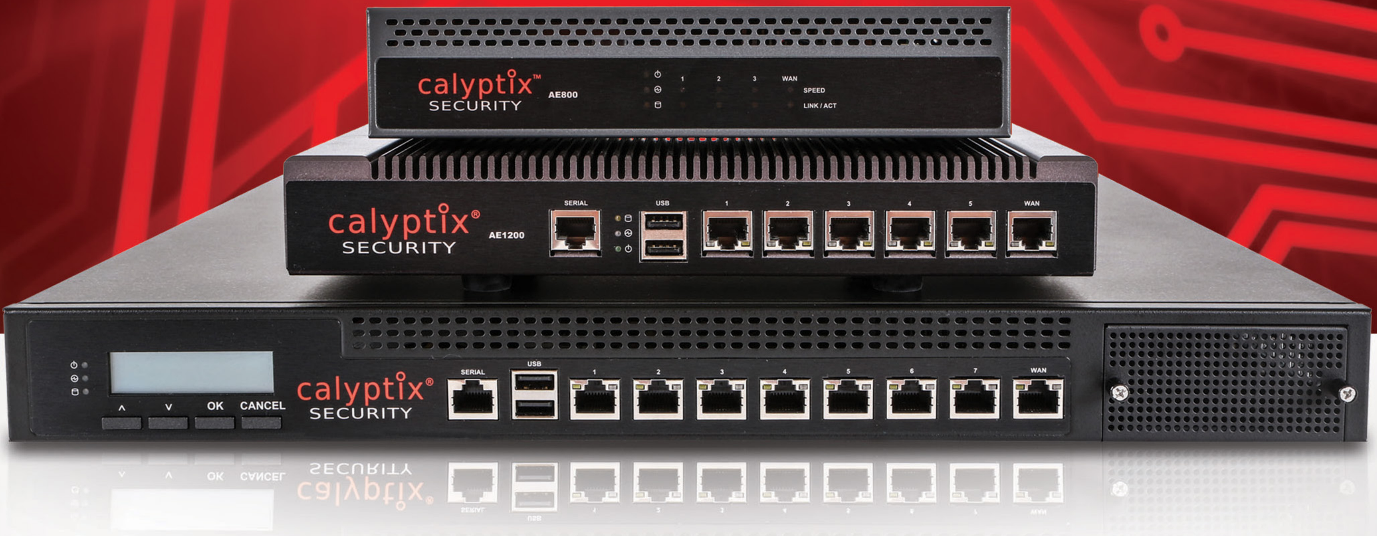
Smaller organizations need the expertise of IT service providers to keep their patients and businesses safe. They need new services and procedures to stay compliant. Many do not have the resources to do this themselves. This market has a massive need that only some IT service providers are working to fill.

Compliance is not security

Healthcare organizations often see compliance as the ultimate goal. In truth, it is only the beginning. Compliance keeps clients safe from regulators, but it is only a minimum. Much more is needed to protect them from hackers and malware.

Solid security is tailored to the organization. It's an on-going process, not an end goal. By helping organizations elevate their standards and maintain effective practices, you can deepen your relationships and extend your services beyond HIPAA.

Tough on hackers. Easy on your budget.



AccessEnforcer

Network security is easy with the AccessEnforcer UTM Firewall from Calyptix. First, you save time and protect clients with an easy-to-use firewall. Second, you solve problems faster with unbeatable tech support. Third, you increase profits with a reseller program that fits your business model.

Secure your network completely

FAST

Make security simple

Improve uptime & reliability

See what easy security looks like with Calyptix
www.calyptix.com/partners

calyptix®
SECURITY