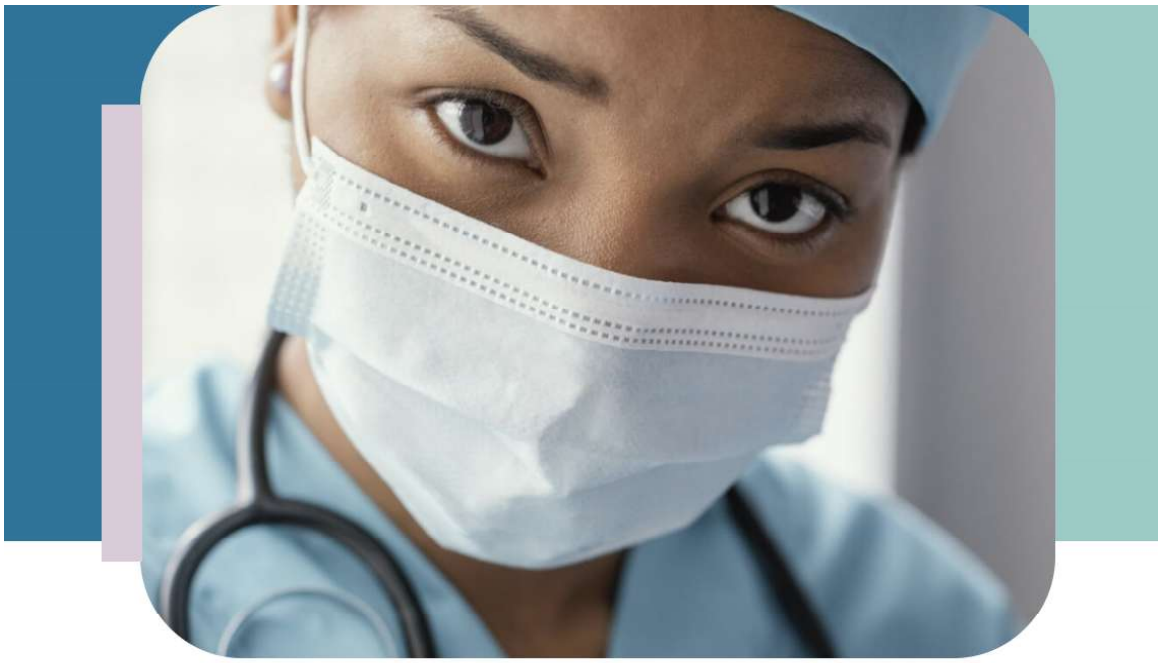
HIPAA Overview for End Users

PDF Terms of Use

This PDF version of this module is intended to be provided as an alternate format of transmission to licensed users of the KnowBe4 content only and may not be distributed beyond the licensed users, published anywhere that provides access beyond this group (including the Internet), or otherwise used outside of the terms of the subscription licensing agreement, including after the subscription ends. This PDF may also not be manipulated or modified. All images, text, and other assets are copyrighted by KnowBe4 and cannot be used in derivative works. Please refer to your master service agreement and/or subscription agreement for more information.

1.0 Welcome



HIPAA Overview for End Users

Your guide to securing protected health information

Duration: 15 minutes

2.0 Objectives

The Health Insurance Portability and Accountability Act, or HIPAA, is a compliance law regulating the healthcare industry. This training module was created to reinforce your knowledge of HIPAA by:

- Providing an overview of what HIPAA is and what it requires
- Examining the Privacy and Security Rules established by HIPAA
- Reviewing your role in protecting data and meeting compliance

Let's get started!

3.0 Introduction

[Narrator] When someone visits a doctor or seeks medical assistance of any kind, they enter into an agreement of trust with the healthcare provider. They expect that provider to not only administer proper treatment but also prioritize privacy and implement safeguards that ensure no unauthorized parties gain access to confidential information. It's those expectations and more that led to the creation of the Health Insurance Portability and Accountability Act, or HIPAA.

HIPAA's purpose is to balance a patient's right to privacy with the needs of healthcare providers who collect, store, and transfer data. It represents a cornerstone compliance law that regulates the flow of healthcare information and establishes federal standards for protecting that information.

What exactly does HIPAA require, and who does it apply to? What kind of information must remain private, and what steps must be taken to ensure security? Why does any of this matter to you? The goal of this training module is to answer these questions for you by providing an overview of HIPAA without getting into confusing legal language.

You are here because you're employed by an organization falling under HIPAA's umbrella of compliance requirements. Therefore, you play an important role in ensuring laws aren't broken, and, more importantly, that someone's private information never ends up in the wrong hands.

As you take this training, remember HIPAA compliance is more than a legal document mandated by the government. It's a law that impacts everyone in the country. We all need medical care, after all, and we all want our personal data to remain confidential and secure. Compliance laws exist to help organizations protect the information entrusted to them.

With that in mind, let's get started with a quick overview of the law. At the end of this module, your knowledge will be tested with a short quiz.

4.0 HIPAA Overview

HIPAA is a robust law with many different provisions, but it can be broken down into a few key concepts.

What is HIPAA?

Signed into law in 1996, HIPAA was initially created to protect workers' access to health insurance during job change or loss, and to help ensure more Americans would receive coverage in general. It has since evolved to include robust standards regarding the privacy and security of patient data while also providing initiatives to reduce healthcare fraud and abuse.

Who must comply with HIPAA?

The law applies to “covered entities” and “business associates”. Examples of covered entities include healthcare providers (like doctors and hospitals), healthcare plans, and clearinghouses that collect and process healthcare data.

Business associates are third-party organizations that have access to healthcare information while providing various services. IT specialists, accountants, lawyers, and billing companies are all examples of business associates.

What does HIPAA require of covered entities?

The law is quite detailed in what it requires, but it can be simplified to a fundamental concept: Maintain the privacy and security of protected health information (PHI). Covered entities can accomplish that by implementing technical and physical safeguards to prevent unauthorized access and developing policies to prevent accidental or intentional disclosure of PHI.

In summary, HIPAA requires that covered entities blend IT security solutions with employee security awareness.

What is protected health information?

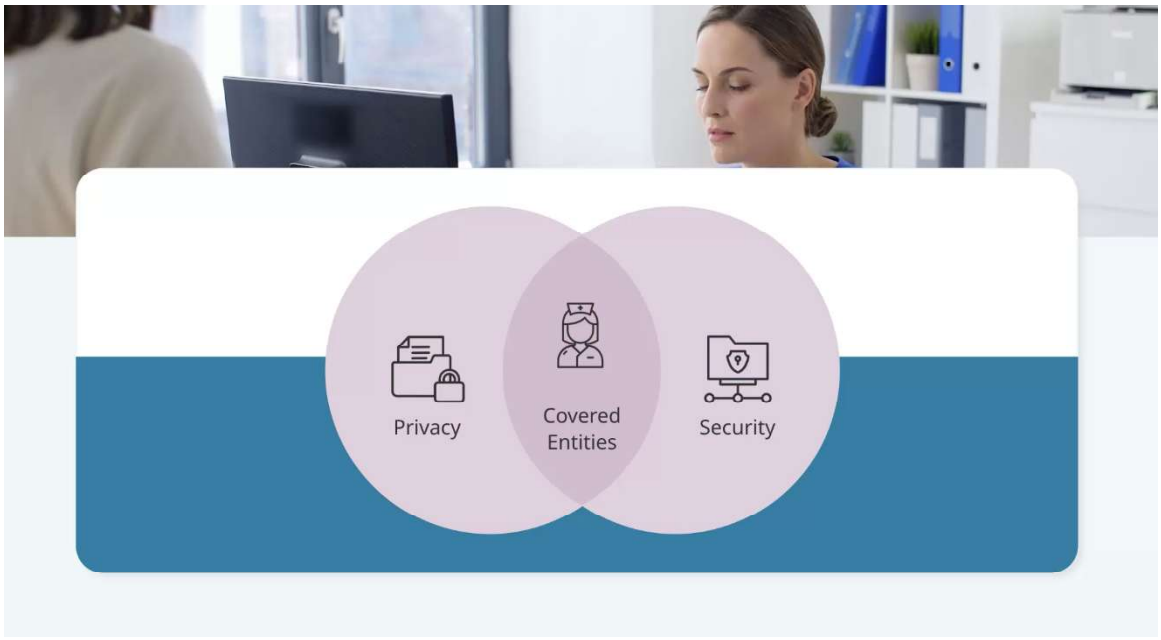
Protected health information (PHI, or e-PHI, when stored electronically) refers to data that can be used to identify specific individuals in conjunction with healthcare. Examples of PHI include full names, addresses, account numbers, billing information, social security numbers, and so on. PHI also includes information such as medical history, test results, insurance details, and anything else related to the health of an individual, regardless of timescale or context.

PHI must be protected no matter how or where it is collected or stored, whether on a computer, in an email, on a patient's chart, on a sticky note, or in a voicemail.

5.0 Privacy and Security

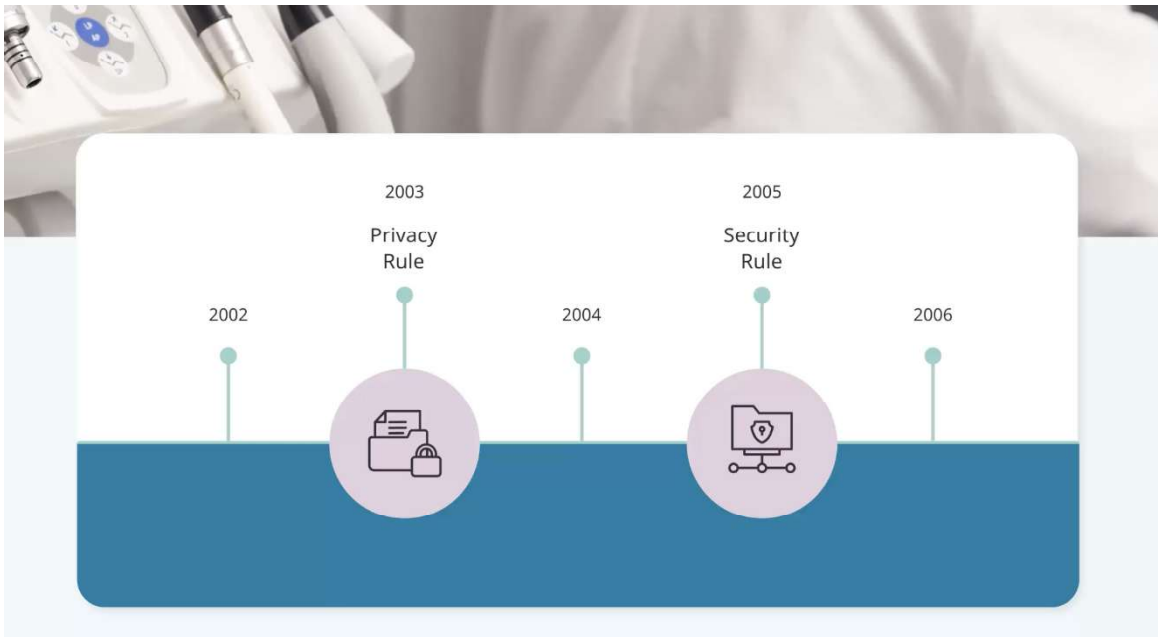
[Narrator] Privacy and security are closely correlated, but they're also two different concepts. In simple terms, privacy refers to the idea of keeping secrets a secret. For HIPAA compliance, that means ensuring that PHI is never disclosed to the wrong party accidentally or intentionally. Security has that same goal but accomplishes it through technical processes, like data encryption.

HIPAA features two important provisions to address both privacy and security that covered entities must adhere to: the Privacy Rule and the Security Rule.



The Privacy Rule implements national standards for proper use and disclosure of PHI, built on a single core principle: the minimum necessary. This means covered entities should collect, use, and disclose only the minimum amount of PHI necessary to render services and only use PHI for the intended purposes for which it was collected.

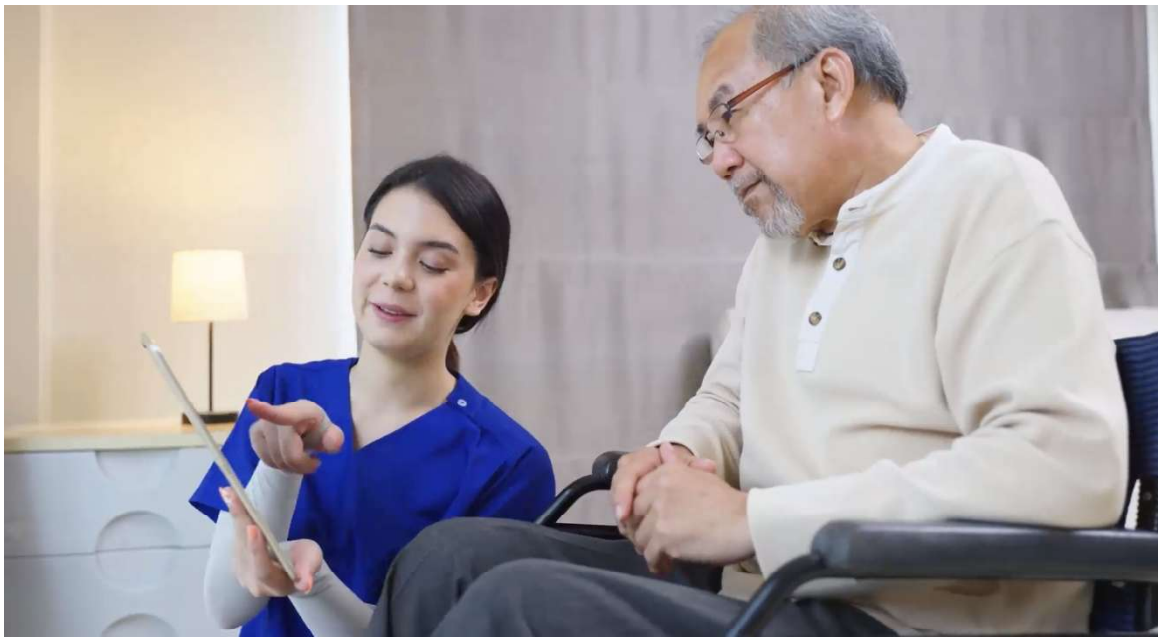
The Privacy Rule also defines what PHI is and grants a variety of rights to individuals that covered entities must uphold. For example, patients have the right to obtain copies of their medical records, to add and correct their information, to learn how their data is being used and shared, to restrict who gets access to PHI, and to file a complaint if they feel their rights have been violated.



The Privacy Rule went into effect in 2003 and was closely followed by the Security Rule, which specifically covers electronic protected health information or e-PHI. It requires covered entities to address and implement three security safeguards: administrative, physical, and technical.

Administrative safeguards focus on the policies and procedures necessary to demonstrate a clear commitment to protecting e-PHI. These safeguards include designating a security officer who develops policies, trains employees on those policies, and performs routine risk assessments to identify potential security vulnerabilities.

Physical safeguards refer to all security measures designed to control and protect physical access to data storage areas containing e-PHI, such as workstations.



Technical safeguards refer to the use of technology and policies to protect the digital storage and transmission of confidential information. For example, covered entities must utilize hardware and software to monitor networks and ensure e-PHI isn't improperly altered or destroyed.

The Privacy Rule and Security Rule both represent key frameworks that blend three vital parts of protecting information: people, processes, and technology. It was designed to be flexible and scalable without limitations on specific requirements, so each entity can implement the solutions that work best for their particular size and structure.

6.0 HIPAA and You

Meeting HIPAA compliance and securing PHI is the responsibility of all members of a covered entity.

Access Is Everything

One of the most important aspects of security is protecting the access you've been granted, both physical and digital. Never allow someone else to use your ID badge, lock workstations when not in use, and create strong, unique passwords for every account. Securely store and properly dispose of any documents that contain confidential information.

Malware Infections Can Steal Data

Malware (malicious software) is the umbrella term given to dangerous computer programs. Malware has many capabilities, including corrupting systems and stealing PHI. It is most often spread via malicious links or attachments, and USB flash drives that cybercriminals intentionally leave in public areas. Avoid malware by thinking before clicking, and never plug in USB devices you don't own.

Phishing Attacks Are a Major Threat

Phishing is a scam used by cybercriminals to lure someone into divulging information, downloading attachments, or clicking on a malicious link. You can identify phishing by staying alert for these common warning signs:

A sense of urgency; asking you to click on a link immediately

Threatening language; claiming an account has been suspended

Generic greetings; not addressing you by name

Poor grammar and misspelled words

Policies Exist to Protect People

While the goal of many compliance laws, including HIPAA, tends to focus on protecting data, it's really about protecting people. When someone's PHI gets stolen or leaked, they often become a victim of identity theft, which is a scam that allows criminals to pose as the victim and cause irreversible financial damage. Policies exist to help prevent such scams, and by always following policies, you help keep people safe.

Security Incidents Can Happen

In a perfect world, the combination of technologies and policies would eliminate all security incidents. Unfortunately, security incidents happen; it's how they're handled that makes the difference. If you see something, say something immediately! The longer an incident goes unreported, the more damage it could cause.

7.0 Wrap Up

HIPAA is a comprehensive compliance regulation that has in-depth provisions regulating the healthcare industry. The purpose of this training module is not to make anyone an expert on the law. Instead, the goal is to raise awareness about what the law is, why it exists, and how it impacts you, both professionally and personally.

Let’s wrap things up with a short quiz.