HIPAA: Basics Self-Paced

Section 1: Introduction

About This Course
Learning Objectives

Section 2: HIPAA Overview

What Is HIPAA?
HIPAA Requirements
Covered Entities
Business Associates
What Is Protected Health Information?
Review
Physical Access
De-Identification
Permitted Uses and Disclosures of PHI
Review
Rights Under HIPAA Privacy Regulations
Review
Breaches
Breach Notification Requirements
HIPAA Penalties
Steps to Avoid HIPAA Violations

Section 3: Conclusion

Course Summary
Course Contributor
Resources
References

Section 1: Introduction

About This Course

The Health Insurance Portability and Accountability Act, commonly called HIPAA, protects the confidentiality and security of healthcare information. HIPAA creates and protects individual privacy rights for protected health information and governs the use and disclosure of that information. In this course, you will learn about HIPAA, violations of HIPAA, and steps to take to prevent these violations.

The goal of this course is to provide all staff with an overview of the principles of HIPAA.

The content of this course is sourced from 45 CFR Parts 160,162, and 164 (2020) or HIPAA-related resources from the Health and Human Services (HHS) unless otherwise noted.

Learning Objectives

After taking this course, you should be able to:

- Define the purpose of HIPAA.
- Recognize when a HIPAA violation has occurred.
- Identify three steps you can take to avoid a HIPAA violation.

Section 2: HIPAA Overview

What Is HIPAA?

HIPAA is the Health Insurance Portability and Accountability Act. It is a federal law that gives individuals rights and protection over their personal healthcare information.

Allowing unauthorized individuals to see this personal information can have severe consequences, even if it happens by accident.

HIPAA Requirements

So, what is your organization required to do to comply with HIPAA? Organizations are required to:

- Develop HIPAA policies and procedures.
- Select a HIPAA privacy and security officer.
- Train its employees on HIPAA laws and ways to prevent violations.
- Discipline employees for violating HIPAA, up to and including termination.
- Reduce or undo any potential harm from a violation an employee may have caused.

You should request a copy of your organization's HIPAA policies and procedures, as well as any other policies related to privacy to review and follow.

Covered Entities

The HIPAA rules limit the ways a person's protected health information may be used or disclosed. Organizations that handle protected health information as part of their business are referred to as covered entities.

A covered entity, or CE, can include, but is not limited to:

- Doctors' and dentists' offices
- Hospitals
- Pharmacies
- Nursing facilities
- Assisted living facilities
- Home health agencies
- Health insurance companies
- Government programs that pay for healthcare
- Correctional facilities
- Child and family services agencies
- Intellectual and developmental disability services providers
- Behavioral health centers

If you are taking this training course, you likely work for a covered entity. This means that you must comply with HIPAA.

If you are unsure whether your employer is a covered entity, check with your supervisor. Some organizations may have stricter guidelines for privacy that they must follow. Your organization will provide additional training on these guidelines if applicable to your organization.

Business Associates

Your organization will often work with outside companies to provide a variety of services to assist with the operations of the organization. Under HIPAA, these outside companies may be considered business associates (BAs).

BAs are persons or entities who perform functions on behalf of, or provide certain services to, a covered entity that involve protected health information.

The following is a list of business associates that may work with your organization:

- An answering service
- A billing company
- Accountants and lawyers
- A shredding company
- A data warehouse
- A document storage vendor
- An electronic medical record, or EMR team member
- A case management software vendor

BAs are responsible for carrying out certain tasks and are directly liable for certain HIPAA violations. All BAs must enter into a contract with a CE to ensure that they understand the importance of safeguarding protected health information.

If you are a BA, make sure you request a copy of the company's HIPAA Policies and Procedures.

What Is Protected Health Information?

Depending on your role at your organization, you may have access to protected health information, or PHI. To comply with HIPAA, you need to understand what PHI is.

PHI is any health information, held or transmitted by a covered entity or business associate, that could be used to identify an individual. PHI can be transmitted verbally, in writing, or electronically. It includes:

- The individual's past, present, or future physical or mental health or conditions
- The health treatment services provided
- The payment information for the services provided

PHI also includes many common identifiers when they can be linked with any of that information.

Common PHI identifiers include:

- Name
- Geographic units smaller than a state (e.g., street address, city, county, zip code)

- All dates, except for the year, related to the person (including birth date, admission date, discharge date, date of death)
- Telephone number, fax number, and email address
- Social Security number
- Medical record number, account number, and health plan beneficiary number

More information that is considered PHI includes:

- Certificate or license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web universal resource locators (URLs) and Internet Protocol (IP) address numbers
- Biometric identifiers, such as a fingerprint or voiceprint
- Pictures of a person's face and comparable images
- Any other unique identifier or code

Review

Kevin is preparing an electronic file for storage at a data warehouse. That file contains last year's billing information for your organization. Is this considered PHI?

A. **Yes**
B. No

Feedback [This is PHI because it would include individuals' identifiable health information, including past physical and mental health conditions, the healthcare they received, and past payment information in electronic form.]

Physical Access

PHI should be kept in an area that can be locked or, at a minimum, an area where access can be restricted. **Do not access any PHI that you do not need to see to perform your job duties.**

If you are given keys, ID badges, or anything else that allows physical access, make sure you keep them secure. You must file a security report immediately if anything is lost or stolen.

De-Identification

You may be wondering if something is considered PHI right now, is it always PHI? Is there any way to work with information so it is no longer PHI and subject to HIPAA rules? What if the person's name is removed from the information?

It is not enough to remove an individual's name from PHI. HIPAA provides only two methods by which PHI can be de-identified:

- The **Safe Harbor** method requires that **18 types** of identifiers of the individual and their relatives, employers, or household members be removed.
- The **Expert Determination** method uses statistical or scientific principles to de-identify information and determine if the risk of using the information to identify an individual is very small.

Obviously, you should not do either of these things alone. In fact, no one should try these

methods on their own. The HIPAA Privacy Officer should be consulted for all de-identification assistance.

Permitted Uses and Disclosures of PHI

The HIPAA Privacy Rule has a lot of specific requirements that ultimately come down to one concept: Regulating the disclosure, or release, of an individual's PHI.

Under HIPAA, no authorization or consent is needed to use or share PHI for the purposes of treatment, payment, or healthcare operations, commonly referred to as **TPO**. However, the person's consent **is** required if the information will be used for certain purposes, such as marketing.

For disclosures of PHI, individuals must follow the **Minimum Necessary Rule**. That means when using, disclosing, or requesting protected health information, you should provide only the minimum information necessary to accomplish the intended purpose of the use.

Review

You are clocking in for work one morning in the break room and notice a note on the wall that reads: Susan should be given her Depakote® in the afternoon rather than the morning, effective June 26th.

Is this an acceptable disclosure of PHI?

A. Yes
B. **No**

Feedback [You, and others who can see this note, may not "need to know" this information. Whoever posted this note did not use any safeguards to prevent you, or anyone else who uses the break room, from seeing this information.

You are covering for Alyssa, the receptionist, while she is on break. The phone rings and you answer it. The person on the phone explains that she thinks her sister was just admitted to your facility and wants to know how she is doing after her stroke. How should you respond?

A. Tell the caller that her sister was admitted, but nothing else about the situation.
B. Tell the caller that her sister was admitted and provide basic information about her condition.
C. **Tell the caller that you are not allowed to provide information without authorization.**

Feedback [Although it may seem okay to answer a question for a family member, in doing so, you are providing PHI in a way that is not allowed.]

A man who received services at your organization a year ago calls to request a copy of his file. Is your organization allowed to send him a copy of it if it includes detailed observations and notes from his course of treatment?

A. **Yes**
B. No

Feedback [Individuals have the right to have access to their own PHI and must receive the requested records within the required response time in accordance with current regulations or organizational policy. However, the provider's office may charge a fee for the cost of copying and mailing.]

It is important to note that your organization has an obligation to take reasonable steps to verify the identity of any individual who requests access to their own PHI before providing access (Department of Health and Human Services, 2020).

Make sure you are familiar with your organization's policies and procedures. Some may require the individual to submit a request in writing, but this is NOT a requirement under HIPAA.

Rights Under HIPAA Privacy Regulations

Under HIPAA, an individual can ask that the provider communicate with them in an alternate way or at an alternate location (e.g., only send mail and phone calls to their office, not home). A provider must agree to reasonable requests.

The individual can ask that the provider restrict or limit use or disclosures of PHI when carrying out treatment, payment, or healthcare operations.

The regulations also state:

- The authorization form must be written in plain language.
- The individual must be given a copy of the signed authorization form.

Review

Ben, the administrator, asks Lindsey, the nurse, to review a referral that contains PHI to determine if the organization can provide the appropriate care. Is this allowed?

A. **Yes**
B. No

Feedback [This is an allowable disclosure of PHI because it is for the purpose of coordinating treatment and care. An organization cannot determine if they can provide care without knowing a person's medical condition. However, if the referral was discussed around others who do not "need to know" the information, then this would be a HIPAA violation.]

At lunch, Santiago overhears a conversation in the break room between staff about a particularly challenging person they provide services to. He overhears information about this person's health condition. Is this acceptable?

A. Yes
B. **No**

Feedback [This is not acceptable. Santiago did not "need to know" this information for any approved purposes. Additionally, the staff did not take appropriate precautions to protect the information.]

Breaches

A "breach" under HIPAA means that unsecured PHI has been acquired, accessed, used, or disclosed.

Rachel is working with PHI. She recognizes the name of the mother of a close friend. Rachel is surprised that her friend did not mention anything about his mother when she talked to him the other day.

She tells you that she is going to post on her friend's Facebook® page asking why he didn't tell

her his mom was receiving services from your organization. What should you tell her?

A. "Just don't be mean about it. Just make contact and offer some words of encouragement."
B. **"Don't do it. Contacting your friend would be considered a breach."**
C. "Call him instead of posting it on Facebook® to prevent a breach."
   Feedback [Communicating anything about it to the friend would be an unacceptable, impermissible disclosure of PHI regardless of the method of disclosure. Although her intentions were good, Rachel would have probably been in serious trouble personally **and** professionally.]

Breach Notification Requirements

Following a breach that meets the requirement of the Breach Notification Rule, covered entities must notify:

- Affected individuals.
- The Secretary of the Department of Health and Human Services.
- The media, in certain circumstances.

If you identify that a breach may have occurred, you should notify your supervisor, another member of management, or the Privacy Officer immediately. Although the rule describing a breach and its exceptions is complicated, it is easy to commit a breach.

Jingyu is working on a billing file when his stomach growls. Because he is working on a tight deadline, he takes his laptop to the break room so he can eat and work at the same time. You are already there having lunch so Jingyu joins you. Halfway through lunch, he wants a cup of coffee and asks you to watch his laptop. What should you do?

A. **Remind Jingyu to lock his laptop, so no sensitive information is available to anyone else.**
B. Tell Jingyu you will keep an eye on his laptop.
   Feedback [Anytime someone steps away from their computer they should take steps to ensure that PHI cannot be seen by other persons. Telling someone you'll keep an eye on their laptop does not protect the privacy of the PHI that may be on the laptop.]

HIPAA Penalties

Failing to comply with HIPAA can be expensive for your organization. There are four tiers of penalties for HIPAA violations varying in amount, based on:

- Whether you knew about the violation.
- If it was committed more than once.
- How quickly it was corrected.

Tier 1
$100 to $50,000 per violation up to a $1.5-million limit* for the same violation within the calendar year, where the violator ***did not know*** about the violation.

Tier 2
$1,000 to $50,000 per violation up to a $1.5-million limit* for the same violation within the calendar year, where the violation was ***due to reasonable cause***. Reasonable cause is an act in which a person knew, or should have known, that the act violated HIPAA.

Tier 3
$10,000 to $50,000 per violation up to a $1.5-million limit* for the same violation within the calendar year, where the violation was ***due to willful neglect*** and **was corrected within 30 days of discovery**. Willful neglect is an intentional failure to comply with HIPAA.

Tier 4
$50,000 per violation up to a $1.5-million limit* for the same violation within the calendar year, where the violation was **due to willful neglect** and **was not corrected within 30 days of discovery**.

*Fines are adjusted annually to account for inflation.

As you can see, the fines associated with HIPAA violations can be pretty large, even for mistakes! This shows to you how important it is to learn about HIPAA guidelines and follow them. You don't want to make a mistake that could cost thousands or even millions of dollars!

Steps to Avoid HIPAA Violations

Now that you understand how HIPAA violations occur and the importance of preventing a breach, let's look at ways you can prevent violations from occurring.

First and foremost, **know and follow your company's HIPAA policies and procedures as well as any additional privacy policies.** While this course provides general information and guidelines regarding HIPAA, your organization's policy will provide specific details on preventing HIPAA breaches.

Do not discuss anyone's PHI with fellow employees unless it is for the purposes of treatment, payment, or healthcare operations. If you do need to discuss PHI with someone who "needs to know," be sure to have these discussions in private areas where they cannot easily be overheard.

No matter how interesting it seems to you, **do not share anyone's PHI with friends or family.** This is an important and often overlooked HIPAA breach. Even if you don't mention the name of the person, it is possible that the information you provide will be sufficient for someone else to identify the person you are talking about. For example, someone might think, "Hey, my cousin had that problem and she was in that hospital!"

Do not leave PHI unattended or allow it to be visible to unauthorized persons. Turn computer screens away from the door, lock up files after you are done using them, and do not discard PHI in an open trashcan. When PHI is no longer needed, it must be properly shredded or made impossible to read or reconstruct. Follow your organization's policy regarding the destruction of PHI.

When sending PHI via fax or email, double check the email address or fax number before you send to ensure you are sending it to the proper person. Also, confirm that the method you are using to transmit PHI is approved by your organization. For example, some email communication is not considered secured and therefore cannot be used to transmit PHI.

Section 3: Conclusion

Course Summary

Now that you have finished viewing the course content, you should have learned the following:

- The purpose of HIPAA
- When a HIPAA violation has occurred
- Steps you can take to avoid a HIPAA violation

All employees are responsible for protecting the privacy and confidentiality of PHI. The HIPAA law identifies what information is deemed to be protected health information and provides limitations surrounding the appropriate use and disclosure of this information. You must ensure that you take the proper steps to prevent protected health information from being seen by or shared with those who do not have a “need to know.”

Course Contributor

This course was reviewed by Jennifer W. Burks, M.S.N., R.N.
Jennifer W. Burks is a Curriculum Designer in Post-Acute Care for Relias. She has over 25 years of clinical and teaching experience, and her areas of expertise are critical care and home health. She earned her Bachelor of Science in Nursing from The University of Virginia in 1993 and her Master of Science in Nursing from The University of North Carolina, Greensboro in 1996. Her professional practice in education is guided by a philosophy borrowed from Florence Nightingale's Notes on Nursing, "I do not pretend to teach her how, I ask her to teach herself, and for this purpose, I venture to give her some hints."

Acknowledgment: Linda Weaver was the previous author of this educational activity but did not participate in the revision of the current version of this course.

Resources

eCFR
https://gov.ecfr.io/cgi-bin/ECFR?page=browse

U.S. Department of Health and Human Services
www.hhs.gov

References

Department of Health and Human Services. (n.d.). Individuals’ right under HIPAA to access their health information. Retrieved January 13, 2022, from http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/

Troklus, D., & Vacca, S. (2016). *Compliance 101*, (4th Edition). Health Care Compliance Association.

Exam and BrainSparks

CE (Y)	BS (Y)	LO #	Q #	Question
	Y	1	1	All of the following are purposes of HIPAA EXCEPT?

			a	It gives individuals rights over their personal healthcare information (PHI).
			b	It provides individuals with protections for their protected health information (PHI), including controls over how the information is used and disclosed.
			c	It describes steps that must be taken to protect protected health information (PHI).
			d	It allows personal health information (PHI) to be unsecured at all times.
	Y	1	2	True or False: The primary purpose of HIPAA is to protect individuals from becoming victims of medical malpractice.
			a	True
			b	False
	Y	2	3	Which of the following scenarios is a clear violation of HIPAA?
			a	An individual asks if you would become their “friend” on social media and you decline.
			b	A private conversation about an individual occurs between a physician and a nurse.
			c	A coworker notifies her church that an individual, who is one of their parishioners, has fallen.
			d	You use the telephone to call a friend from work during your break.
	Y	2	4	Under which circumstance can you disclose PHI?
			a	If you know a person won’t mind
			b	If it is for the purpose of treatment
			c	If the person dies
			d	If you no longer work for the company
	Y	2	5	All of the following are PHI EXCEPT:
			a	The person’s address
			b	The person’s education level
			c	The person’s name

			d	The person's telephone number
	Y	3	6	All of the following steps can help to avoid a HIPAA violation EXCEPT:
			a	Learn your organization's HIPAA policies and procedures.
			b	Lock up all files containing protected health information prior to leaving your work area.
			c	Ask your friends to promise they won't repeat anything you tell them about work.
			d	Refuse to discuss the treatment of an individual recently admitted to your facility.
	Y	3	7	True or False: It is acceptable to access PHI that is unnecessary to perform your job duties.
			a	True
			b	False
		2	8	You can expect your organization to do all of the following EXCEPT:
			a	Develop HIPAA policies and procedures.
			b	Designate a HIPAA privacy and security officer.
			c	Train its employees on HIPAA laws and ways to prevent violations.
			d	Terminate anyone who talks about a person's care with other caregivers.
		1	9	Following a breach that meets the requirement of the Breach Notification Rule, covered entities must ALWAYS provide notification of the breach to:
			a	Non-affected individuals
			b	The Secretary of the Department of Health and Human Services
			c	Social media and local media
			d	All healthcare organizations within a 10-mile radius
		2	10	All of the following are acceptable, permissible disclosures of PHI without an authorization EXCEPT:

			a	For entertainment purposes
			b	For treatment purposes
			c	For payment purposes
			d	For healthcare operations