HIPAA: Basics

Section 1: HIPAA Basics

A Computer Technician Meets HIPAA

Kevin, your brother-in-law, has just started working at your company. His job is to train new staff to use company software and to resolve computer problems when they arise.

When Kevin assists employees with their computers, he sometimes sees files that include the names, diagnoses, and treatments of persons served by the organization. He also prepares electronic files containing healthcare information for transmission to a data warehouse for storage.

You know that HIPAA is new to him and can be tricky to navigate. He really needs this job, so you take it upon yourself to help him apply what he learned about HIPAA during orientation and make sure he avoids any violations.

He should really be able to define the purpose of HIPAA, recognize when a HIPAA violation has occurred, and identify ways to avoid making a HIPAA violation.

What Is HIPAA?

On his first day after onboarding, Kevin asks you to confirm his understanding of HIPAA.

You remind him that 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.

Kevin wonders how much this information will affect him, since he works mainly with computers. As he goes through his first week, he learns a lot about HIPAA.

Covered Entities, Business Associates, and Protected Health Information

Kevin still isn't clear on everything that HIPAA includes and who it affects. You know there are people in your office who can offer a better explanation.

Sally in HR
Sally in HR: HIPAA applies to all **covered entities (CEs)** and their business associates. HIPAA-covered entities include healthcare providers, health plans, and healthcare clearinghouses.

Kevin: Does this company qualify as a CE?

Sally in HR: "Yes, and so do many other businesses, including but 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 work for a CE, you must comply with HIPAA. Some states or organizations have to follow stricter guidelines than HIPAA. Consult with your supervisor to determine whether these apply to you.

You can also request a copy of the HIPAA Policies and Procedures to review and follow.

HIPAA Privacy and Security Officer Jen
Kevin: Since my job requires me to work with outside companies, do they have to follow HIPAA guidelines as well?

HIPAA Privacy and Security Officer Jen: The outside companies **do** qualify as Business Associates (BAs). BAs are persons or entities who perform functions on behalf of, or provide certain services to, a covered entity that involves protected health information. Here is a list of other BAs that work with the company:

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

HIPAA Privacy and Security Officer Jen: Did you discuss vendor contracts during orientation?

Kevin: I remember seeing something then, but I didn't read it thoroughly.

Jen: Let's review it together.

She pulls up a copy of the document.

HIPAA Privacy and Security Officer Jen: BAs are responsible for carrying out contractual obligations and are directly liable for certain HIPAA violations. All BAs must enter into a contract with a CE to ensure that they understand the responsibility of safeguarding protected health information, or PHI.

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

Supervisor Bill
Supervisor Bill: Covered entities must protect the privacy and security of protected health information, or **PHI**.

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, or zip code)
- All dates, except for the year, related to the person (including birth date, admission date, discharge date, and 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

Kevin reports to you that he has learned a lot about HIPAA, but you still wonder how he will do when actual situations arise.

On the Job

PHI should be kept in an area that can be locked or, at a minimum, in an area where access can be restricted. As Kevin starts working, he finds out that he will have access to PHI in a locked filing cabinet. He comes to you with the following concern:

Kevin: I'm preparing an electronic file for storage at a data warehouse and that file contains last year's billing information for a community health clinic. 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.]

Permitted Uses and Disclosures of PHI

You bump into Kevin at the time clock one morning and he is reading a note on the wall: "Susan should be given her Depakote® in the afternoon rather than morning, effective June 26."

(Kevin): Is that an acceptable disclosure of PHI?

A. Yes
B. **No**
   Feedback [Since Kevin shouldn't be seeing this information, this is most likely a HIPAA violation. The staff member did not use any safeguards to prevent Kevin, or anyone else who clocks in, from seeing the record.]

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.

Alyssa
Kevin is helping Alyssa, a receptionist, with her computer. She asks him to cover the phone while she runs to the restroom.

The phone rings and Kevin answers.

Hi, I think my sister was admitted to your facility this morning, but I'm not 100% sure. Her name is Abby Gilbert. Can you tell me if she's there and how she's doing?

How should Kevin respond?

A. Your sister was admitted, but I'm not allowed to tell you anything else about the situation.
B. Your sister was admitted here. She's doing fine and will probably be ready to go home soon.
C. **I'm sorry, but I'm 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.]

Later, Alyssa asks her supervisor to come by after Kevin leaves to review a referral that contains PHI to check its accuracy. Is this allowed?

A. **Yes**
B. No
   Feedback [This is an allowable disclosure of PHI because it is for purposes of coordinating treatment. However, if Alyssa had this discussion in front of Kevin, this would be a HIPAA violation.]

A man who received services at your organization a year ago calls to request a copy of his file. Is Alyssa allowed to send him a copy of his PHI 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, however, that your organization has an obligation to take reasonable steps to verify the identity of the individual before providing this access (Department of Health and Human Services, 2020).

Be 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.

At lunch, Kevin overhears a conversation in the breakroom 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. Kevin did not need to know this information for any approved purposes, and the staff did not take appropriate precautions to protect the information.]

Breaches

Keeping PHI confidential means making sure that electronic systems that receive, maintain, or send PHI are secure. Failure to do this could result in a breach.

A “breach” under HIPAA means that unsecured PHI has been acquired, accessed, used, or disclosed. Breaches pose a large risk of financial and reputational harm to the individual and covered entity.

Affected individuals and the government must be notified of any breach unless the covered entity conducts a risk assessment and proves that disclosure is unlikely.

Penalties for HIPAA violations can range from $120 to over $1,500,000 annually, depending on the severity* (Alder, 2021). Penalties are increased when violations are not corrected within a specific time frame.

*Fines are adjusted annually based on inflation.

Later in the Week

Kevin is working on a file. He recognizes the name of a close friend of his on a list of people receiving services. He is surprised that his friend did not mention he was familiar with the organization when Kevin talked to him the other day about working there.

Kevin tells you that he is going to post on his friend’s Facebook® page and ask why he’s being so secretive. What should you tell him?

A. Don’t be mean about it. Just make contact and offer some words of encouragement.
   Feedback [Wrong move. This is a breach. Kevin’s friend is furious and demands to know how Kevin found out he was receiving treatment. Kevin’s friend contacts the organization and files a complaint.]
B. **Don’t do it. Contacting your friend would be considered a breach.**
   Feedback [Good save! Although his intentions were good, Kevin would have probably been in serious trouble personally **and** professionally if he contacted his friend.]

Kevin is continuing to work on a billing file when his stomach growls. Because he is working on a deadline, he takes his laptop to the cafeteria with him so he can eat and work at the same time. You are already there having lunch, so Kevin joins you. Halfway through lunch, Kevin wants a cup of coffee. He asks you to watch his computer and starts to walk toward the breakroom.

What should you do?

A. **Remind Kevin to lock his computer, so no sensitive information is available to anyone else.**
   Feedback [Anytime you step away from your computer you should take steps to ensure any PHI cannot be seen by other persons.]
B. Tell Kevin you will keep an eye on his computer.
   Feedback [Unfortunately this is not enough. Jen, the HIPAA security officer, walks by and sees Kevin’s computer screen and asks whose computer it is. When Kevin returns,

Jen asks to speak privately with him in her office about the lack of security. This could be bad for Kevin.]

C. Do nothing.
Feedback [While you were eating, you began talking to a coworker at the next table and someone came by and picked up the computer! This is a serious breach and Kevin must report it to the HIPAA privacy officer according to company policy. The company will have to report the breach.]

Steps to Avoid HIPAA Violations

As Kevin's first week comes to a close, you remember you will be out next week on a business trip. Kevin needed a lot of help this week and you don't want him to commit any HIPAA violations while you are gone. You decide to make some sticky notes that he can put at his desk to remind him of a few steps he (and you) can take to avoid HIPAA violations.

A. **Know and follow your company's HIPAA policies and procedures**.
Feedback [Correct!]

B. **Do not discuss anyone's protected health information (PHI) with fellow employees unless it is for the purposes of treatment, payment, or healthcare operations.**
Feedback [Only have those discussions in private areas where you cannot easily be overheard.]

C. Never discuss your job outside of the work environment.
Feedback [It is actually okay to discuss your job as long as you maintain the privacy of any individuals with whom you work and do not disclose any PHI.]

D. Shred all documents containing PHI at the end of each workday.
Feedback [You definitely don't want to shred ALL documents containing PHI; just make sure to lock them back up or put them in the appropriate place where they are supposed to be kept.]

E. **No matter how interesting it seems to you, do not share anyone's PHI with friends or family.**
Feedback [This is important. 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. Someone might realize, "Hey, my cousin had that problem and she was in that hospital!".]

F. **Do not leave PHI unattended or allow it to be visible to visitors.**
Feedback [Don't forget this one! Turn computer screens away from the door, lock up files after you are done using them, and avoid discarding PHI in an open trashcan. When PHI is no longer needed, it must be properly shredded or made impossible to read or reconstruct.]

G. Never send any PHI electronically.
Feedback [You actually can send PHI electronically as long as it is adequately protected.]

H. **Confirm you are following your company's HIPAA policies before sending PHI in an email or by fax to anyone inside or outside of the organization.**
Feedback [Double check the email or fax addresses before you send them.]

Section 2: Conclusion

Course Summary

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

- The purpose of HIPAA
- Various types of HIPAA violations
- Steps to take to avoid a HIPAA violation

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

Health Insurance Portability and Accountability Act of 1996 (HIPAA), P.L. 104-191. 42 U.S.C. § 1320d-9 (2010).

Health Information Technology for Economic and Clinical Health Act (HITECH). P.L. 111-5, div. A, Title XIII, Sec. 13111, Feb. 17, 2009, 123 Stat. 242. 42 U.S.C. § 156 (2011).

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

References

Alder, S. (2021). What are the penalties for HIPAA violations. Retrieved from https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/

Department of Health and Human Services. (2020). Individuals' right under HIPAA to access their health information. Retrieved from http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/

Exam and BrainSparks

CE (Y)	BS (Y)	LO #	Q #	Question
		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.
		2	2	True or False: Your company can be fined up to $50,000, per violation, for violating HIPAA even when you disclose PHI by mistake.
			a	True
			b	False
		3	3	Mark is catching up on progress notes after his shift. He remembers a funny incident in which a patient forgot to put on his pants before he went to breakfast. Mark tells the other professionals about the incident, who are also catching up on progress notes. Mark laughingly says, “Mr. Jones’ dementia is really getting the best of him.” Is Mark in violation of HIPAA?
			a	Only if the information revealed exposes Mr. Jones to reputational harm.
			b	No, it is an acceptable disclosure because only other professionals were in the room.
			c	Yes, this information is protected by HIPAA.
			d	No, it is an acceptable disclosure because it was for the purposes of treatment.
		3	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
		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
		3	6	Which of the following is the LEAST likely way to avoid a HIPAA violation?
			a	Learn the company's HIPAA policies and procedures.
			b	Lock up all files containing PHI prior to leaving your office or desk area.
			c	Ask your friends to promise they won't repeat anything you tell them about work.
			d	Refuse to discuss the treatment of a celebrity recently admitted to your facility.
		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	Tamara is behind on her work as an analyst and decides she needs to do some work at home tonight. She copies the files she has been working on (which contain PHI) to a flash drive and drops the flash drive in her purse for later use. When Tamara gets home, the flash drive is missing. Is this a security breach?
			a	No. Tamara doesn't know who has the flash drive or whether the PHI was accessed, so it is not a security breach.
			b	Yes, it is a security breach. The data on the flash drive was not protected and there is no way to undo the potential damage because the flash drive is lost.

			c	No, because Tamara's loss of the flash drive was accidental.
			d	No. Anyone who picked up the flash drive wouldn't know what it is or how to use it.
		2	9	Raj has been reviewing copies of medical records of patients from his clinic to see if he can identify any opportunities for quality improvement. Company policy requires Raj to shred documents containing PHI. But the door to the shredder room is locked and Raj is tired. He decides to throw the copies out in the garbage can without shredding them, just this once. Has Raj violated HIPAA?
			a	Yes. Raj did not follow the company's HIPAA policies and procedures about proper disposal of PHI. He could have locked them up for later "proper" disposal. He has violated company policy and HIPAA.
			b	No. Because Raj usually shreds PHI, throwing PHI in the garbage one time is not a violation.
			c	No. The door to the shredder was locked so Raj couldn't comply.
			d	Yes. Raj should have taken the documents home with him until he could shred them the next day.
		2	10	You may disclose PHI without an authorization EXCEPT:
			a	For entertainment purposes
			b	For treatment purposes
			c	For payment purposes
			d	For healthcare operations