

HIPAA Basic Privacy Training

2015

Objectives

By the end of this program, participants should be able to:

- Discuss the background and purpose of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule
- Identify the ways in which HIPAA applies to healthcare providers
- Review basic HIPAA definitions
- Apply HIPAA basics in the practice setting



What is HIPAA?

HIPAA is a federal law enacted in 1996.



The original intent of HIPAA was to reduce costs, simplify administrative processes, and improve the privacy and security of individuals' health information in the healthcare industry.



HIPAA has five major provisions.



HIPAA's Privacy Rule was enacted to protect the confidentiality of patients' health information.



Definitions

Covered Entity (CE)

Healthcare providers, health plans, and healthcare clearinghouses who electronically transmit any health information.

Protected Health Information (PHI)

Information the CE creates or receives that identifies the patient, including demographic information (e.g., addresses, phone numbers, etc.). PHI can relate to the past, present, or future physical or mental health or condition of a patient.

Business Associate (BA)

A person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a CE.

Breach

An impermissible use or disclosure of PHI that compromises the security or privacy of PHI.



To Whom Does HIPAA Apply?

HIPAA applies to all staff (including temporary staff, students, and volunteers) and any vendors (business associates) that have access to PHI.



Staff responsibilities

All staff members have a duty to:

- Maintain the confidentiality of patients' PHI as required by HIPAA
- Use, view, or discuss patients' PHI only as required by job responsibilities
- Understand HIPAA policies
- Immediately notify the organization's privacy officer of any suspected or actual breach of patients' PHI
- Direct questions or concerns to the organization's privacy officer

NOTE: Never informally discuss or make comments about patients.



Applying HIPAA in the Practice Setting

Notice of Privacy Practices

- The Notice of Privacy Practices sets forth how an organization will use and disclose patients' PHI (including examples).
- All patients are required to have an opportunity to obtain and read a copy of the organization's Notice of Privacy Practices and sign an acknowledgement form on their first visit or encounter.



Releasing Patients' PHI — Patient Rights

Patients have a right to:

- View and receive a copy of their medical records
- Request amendments or changes to their medical records
- Request restrictions to the use or disclosure of their PHI
- Request an accounting of the disclosures of their PHI



Releasing Patients' PHI — Basic Rules

Patients' information can be released without authorization if the purpose is for treatment, payment, or healthcare operations.

Disclosure of patients' PHI for anything other than treatment, payment, or healthcare operations requires completion of an authorization.

Certain exceptions exist for public health monitoring activities (e.g., disease reporting), government oversight, and some law enforcement investigations; however, staff should always consult with the privacy officer to ensure proper release.



Disclosure of PHI to BAs

Authorizations are not required for BAs who perform certain functions for the CE.

Examples of BAs include billing companies, transcription services, IT vendors, and accountants.

Patient authorizations are not necessary for BAs; however, business associate agreements — which set out the duties required of the BA to protect patients' PHI — are required.



What is the Minimum Necessary Standard?

Whenever patients' PHI is used or disclosed, whether to another CE or BA, only the information necessary to accomplish the intended purpose should be disclosed.

Example: The practice uses a collection agency that has requested billing information on several patients. The practice sends the billing information, but also includes patients' diagnostic information. The collection agency does not need the diagnostic information to perform its tasks; thus, the practice has violated the minimum necessary standard.



Breach Notification — Examples

Looking at a neighbor's medical record out of curiosity

Mailing billing information to the wrong patient

Losing an unencrypted thumb drive

Talking to a family member about a patient

Providing records to an attorney without authorization

Lost or stolen computer that contains PHI

NOTE: Staff should immediately notify a supervisor or privacy officer if they suspect or discover a breach has occurred.



Civil Monetary Penalties

- Failure to comply with policies and procedures may result in corrective action.
- CEs (including individual employees) and BAs are subject to civil monetary penalties (fines) and criminal penalties.

TABLE 1—CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE

Violation category—Section 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	\$100–\$50,000	\$1,500,000
(B) Reasonable Cause	1,000–50,000	1,500,000
(C)(i) Willful Neglect—Corrected	10,000–50,000	1,500,000
(C)(ii) Willful Neglect—Not Corrected	50,000	1,500,000



Criminal Penalties

Prohibited Conduct	Penalty
Knowingly obtaining or disclosing PHI without authorization	Up to \$50,000 fine and 1 year in prison
If done under false pretenses	Up to \$100,000 fine and 5 years in prison
If done with intent to sell, transfer, or use the information for commercial advantage, personal gain, or malicious harm	Up to \$250,000 fine and 10 years in prison



Frequently Asked Questions

Can I call a patient's name in the waiting room?

- Yes, as long as the patient does not object.

A patient's spouse calls to ask about recent test results? Can I provide him/her with this information?

- You can provide the information only if the patient has listed his/her spouse as a person who may receive their PHI.

Can I fax or mail a copy of a patient's medical record?

- Yes, if the patient designates faxing or mailing as the way he/she wants to receive a copy of the record. The patient should sign an authorization to provide a record of the release.



Frequently Asked Questions

The patient asks for his/her original record. Can I provide the original?

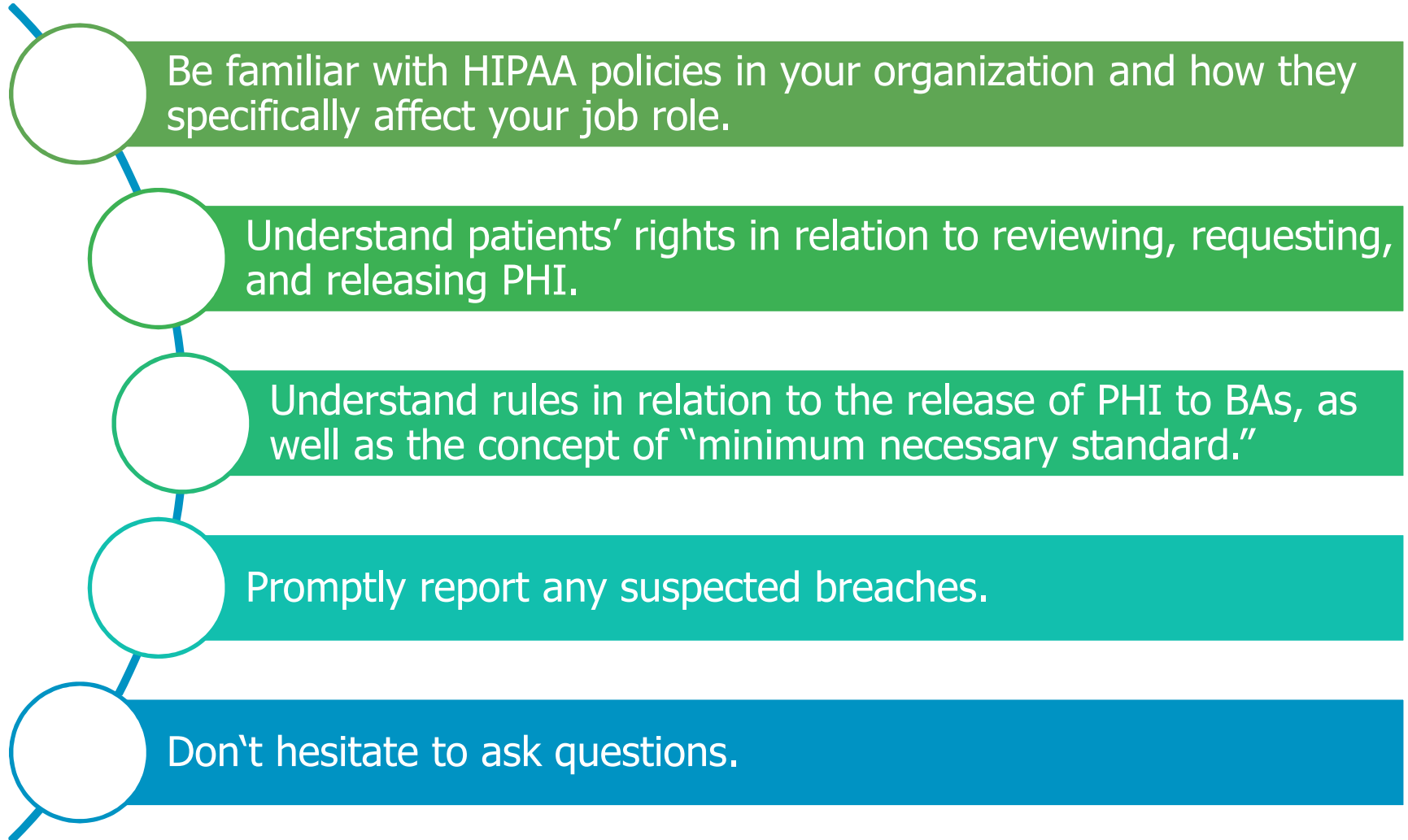
- You should never release the original record, which is the property of the healthcare organization. HIPAA stipulates that patients may receive a copy. You can offer to allow the patient to inspect the original record onsite with someone present.

The patient has requested that we do not provide information to his/her insurance company. Can we honor that request?

- Yes, you are required to comply with the request as long as the patient pays for the services out of pocket.



Summary



Be familiar with HIPAA policies in your organization and how they specifically affect your job role.

Understand patients' rights in relation to reviewing, requesting, and releasing PHI.

Understand rules in relation to the release of PHI to BAs, as well as the concept of "minimum necessary standard."

Promptly report any suspected breaches.

Don't hesitate to ask questions.

