

HIPAA Training for the MDAA Preceptorship Program

Health Insurance Portability and
Accountability Act

Objectives

- Understand what information must be protected under the HIPAA privacy laws
- Understand the HIPAA patient rights
- Be aware of consequences for non-compliance

History

- **HIPAA, passed in 1996, sought to make health insurance more efficient and portable. Administrative simplification will save the healthcare industry billions of dollars. Because of public concerns about confidentiality, it also addresses information protection.**

HIPAA

- **HIPAA Privacy Standards:**

- Protect the privacy and security of a person's health information

- ***When:***

That health information is used, disclosed or created by
a:

- Healthcare Provider
 - Health Plan
 - Healthcare Clearinghouse

PHI

- **What information must you protect?**

Information you create or receive in the course of providing treatment or obtaining payment for services or while engaged in teaching and research activities, including:

- Information related to the past, present or future physical and/or mental health or condition of an individual
- Information in ANY medium –whether spoken, written or electronically stored –including videos, photographs and x-rays

This information is:

PROTECTED HEALTH INFORMATION (PHI)

- **The Notice of Privacy Practices allows PHI to be used and disclosed for:**
 - Treatment
 - Payment
 - Operations (teaching, medical staff/peer review, legal, auditing, customer service, business management)
 - Hospital directories
 - Public health and safety reporting
 - Other reporting required by government, such as in cases of abuse
 - Subpoenas, trials & other legal proceedings

- **Other uses require authorization:**

- For many other uses and disclosures of PHI, a written authorization from the patient is needed
 - Example: disclosures to an employer or financial institution or to the media or for research when the IRB has not provided a waiver of authorization
- HIPAA has very specific requirements for the authorization. It must:
 - Describe the PHI to be released
 - Identify who may release the PHI
 - Identify who may receive the PHI
 - Describe the purposes of the disclosure
 - Identify when the authorization expires
 - Be signed by the patient/patient representative

“Minimum Necessary”

- **Except for treatment, the “Minimum Necessary” applies**
- For patient care and treatment, HIPAA does not impose restrictions on use and disclosures of PHI by health care providers.
 - There are restrictions on disclosure of psychotherapy notes, AIDS test results and substance abuse information.
- For anything else, HIPAA requires users to access the least amount of information necessary to perform their duties.
 - Example: a billing clerk may need to know what laboratory test was done, but not the result.

Incidental Uses and Disclosures of PHI

- “Incidental” means a use or disclosure that cannot reasonably be prevented, is limited in nature and occurs as a by-product of an otherwise permitted use or disclosure.
 - Example: discussions during teaching rounds; calling out a patient’s name in the waiting room; sign in sheets in hospital and clinics.
- Incidental uses and disclosures are permitted, so long as reasonable safeguards are used to protect PHI and minimum necessary standards are applied.

HELP KEEP PHI CONFIDENTIAL

Consider the following example:

- You are a healthcare provider. Your friend's spouse is in the hospital after an accident. Your friend asks you to review what treatment has been provided to the spouse and see if you concur. What are you able to do under HIPAA?
 - A. Access the person's chart so that you can communicate with your friend about the patient's condition.
 - B. Contact the charge nurse on the floor and ask her to look into the patient records for you.
 - C. Advise your friend that you can only look at the medical records if you are treating the patient or you receive the patient's authorization to review the medical record.

Answer

- C. Under HIPAA you are only allowed to use information required to do your job.
- Since you are not part of the patient care team, it is against the law to access the patient record or ask someone to access it on your behalf –even though you may know the person and just want to be helpful. Remember, that if you were in a similar situation, you may not want your colleagues going through your medical records or those of your spouse or close friend.

Consider the following example

- The father and mother of an adult married competent patient are visiting the patient. As a member of the care team, you need to review and provide education to her on the new meds ordered by the physician. One medication is Prozac, a well known anti-depressant. What is the best way to approach a patient when her relatives are in the room?
 - A. Ask the patient's relatives to leave the room.
 - B. Go ahead and explain the medications to her. She won't mind her family members overhearing.
 - C. Explain to the patient that you need to discuss her medications with her, and that the information is confidential. If she says her relatives may stay in the room, go ahead explain the medications to her

Answer

- C. Never assume that the patient has shared her medical information with her relatives.
- You should ideally ask the patient's relatives to step out of the room. If the patient understands that the information is sensitive and she agrees to have her relatives present, you can go ahead and have the discussion with the patient.
 - The answer would be the same if it had been her husband visiting her. The patient may not have shared all of the information with her husband.

Penalties for Violations:

- A violation of federal regulations or University Policy can result in discipline, loss of employment, fines or imprisonment.
- If a disclosure of PHI is made willfully and with an intent for personal gain, the penalty can be as high as a \$250,000 fine and 10-year imprisonment. The University would not consider such an action as in the course and scope of your employment and would not defend you.

HIPAA Do's and Don'ts

- Treat all patient information as if you were the patient. Don't be careless or negligent with PHI in any form, whether spoken, written or electronically stored.
- Shred or properly dispose of all documents containing PHI that are not part of the official medical record. Do not take the medical record off of University property. Limit the PHI you take home with you.
- Use automatic locks on laptop computers and PDAs and log off after each time you use a computer. Do not share passwords. Purge PHI from devices as soon as possible.

HIPAA Do's and Don'ts

- Use secure networks for e-mails with PHI and add a confidentiality disclaimer to the footer of such e-mails. Do not share passwords.
- Set a protocol to provide for confidential sending and receipt of faxes that contain PHI and other confidential information.
- Discuss PHI in secure environments, or in a low voice so that others do not overhear the discussion.

Consider the following example:

- A physician and a nurse were discussing a patient in an elevator filled with people. In the conversation the patient's name, diagnosis and prognosis are mentioned. What could have been done differently to protect the patient's privacy?
 - A. The patient's privacy was protected, nothing was done wrong since no written PHI was exchanged.
 - B. It is important to be aware of your surroundings when you discuss patient information (PHI). The patient's case should have been discussed in another room, away from other patients, or at least in low voices that could not be overheard.
 - C. No patients or patient families should be allowed to use hospital staff elevators to avoid such situations.

Answer:

- B. Although HIPAA allows incidental uses and disclosures, this type of disclosure is not allowed. PHI includes oral communications. The patient's case should have been discussed in a location that allowed for privacy of the information discussed.

Consider the following example

- You are in the ER examining a 6-year-old boy and observe cigarette burns on the arms and hands of the boy. What does HIPAA require you to do?
 - A. HIPAA requires you to protect patient confidentiality so no disclosure of PHI should be made.
 - B. Patient safety is involved, and federal and state law require that you report this.
 - C. HIPAA does not allow you to report this incident, but state law requires it.

Answer:

- B. While HIPAA requires you to maintain patient confidentiality, exceptions exist which allow PHI disclosures. State law requires and HIPAA allows the reporting of child or elderly abuse and communicable diseases.