CCP Online Orientation

HIPAA ORIENTATION & EDUCATION

Objectives

At the conclusion of this presentation, students will be able to:

- Discuss application of HIPAA to student's role.
- Discuss the penalties that can be imposed for violating HIPAA.
- Identify what information must be protected.
- Describe how to protect confidential and sensitive information.
- State their responsibility for good computer practices.

What is HIPAA?

HIPAA is an acronym for the **H**ealth **I**nsurance **P**ortability and **A**ccountability **A**ct, which was enacted by the US Congress in 1996 and stresses three major areas:

- **1. Insurance Portability:** Ensures that individuals moving from one health plan to another will have continuity of coverage and will not be denied coverage.
- **2. Fraud enforcement (accountability):** Significantly increases the federal government's fraud enforcement authority to reduce health care fraud and abuse.
- **3. Administrative simplification:** Ensures system-wide, technical and policy changes in healthcare organizations in order to protect patient and resident privacy and the confidentiality of identifiable/protected health information (PHI).

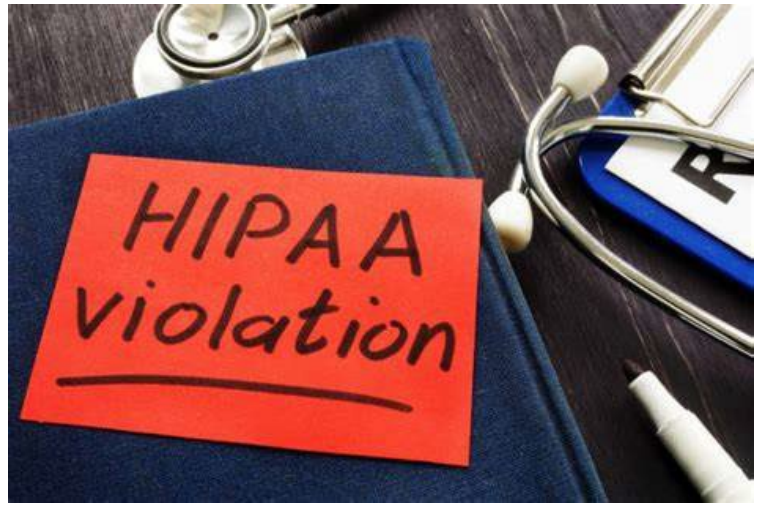
HIPAA Privacy Act

Effective April 14, 2003, each healthcare organization is required to:

- Give each patient or resident a written Notice of Privacy Practices that describes:
  - How health care organizations may use and share protected health information (PHI)
  - The patient's/resident's privacy rights
- Ask all patients/residents to sign a written acknowledgment that they received the Notice of Privacy Practices, except in emergency situations. If a signature is not obtained, the health care organization must document the reason why it was not role.

Breach

- A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.



Examples of Breaches

- Reviewing the medical records of family members, neighbors, celebrities, etc. to see how they are doing.
- Leaving papers with a patient's/resident's identifiable information in public areas visible to others.
- Failing to confirm the accuracy of a fax number before faxing patient-identifiable health information.
- Talking in public areas, talking too loudly, talking to the wrong person.
- Email or faxes sent to the wrong address, wrong person, or wrong number.
- User not logging off from the computer system, allowing others to access their computer or system.

Real Examples of Student Breaches

- Used a cell phone to take pictures of a patient/resident.
- Used a cell phone to record a health care provider explaining a surgical procedure.
- Posted a picture of themselves with a patient/resident on Facebook.
- Provided treatment advice to a patient/resident via Twitter.
- Posted a picture of a patient's/resident's open wound on the Internet.
- Posted details about their clinical day without mentioning the patient/resident's name but shared enough details about the injuries so that readers could guess who it was.
- Posted comments to a blog about a patient/resident they cared for in the previous year, including the name of the unit.
- Accessed their own medical record during clinical.

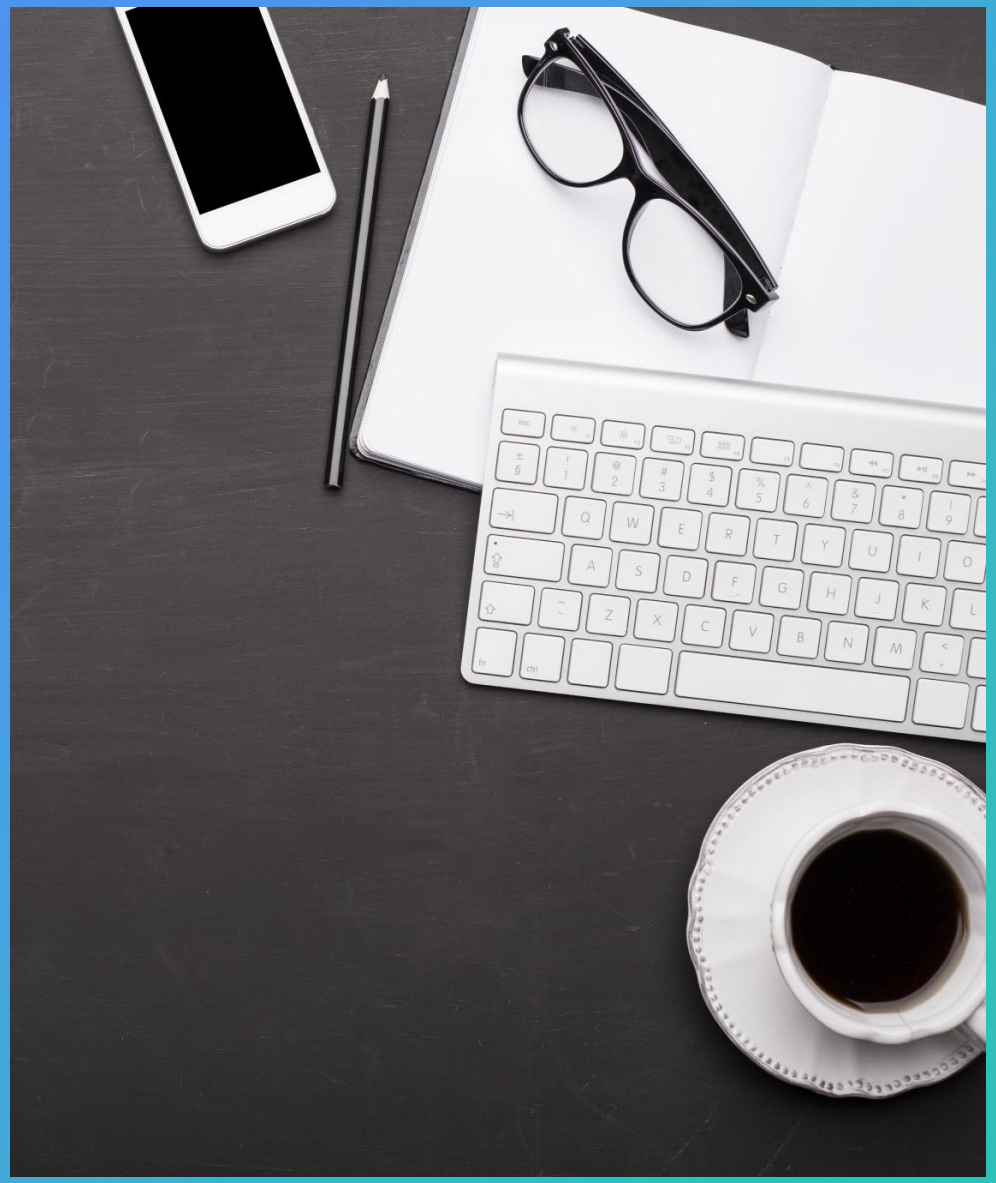
Unethical Behavior and Possible Breaches

- It is unethical and disrespectful to post negative comments about the health care organizations to which you are assigned for clinical or the staff who work there.
  - Instead, share questions and concerns with your clinical instructor rather than posting it on a social media site.

HIPAA Penalties

- Verbal or written warnings.
- Loss of job or dismissal from nursing program
- HIPAA Criminal Penalties
  - $60,000 - $1,800,000 fines
  - Imprisonment up to 10 years
- HIPAA Civil Penalties
  - $100 - $50,000 for each violation
- State Laws
  - **Fines and penalties apply to individuals as well as health care providers; may impact professional licensure.**

PENALTIES FOR STUDENTS MAY LEAD TO DISMISSAL FROM ACADEMIC PROGRAM.



What is Protected Health Information (PHI)

- PHI is all personal and health information specific to a patient or resident and must be kept confidential
    - Spoken
    - Written
    - Electronic

Examples of PHI

- Name, address, date of birth, social security number, phone number, email address, fax number, URL address, IP address, license number, biometric identifiers (finger and voice prints), vehicle identifiers.
- Medical record, health plan number, diagnosis, photographs, test results, prescriptions and labels on IV bags.
- Billing information, account number, claim data, referral authorization.
- Research records.
- Telephone notes.

Uses and Disclosures of PHI

- **Healthcare Organizations may Create, Use and Share PHI for: TPO**
  - **Treatment** that is routinely shared among health care professionals involved in the care to coordinate or manage treatment, both within and outside each healthcare organization, including appointment reminders or laboratory results as part of discharge planning.
  - **Payment** of health care bills may be shared with the medical insurer so that the health care organization can be paid for services provided to the patient or resident.
  - **Operations** to assess and improve quality of care or re-allocate resources. The details of a patient's surgical procedure may be shared among surgeons to evaluate the patient's surgery based on the outcome.
- EXCEPTION: Whenever state law is more stringent, it preempts HIPAA. In Massachusetts, New Hampshire, Maine & Rhode Island, statutorily protected information including HIV status, behavioral health, psychotherapy notes, and sexually transmitted diseases requires patient authorization prior to use / disclosure.

Examples of TPO

- The patient's referring physician calls and asks for a copy of the patient's recent lab report completed at the health care organization (**Treatment**)
- A patient's insurance company calls and requests a copy of the patient's medical record for a specific service date (**Payment**)
- The Quality Improvement office calls and asks for a copy of an operative report (**Health Care Operations**)

For these TPO purposes, patient information may be provided

Other Uses and Disclosures of PHI

- Facility Directory may include (a) name, (b) location in the health care organization, (c) general condition, and (d) religious affiliation, unless the patient/resident tells the health care organization not to.
- State Law mandates sharing of the PHI to state agencies under certain circumstances, without the patient's or resident's consent, such as abuse reporting to the Department of Social Services and Death Reports to the Office of the Medical Examiner.
- Medical Research may use PHI to further medical research, but only after approval by the Institutional Review Board (IRB), when written permission is not required by Federal or State law.

HIPAA Rule

- Mandates that all employees, physicians, volunteers, students and other members of the healthcare organization's workforce follow the HIPAA-required procedures and do the **RIGHT THING** when it comes to protecting the privacy and security of their patients or residents.

Receiving Request for PHI in Emergency

- Obtain the requesting provider's name, facility name, location and telephone number.
- Verify the requestor's identity by telephoning the number provided.
- Document the call and identity of the individual who received the call.
- Document the information being sought or requested.
- Document the reason for the request.
- Provide minimum necessary PHI.
- Provide additional information requested as in non-emergency.

As a Student you may:

- Look at a person's PHI only if you need it to do your assignment.
- Use a person's PHI only if you need it to do your assignment.
- Give a person's PHI to others when it is necessary for them to do their jobs.
- Talk to others about a person's PHI only if it is necessary to do your assignment.

- * **REMEMBER**:
  - **If it doesn't pertain to Treatment, Payment or Operations (TPO), don't discuss it.**

As a Student you may NOT:

- Access your own personal medical record or the medical records of family or friends.
- Post any information about a patient/resident or the health care organization on any social media site, such as:
  - Facebook,
  - Twitter, Tumblr,
  - Blogs,
  - Podcast,
  - Discussion forums,
  - Photo Sharing, Snapchat, Flickr, Instagram,
  - YouTube/Video, TikTok, etc.

Providing for Security of PHI

- **General awareness**
  - Use the healthcare organization's policies to know what information is confidential.
  - Never discuss patient/resident information outside the workplace.
  - Be careful not to discuss patient or resident information in hallways, elevators, cafeterias, or other common areas where you may be overheard.
  - Ensure that anyone looking at a patient's/resident's chart or inquiring about information has valid and appropriate identification and a need to know (part of the healthcare team).

Providing for Security of PHI

- **Computers**
  - Sign on promptly with your password/login.
  - Do not share your passwords.
  - Do not use another's password/login, including *Instructor's* or *Preceptor's.*
  - Be sure that prior **users** are logged off the system before **using** the computer.
  - Log-off computers when finished.
  - Point computer monitors away from the view of visitors or passers-by.
  - **Note:**
  - Personal information must be protected and encrypted on laptops or other portable devices.
  - Personal information must be encrypted when sent across the internet.

Providing for Security of PHI

- **Telephone**
  - Do not leave confidential information on an answering machine.
  - Follow established policies about what patient or resident information can be given over the phone.
  - Do not listen to your voice mail messages over the telephone speaker.
  - Never discuss confidential information on an analog mobile phone (although this is illegal, analog calls can be intercepted and recorded).
- **Printers/Copiers**
  - Promptly remove printouts of confidential material.
  - Do not leave printouts with a patient's or resident's information unattended.
  - Stay at the copier while copying is in process.
  - Do not forget to take the original.
  - **Do not copy a patient's/resident's medical record.** If patient/resident requests a copy, follow health care organization's policy.

Providing for Security of PHI

- **Email**
  - Do not share your password.
  - Never forward messages that have confidential patient information unless authorized to do so.
  - Do not use sensitive information. Emails can be intercepted.
- **Fax Machines**
  - Make sure the fax machine is in a secure location.
  - Notify receiver ahead of time that you are faxing information and verify the fax number.
  - After you dial the number, double check it on the display before you press send.
  - Confirm receipt by calling the recipient or checking the transmission report.
  - Retrieve faxed information as soon as it arrives.
  - Always use a cover sheet stating that the information being sent is confidential.
  - If a fax is sent to the wrong machine, contact the recipient and request the fax be destroyed. NOTIFY PRIVACY OFFICER.

Providing for Security of PHI

- **Cell Phone Camera**
  - Do not use a cell phone camera to take a picture of a patient/resident.
  - Do not text information about a patient/resident.

- **Interviewing**
  - Close patient/resident room doors.
  - Close curtains and speak with a softer voice in a semi-private room.

- **Sensitive Data**
  - Secure paper records that contain PHI.
  - Destroy, shred or put in the designated bins all papers that could contain PHI. **Do NOT put in wastebaskets!**
  - Understand healthcare organization's policies for handling any patient/resident information.

Security of Electronic Information (ePHI)

- **Good security standards follow the "90/10" Rule:**
  - 10% of security safeguards are technical
  - 90% of security safeguards rely on the computer user (**YOU**) to adhere to good computer practices

Why is Protecting Privacy & Security so Important?

- It is the right and ethical thing to do.
- It is the legal thing to do and the Federal law requires it
- **DO NOT ACCESS INFORMATION THAT YOU DO NOT NEED TO KNOW FOR YOUR JOB**

Patient/Resident Rights

- **Under HIPAA privacy laws, patients/residents have the right to:**
  - Have their information protected.
  - Have their questions answered.
  - Receive written notice of how their health information will be used and disclosed.
  - Access their own records and request correction of incorrect or incomplete information.
  - Receive a list of disclosures of information within the previous six years (beginning 4/14/03).
  - Sign an authorization form prior to non-routine uses or disclosures of their health information before the information can be shared with:
    - Employers
    - Insurance Companies
    - Marketing Activities
    - Fundraising Activities

Consequences of Privacy or Security Failure

- Disruption of patient/resident care.
- Increase cost to institution.
- Legal liability and lawsuits.
- Negative publicity.
- Negative patient/resident perception.
- Identify theft.
- Disciplinary action.

Summary

- Patients/residents or their representatives have the right to control who will see their protected health information (PHI).
- HIPAA privacy requirements have been put in place to protect the patient.
- **NOTE:** These HIPAA privacy requirements apply just as much outside the workplace as they do inside. Patient/resident information is never shared outside the workplace, and only as necessary for care within the workplace.

References

- United States Health & Human Services . (AUG. 21, 1996). Public Law 104-191, 104th Congress, Health Insurance Portability and Accountability Act (HIPAA) of 1996. Retrieved from http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf.

- United State Center for Medicare and Medicaid. (n.d.). Health Information Privacy: General Information. Retrieved from https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/general-overview/index.html.

- United State Center for Medicare and Medicaid. (n.d.). Health Information Privacy. Retrieved from https://www.hhs.gov/hipaa/index.html