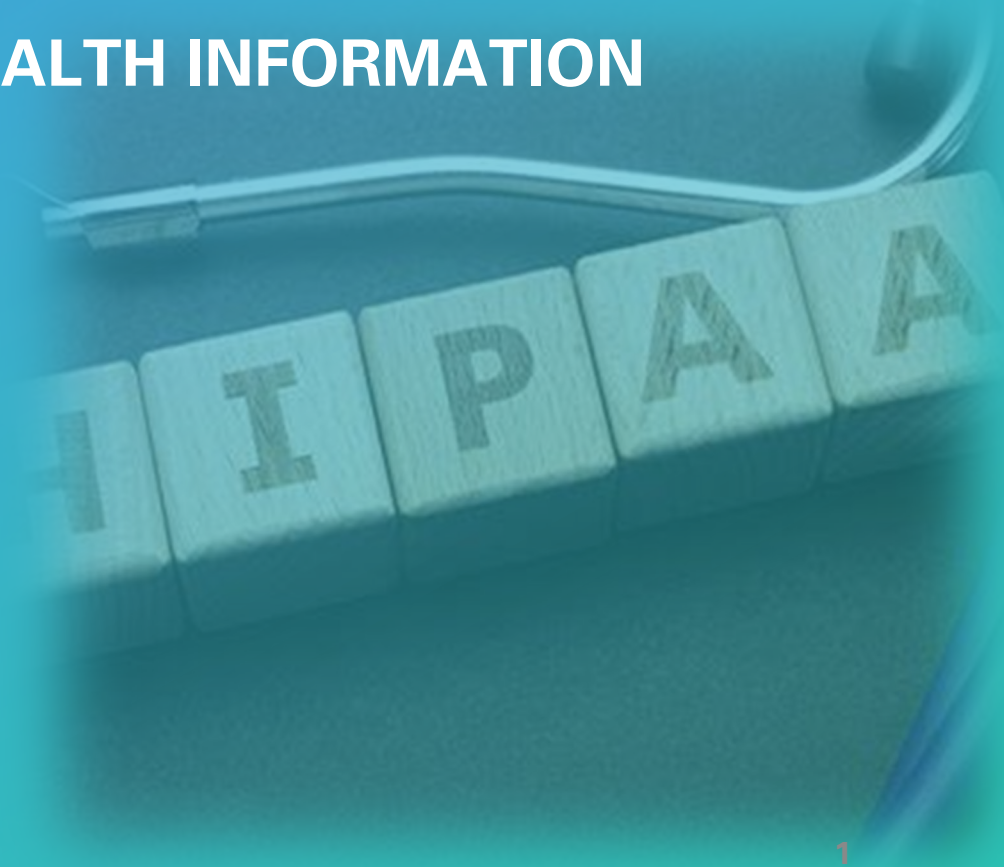
CCP Online Orientation

HIPAA TRAINING & COMPLIANCE

PROTECTING PATIENT PRIVACY & HEALTH INFORMATION



Objectives

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

- Understand the purpose and scope of HIPAA.
- Define PHI and recognize privacy risks.
- Learn how to maintain compliance in clinical settings.
- Know your responsibilities under HIPAA as a student.

What is HIPAA?

HIPAA standards for **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 can maintain health insurance coverage when changing or losing jobs..
- **2. Fraud enforcement (accountability):** Expands federal authority to investigate and penalize healthcare fraud, abuse, and waste.
- **3. Administrative simplification:** Sets national standards for electronic health care transactions and mandates the protection of **Protected Health Information (PHI)** through secure systems, policies, and training.

HIPAA Privacy Rule & Key Updates

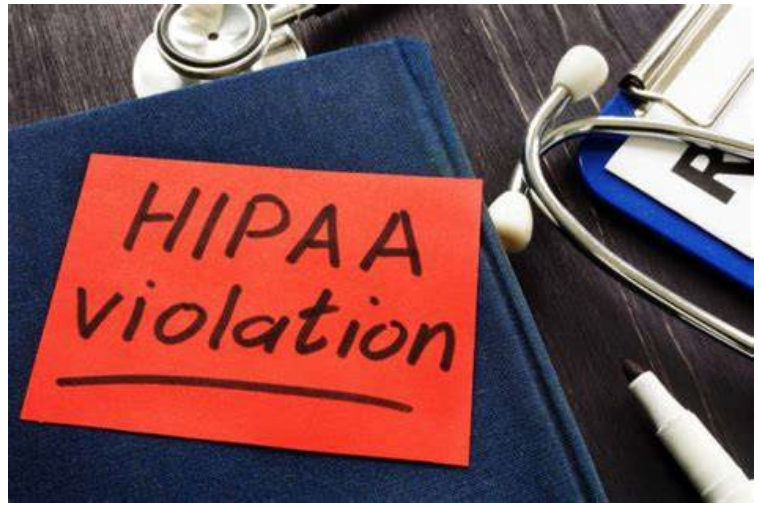
Effective April 14, 2003, the HIPAA Privacy Rule requires all healthcare organizations to**:**

- Provide each patient or resident with a **written Notice of Privacy Practices (NPP)** that explains:
  - How the organization may use and disclose **Protected Health Information (PHI)**
  - The patient's/resident's **rights** under HIPAA
- Obtain a **signed acknowledgment** from the patient/resident confirming they received the NPP.
  - If the patient cannot sign (e.g., due to an emergency), the reason **must be documented** in the medical record.

- **Key Enhancements**
  - **HITECH Act (2009)**: Strengthens HIPAA by increasing penalties for violations and encouraging secure **electronic health record** (EHR) use.
  - **HIPAA Omnibus Rule (2013)**: Reinforces HITECH by expanding privacy protections, mandating breach notifications, and extending compliance to business associates.

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.

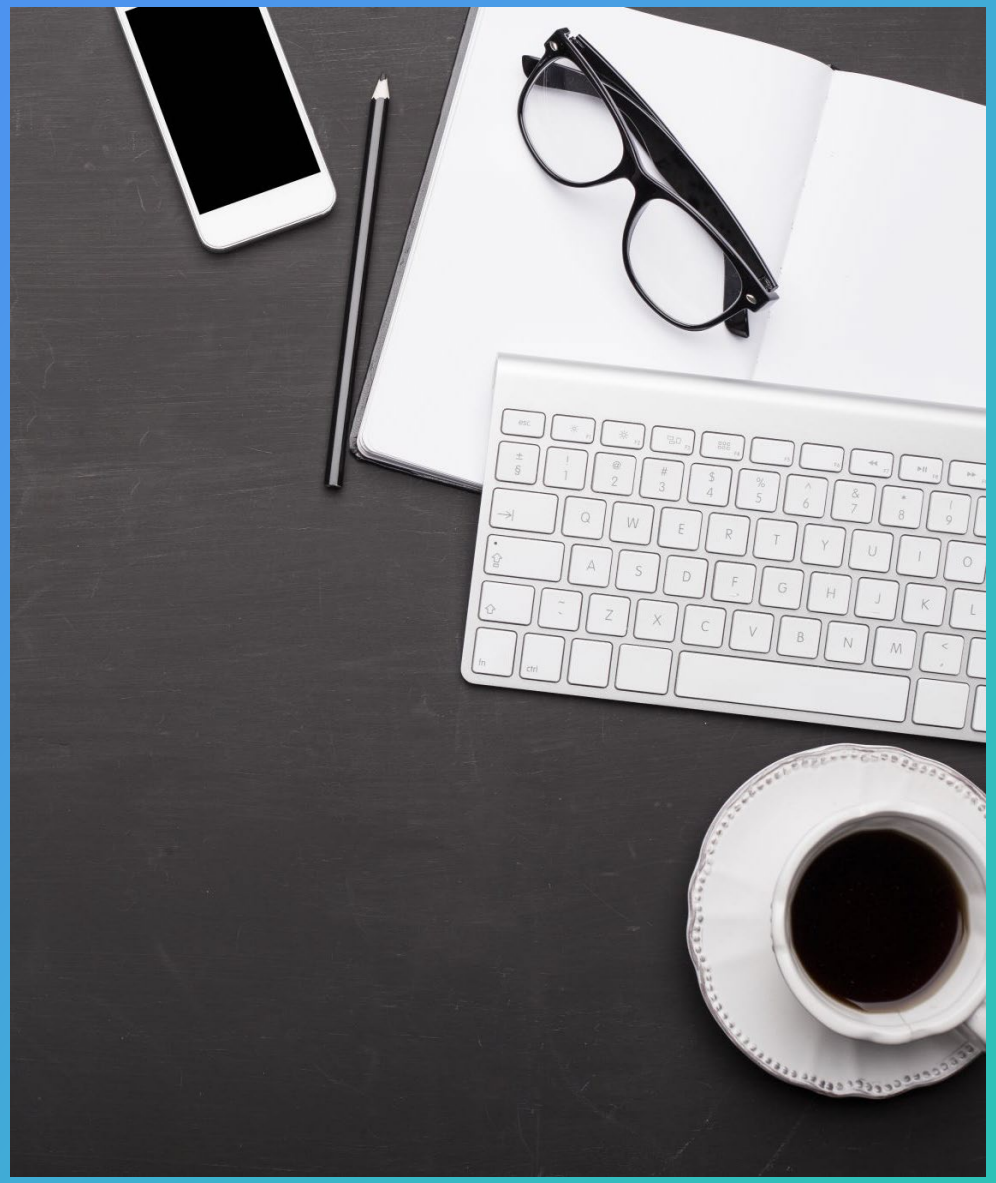
Unethical Behavior and Possible Breaches

- Its 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 it on a social media site.

HIPAA Penalties

- Verbal or Written Warnings
- Loss of Employment or Dismissal from an academic or clinical program *(especially for students in healthcare programs)*
  - HIPAA Criminal Penalties
    - **Fines:** $60,000 to **$1.8 million**
    - **Imprisonment:** Up to **10 years** for knowing misuse of PHI
  - HIPAA Civil Penalties
    - **Fines per Violation:** $100 to **$50,000**
    - **Annual Cap:** Up to **$1.5 million**
  - State Laws
    - Fines and penalties apply to individuals as well as health care providers
    - **May impact professional licensure**.

STUDENTS: Violations may result in dismissal from your 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
    - Oral
    - Written
    - Electronic

Examples of PHI

- **Personally Identifiable Information:** 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.
- **Health-Related Information:** Medical record, health plan number, diagnosis, photographs, test results, prescriptions and labels on IV bags.
- **Financial and Administrative Data:** Billing information, account number, claim data, referral authorization.
- **Additional Identifiers:** Research records, and 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.
- **Important Exceptions to PHI Disclosure:**
  - **State Law Preemption (Stricter Law Applies):**
    In states like **Massachusetts, New Hampshire, Maine, and Rhode Island**, patient authorization is **required** to use or disclose certain **statutorily protected information**, including HIV status, Behavioral health information, Psychotherapy notes, Sexually transmitted diseases.
  - **Federal Confidentiality Law (42 U.S.C. § 290dd-2 & 42 CFR Part 2):**
    Part 2 regulations **strictly limit disclosure** of information from **federally assisted alcohol and drug abuse programs.** PHI that could identify a person as a substance use patient is protected. **Patient consent is required**, with few exceptions (e.g., medical emergencies, audits)

Examples of TPO

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

- 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 Requirements** 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

- All employees, physicians, volunteers, students, and other workforce members **must follow HIPAA procedures** and **protect patient privacy and security** by doing the **right thing**—always.

Receiving Request for PHI in Emergency

- **Collect** requester's name, facility, location, and phone number
- **Verify** identity by calling the provided number
- **Document**:
  - Who received the call
  - Requester's identity
  - Information requested
  - Reason for request
- **Disclose** only the **minimum necessary PHI**
- **Follow up** with additional info as in a non-emergency

As a Student you may:

- **Access** PHI only if needed for your assignment
- **Use** PHI only when required for your assignment
- **Share** PHI only when others need it for their job
- **Discuss** PHI only when necessary for your assignment

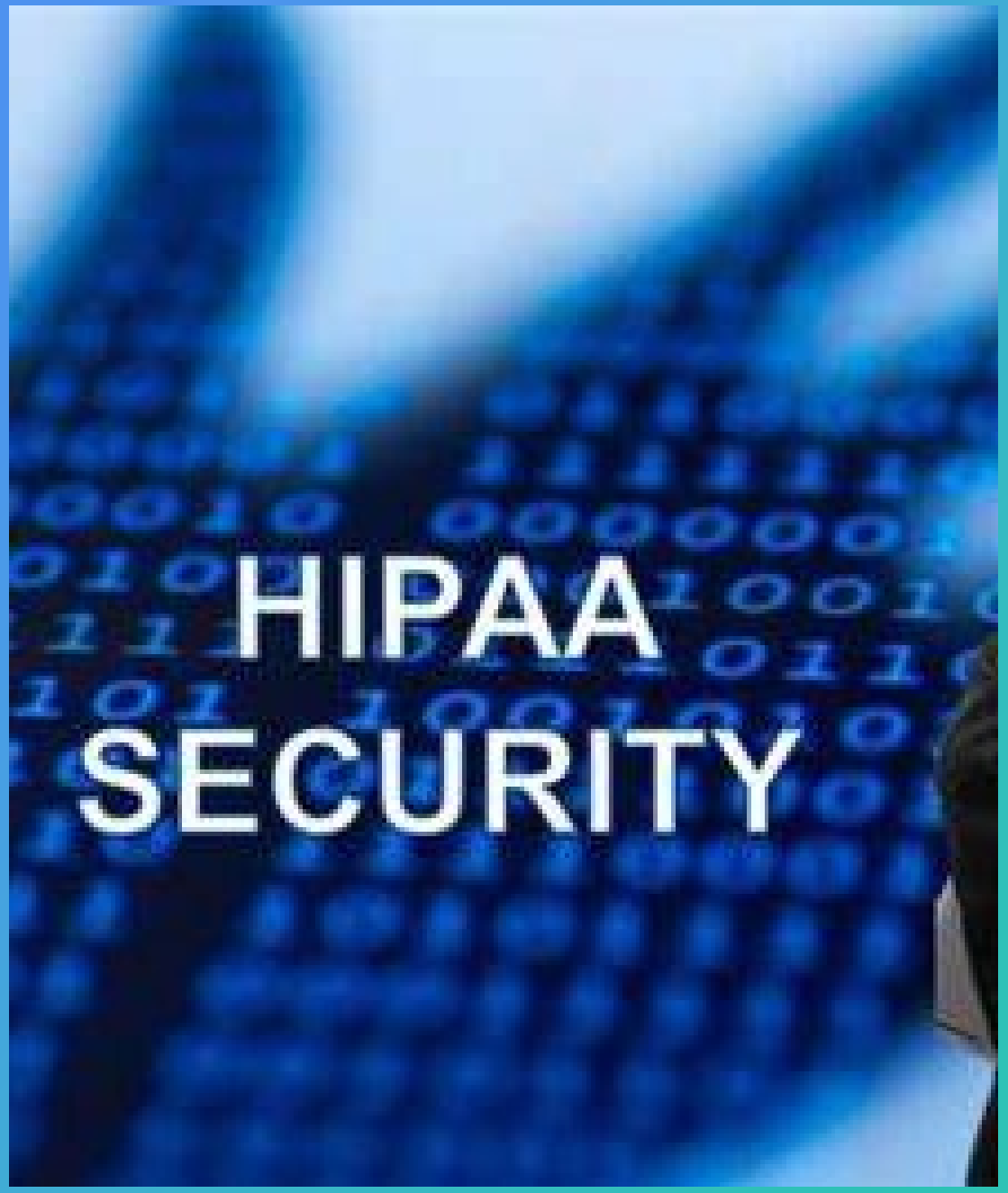
* **REMEMBER**:

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

As a Student you may *NOT*:

- **Access** your own medical record or those of family/friends

- **Post or share** any patient or facility information on **social media**, including:
  - Facebook, X (formerly Twitter), TikTok, Instagram
  - Snapchat, YouTube, Flickr
  - Blogs, Podcasts, Forums
  - Photo/Video sharing sites or apps



Providing for Security of PHI

- **General awareness**
  - Follow organization policies on confidential info
  - Never discuss patient info outside work
  - Avoid conversations in public areas (hallways, elevators)
  - Verify ID and need-to-know before sharing patient info

Providing for Security of PHI

- **Computers**
  - ➢Use your own login; never share or use others' passwords
  - ➢Ensure prior users are logged off before use
  - ➢Log off when done
  - ➢Position screens away from public view
  - ➢Encrypt PHI on laptops and when sent online

Providing for Security of PHI

- **Telephone:**
  - Don’t leave confidential info on answering machines
  - Follow policies on phone info sharing
  - Avoid voicemail on speakerphone
  - Don’t discuss PHI on analog phones (can be intercepted)

- **Printers/Copiers:**
  - Remove printouts promptly; never leave unattended
  - Stay by copier while printing
  - Take originals with you
  - Don’t copy medical records yourself; follow policy

Providing for Security of PHI

- **Email:**
  - Never share passwords
  - Only forward PHI if authorized
  - Avoid sending sensitive info via email

- **Fax:**
  - Use fax machines in secure areas
  - Verify recipient and fax number before sending
  - Notify recipient and confirm receipt
  - Retrieve faxes promptly
  - Always use confidential cover sheets
  - If sent wrong, request destruction and notify Privacy Officer

Providing for Security of PHI

- **Cell Phones:**
  - Don’t take patient photos or text PHI

- **Interviewing:**
  - Close doors and curtains
  - Speak softly in semi-private areas

- **Sensitive Data:**
  - Secure paper PHI records
  - Shred or use designated bins for PHI documents—no trash cans!
  - Follow organization policies for handling PHI

Security of Electronic Information (ePHI)

- Good security 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 Protect Privacy & Security?

- 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 control who will see their PHI.
- PHI is only shared as needed for care within the workplace
- **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