What is HIPAA?

• Health Insurance Portability and Accountability Act of 1996
• Bird’s eye view this Act aims to:
  – Establish national standards of electronic health transactions
  – Improve the Medicare and Medicaid programs and the efficiency and effectiveness of the health care system
HIPAA Components

HIPAA is comprised of three sets of regulations:

• **Transactions**: Standards for the content and format of certain electronic transactions.

• **Privacy**: Regulations safeguarding the privacy of an individual’s health care information.

• **Security**: Standards for assuring the confidentiality, integrity, and accessibility of electronic health information.

The remainder of this education will focus on HIPAA’s Privacy and Security components.
What is PHI?

- Protected Health Information is information that is:
  - Identifies a specific individual,
  - Transmitted or maintained in any form or medium; and
  - Relates to the past, present, or future
    - physical or mental health condition;
    - provision of health care; or
    - payment for health care.
So, once a specific individual can be identified, all health-related information is considered PHI. This can include, but is not limited to, the following:

- Name
- Address
- Age
- Social Security number
- Diagnosis
- Medical history
- Medications
- Observations of health status
Protected Health Information

• As students you will be exposed to and accessing large amounts of PHI.

• It is crucial as students and health professionals to keep PHI secure and take proper care when handling PHI.
Passwords

• Passwords are the individual’s responsibility and **are not** to be shared under any circumstances.

• **Never** write down passwords, store them on hard copy or to local workstations or laptop computers.

• **Never** write down your passwords on sticky notes and leave under your keyboard or in a desk.
Email

• Avoid transmitting PHI over email; however, if absolutely necessary:

  – Avoid putting PHI in the subject field.

  – Do not use an off-campus or non-secure email account (i.e., AOL, Hotmail, Yahoo).

  – Never transmit PHI through “instant messaging” programs or text.
Portable Devices

• **Never** store PHI on portable devices:
  – Laptops
  – iPads/Tablets
  – iPhone/Smart Phones
  – Jump (Thumb, Flash) Drives
Photography

• Photographs are considered PHI.

• Patients **must** provide written consent before you are permitted to take a photo.

• **NEVER** use cell phones/personal devices to take photos.

• Photos can only be taken by department approved devices.
Social Media

• **Never** post any patient information on a social media site.

• Social Media includes but not necessarily limited to: blogs, podcasts, discussion forums, Instagram, FaceBook, YouTube, LinkedIn, Twitter, location-based platforms and other online social networks.

• As a student you are obligated to comply with all HIPAA Privacy rules at all times and on/off campus.
Electronic Medical Record (EMR)

- As students you will be given access to the EMR at your clinical site.
- The EMR should be used for clinical care of the patients assigned to you or your team.
- Use of the EMR to view records of patients not on your service is a HIPAA violation:
  - Employees have been fired for viewing medical records of patients with whom they have no professional relationship
  - Do not look up a patient in the EMR unless you are caring for that patient!
What are some Common Breaches of Confidentiality?

• Loose talk with friends/family

• Faxing to wrong number

• Misplacing a flash drive

• Lost rounding sheets

• Talking to friends about patients

• Posting Facebook status about a patient

• Disclosing the identity of a celebrity patient

• Tossing PHI into the trash
Even the Trash is Private

- Trash cans can trap you into violating HIPAA. Patient information stored on paper or electronic storage media should never be thrown into an open trash can.

- Any paper containing PHI must be shredded or placed in a designated shred box.
Overheard Conversations

• On one side, you will be exposed to PHI including overhearing PHI as you do your day-to-day work. As long as you keep it to yourself, you have nothing to worry about.

• On the other side, you will be the one discussing PHI. Be aware of your surroundings and speak in a low tone.
Verifying Before You Send

Before disclosing PHI:

• Verify the identity of the individual before making a disclosure

• Call to verify a fax number before sending it.

• Use a cover sheet with preprinted confidentiality statement with the fax containing PHI.
Sanctions

• Covered entities (i.e., hospitals and clinics) are required by law to sanction students, staff, and faculty who violate HIPAA Privacy regulations.

• Disciplinary actions can include termination or dismissal from school
Sanctions

The Office of Civil Rights (OCR) may impose a penalty on a covered entity for failure to comply with HIPAA:

– $100 – to over $50,000 per violation

Criminal Penalties (to individual):

– Up to $50,000 and up to 1 year imprisonment
– Wrongful conduct $100,000 up to 5 years imprisonment
– Intent to sell, transfer, or use PHI for commercial advantage, personal gain or malicious harm is $250,000 up to 10 years imprisonment
THANK YOU:

We hope this module has been both informative and helpful.

Please feel free to review this information until you are confident about your knowledge of the material presented.

Complete & Submit the Supplemental HIPAA Module.