

Orientation to HIPAA For Students



What is HIPAA?

- The Health Insurance Portability and Accountability Act (HIPAA) affects three areas:
 - Insurance portability
 - Fraud enforcement
 - Administrative simplification



Insurance Portability

- Provides for continuity of coverage when individuals move from one health plan to another.
- Individuals cannot be denied coverage under pre-existing condition clauses.



Fraud Enforcement (Accountability)

- The Act sets standards and enforcement mechanisms to help reduce
 - fraud,
 - waste,
 - and abuse in health care.



Administrative Simplification (Reduction in Health Care Costs)

- Most significant portion of HIPAA
- Requires security and privacy for all forms of personally identifiable protected health information (PHI).
- A breach is punishable by law.



What is Protected Health Information (PHI)?

- Individually identifiable information
- Includes:
 - Name
 - Address
 - Employer
 - Relative's names
 - Birth date
 - Phone/fax numbers
 - Email address
 - Social Security #
 - Medical Record #
 - Member/Account #
 - Certificate #
 - Voiceprints
 - Fingerprints
 - Photos
 - Codes
 - Any other characteristics, such as occupation that can be used to identify an individual.



Why Health Privacy Matters

- Numerous uses of PHI
- PHI can be accessed by many
- Patient fear of misuse of PHI
- Fear magnified by increased use of technology such as identity theft



What is Confidentiality?

- An individual's right, within the law, to personal and informational privacy, including his or her health records
- The restriction of access to data and information
- Ensures information is only available for access with permission and on a need-to-know basis



Confidentiality Breach (violation of a law)

- Confidentiality is considered a contract ensuring the patient's medical privacy is protected
- Breaking the contract is considered a breach of contract (confidentiality)
 - Breach is unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of the information



Common Breaches of Confidentiality and Security

- “Elevator, Hallway, or Cafeteria Talk”
- Speaking loudly on the telephone to a patient when others can overhear
- Medical records/information placed in full view on desks or PC monitors
- Allowing unauthorized individuals into the department or work area



Common Breaches of Confidentiality and Security (cont)

- Allowing an individual to access a medical record without proper identification and authorization
- Sharing passwords or access codes
- Failing to log out of computer when leaving work area
- Faxing PHI to the wrong person, business, etc.



What Can We Do?

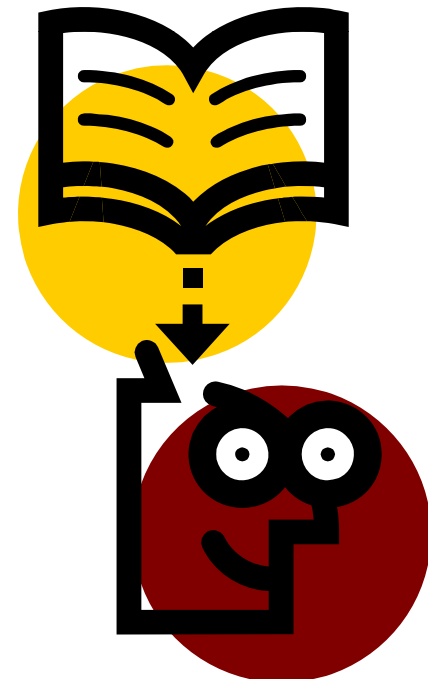
Protect and Prevent

- Be aware of confidentiality and security breaches at all times
- Report any breaches to your supervisor(s)
- Review, understand, and comply with Policy and Procedures pertaining to confidentiality and security of PHI
- Question individuals when they enter the department:
 - “May I help you with something?” Don’t be intimidated.



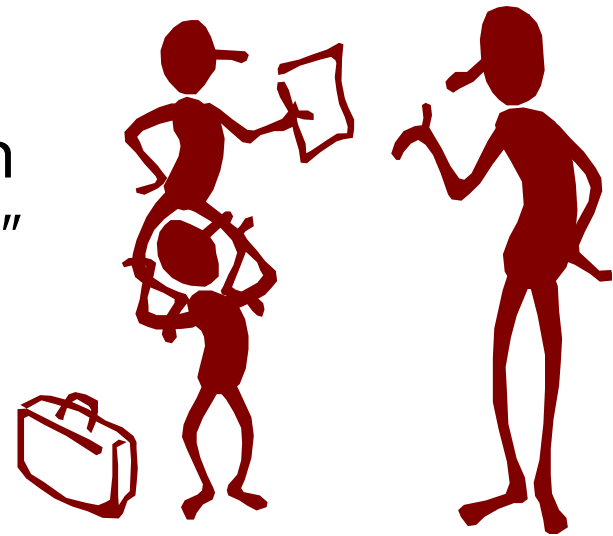
Protecting Patient Privacy

- Before looking/accessing patient health information always ask yourself, "Do I need to know this information to do my job?"
 - If the answer is "No," do not look at or access the information.



Protecting Patient Privacy

- Before telling/providing someone patient health information always ask yourself, "Do they need to know this information in order to do their job?"
 - If the answer is "No," do not tell that person the PHI.



Protecting Patient Privacy

- You will overhear PHI as you are working in the hospital, but all information must be kept to yourself.
- Even if you see an acquaintance in the hospital, you must not tell anyone else.



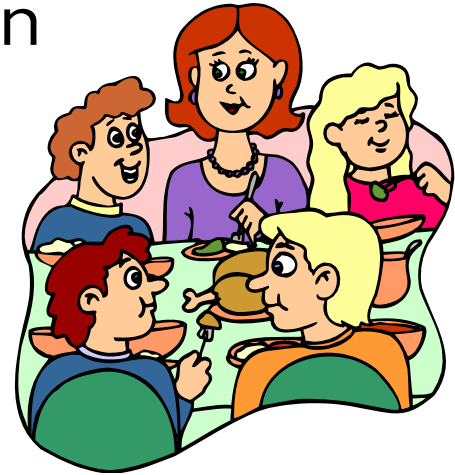
Protecting Patient Privacy

- Data/documents containing PHI should never be thrown into an open trash can. If you see this has happened, contact your supervisor.
- PHI (in paper form) that needs to be thrown away should be shredded immediately or thrown into a locked bin.



Prevent Privacy Violations

- You may be asked by family or friends to find out information on someone that has been a patient at the hospital –
 - You should not look for information or share any information you might already know.
 - Respond by telling the individual to contact the patient or the patient's family





Prevent Privacy Violations

- Nursing, allied health, and medical students may observe patient care with permission of the appropriate department designee.
 - Students are responsible for notifying their instructor and/or designee if they have been assigned to a patient who is a family member or known to the student.

Government Imposed Penalties for Patient Privacy and Security Violations

- Government actions against individuals who have breached confidentiality may include:
 - Civil or criminal sanctions
 - Civil penalties can result in a \$100 - \$50,000 fine per violation (dependent on the severity of the breach).
 - Criminal penalties can result in a fine from \$50,000 to \$250,000 and/or up to 10 years in prison.





Privacy/Security Violations by Students

- Students committing privacy and/or security violations are subject to termination of the clinical rotation experience in addition to government imposed civil or criminal penalties.

Reporting a Violation

- If you suspect or know of a HIPAA regulation violation, report this immediately to:

**SIH Privacy Officer, Marcia Matthias—
Ext 67122**

Or
Compliance Hotline
618-529-2540
or
1-800-965-4583



Reporting a Violation

- Reporting is:
 - Confidential
 - Protected against retaliation
 - The responsibility and duty of every employee when a violation has occurred.

