HIPAA Privacy Training

Two (2) parts of HIPAA covered in this presentation:

- **HIPAA Privacy** – Protection for the privacy of Protected Health Information (PHI) effective April 14, 2003 (including Standardization of electronic data interchange in health care transactions, effective October 2003)

- **HIPAA Security** – Protection for the security of electronic Protected Health Information (e-PHI) effective April 20, 2005

What is the difference between Privacy and Security?

- The **Privacy Rule** sets the standards for how covered entities and business associates are to maintain the privacy of Protected Health Information (PHI)
- The **Security Rule** defines the standards which require covered entities to implement basic safeguards to protect electronic Protected Health Information (e-PHI)

The HIPAA Training Program will help you to understand:

- What is HIPAA?
- Who has to follow the HIPAA law?
- When is the HIPAA implementation date?
- How does HIPAA affect you and your job?
- Why is HIPAA important?
- Where can you get answers to your questions about HIPAA?

What is HIPAA?

- HIPAA is the Health Insurance Portability and Accountability Act of 1996.
- HIPAA is a Federal Law.
- HIPAA is a response, by Congress, to healthcare reform.
- HIPAA affects the health care industry.
- HIPAA is mandatory.

HIPAA …

- Protects the privacy and security of a patient's health information.
- Provides for electronic and physical security of a patient's health information.
- Prevents health care fraud and abuse.
- Simplifies billing and other transactions, reducing health care administrative costs.

Who must follow the HIPAA Law?

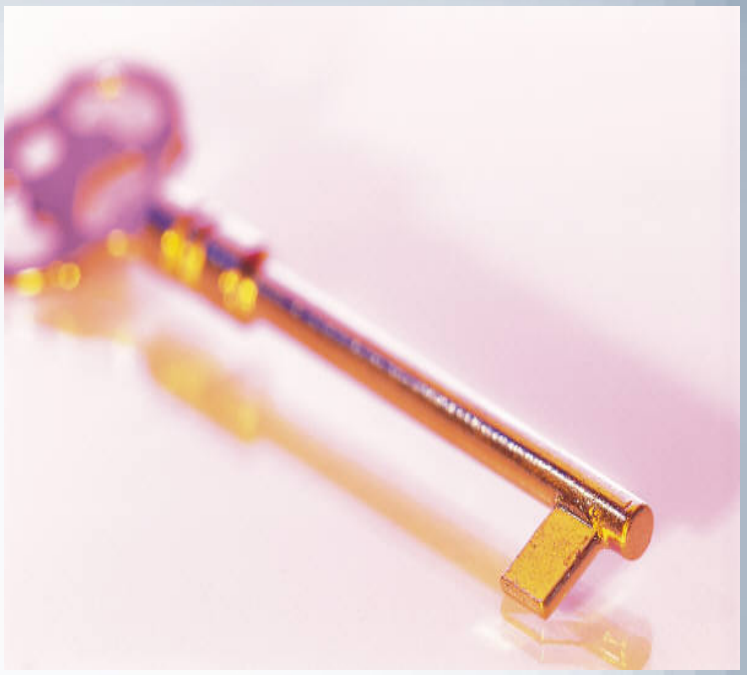
Covered Entities must follow the HIPAA Law.

Examples of Covered Entities

- Providers
- Health Plans
- Clearinghouses for Electronic Billing
- Business Associates (through contracts)

Covered Entity?

- The key is whether any of the Covered Transactions are performed electronically



Covered Entity…Always

Once you are part of a covered entity, you are a covered entity with respect to **all** Protected Health Information (PHI), whether it is transmitted electronically, in paper format, or transmitted orally.

Covered Transactions Consist of

- Enrollment and dis-enrollment
- Premium payments
- Eligibility
- Referral certification and authorization
- Health claims
- Health care payment and remittance advice

What Patient Information Must We Protect?

- Protected Health Information (PHI)
  - Relates to past, present, or future physical or mental condition of an individual; provisions of healthcare to an individual; or for payment of care provided to an individual.
  - Is transmitted or maintained in any form (electronic, paper, or oral representation).
  - Identifies, or can be used to identify the individual.

Examples of PHI
PHI = Health Information with Identifiers

- Name
- Address (including street, city, parish, zip code and equivalent geocodes)
- Name of employer
- Any date (birth, admit date, discharge date)
- Telephone and Fax numbers
- Electronic (email) addresses
- Social Security Number
- Medical Records

A Covered Entity…

…may not use or disclose an individual's protected health information, except as otherwise permitted, or required, by law.

But…

A Covered Entity MAY Use and Share a Patient's PHI for

- Treatment of the patient, including appointment reminders
- Payment of health care bills

And for…

- Business and management operations
- Disclosures required by law
- Public Health and other governmental reporting

"Treatment" Includes…

- Direct patient care
- Coordination of care
- Consultations
- Referrals to other health care providers

"Payment" Includes any activities required to bill and collect for health care services provided to patients.

"Health Care Operations" Includes business management and administrative activities, quality improvement, compliance, competency, and training.

A Covered Entity

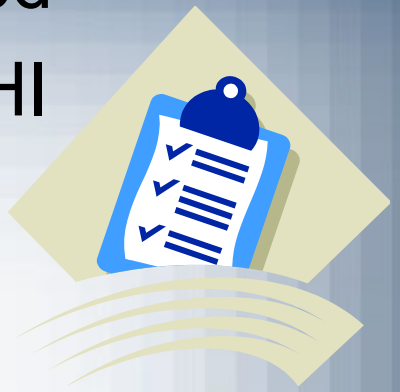
- Must use or share **only** the minimum amount of PHI necessary, **except** for requests made
  - for treatment of the patient
  - by the patient, or as requested by the patient to others
  - by the Secretary of the Department of Health & Human Services (DHHS)
  - as required by law
  - to complete standardized electronic transactions, as required by HIPAA

For many other uses and disclosures of PHI…

A Covered Entity must get a signed authorization from the patient (for example, to disclose PHI to a pharmaceutical company).

The Authorization MUST

- Describe the PHI to be used or released
- Identify who may use or release the PHI
- Identify who may receive the PHI
- Describe the purposes of the use or disclosure
- Identify when the authorization expires
- Be signed by the patient or someone making health care decisions (personal representative) for the patient (as per Policy GC-022)



HIPAA Requires

A Covered Entity to:

- Give each patient a Notice of Privacy Practices that describes:
  - how the facility can use and share his or her Protected Health Information (PHI)
  - a patient's privacy rights

and

- Request every patient to sign a written acknowledgement that he/she has received the Notice of Privacy Practices.

Patient Rights

- The right to **request restriction** of PHI uses & disclosures
- The right to **request alternative** forms of **communications** (mail to P.O. Box, not street address; no message on answering machine, etc.)
- The right to **access and copy patient's PHI**
- The right to an **accounting of the disclosures of PHI**
- The right to request **amendments to information**

How does HIPAA affect MY job?

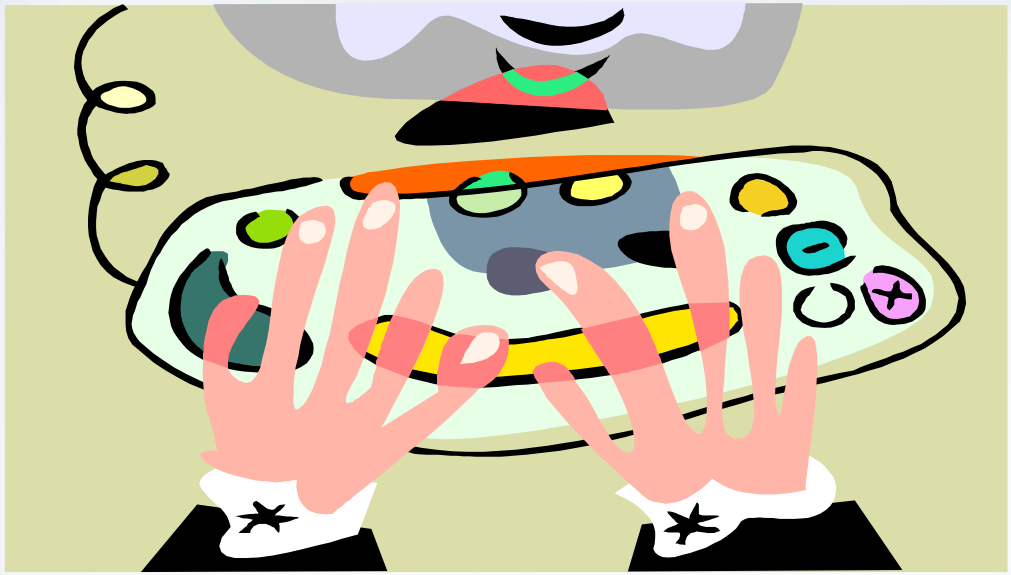
Well, if…

- You currently see, use, or share a person's PHI as a part of your job, HIPAA may change the way you do your job
- You currently work directly with patients, HIPAA may change the way you do your job

As part of your job, you must protect the privacy of the patient's PHI

When can you use PHI?

Only to do your job!



At all times…
Protect a patient's information as if it were your own!

- Look at a patient's PHI only if you need it to perform your job.
- Use a patient's PHI only if you need it to perform your job.
- Give a patient's PHI to others only when it's necessary for them to perform their jobs.
- Talk to others about a patient's PHI only if it is necessary to perform your job, and do it discreetly.

For Example…

1. You are a physician whose friend's wife is in a coma in the hospital after an accident. He asks you to review the admitting physician's orders and see if you concur. What can you legally do under HIPAA?
   A. You can look at her chart so you can answer your friend's questions about his wife's condition.
   B. You can ask the charge nurse on the floor to look into her records for you.
   C. You can tell your friend that you can only look at his wife's medical records if her physician, the patient, or in this case, the patient's representative, allows you to do so. Suggest that your friend ask to discuss her treatment and progress with the attending physician.

Answer:

C. Under HIPAA, you are only allowed to use information required to do your job. Since you are neither the attending physician nor part of the patient's 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 might not want your colleagues going through your own medical records, or those of your spouse or close friend.

Public Viewing / Hearing of PHI

- Refrain from discussing PHI in public areas, such as elevators and reception areas, unless doing so is necessary to provide treatment to one or more patients.
- Medical and support staff should take care of sharing PHI with family members, relatives, or personal representatives of patients. Information cannot be disclosed unless the patient has had an opportunity to agree with or object to the disclosure.
- Personal representatives are those individuals who, under Louisiana law, are able to make healthcare decisions on behalf of the patient.

For Example

Dr. Fortissimo was eating breakfast in the Med School Cafeteria one Monday morning, and talking on his cell phone to another doctor. During the conversation, he referred to the patient by name, and described her diagnosis. The cafeteria worker at the next table heard the call. 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 PHI was mentioned.

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 a more private location, or, at least, in a low voice that could not be overheard.

C. Other customers should not be allowed to eat in that section of the cafeteria so as 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 only have been discussed in a location that provided for the privacy of the information discussed.

Use and Disclosures of PHI for Research

- The I.R.B. (Institutional Review Board) may not authorize the use or disclosure of PHI for research purposes except:
  - For reviews preparatory to research;
  - For research on the protected health information of a decedent;
  - If the information is completely “de-identified”;
  - If the information is partially de-identified into a “limited data set” and the recipient of the information signs a data use agreement to protect the privacy of such information;

Why is protecting privacy and security important?

- We all want our privacy protected when we are patients – it's the right thing to do.
  - Don't be careless or negligent with PHI in **any** form.
- HIPAA and federal and state law require us to protect a patient's privacy.

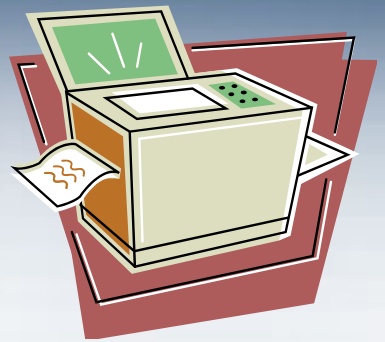
Penalties

are

- $100 per violation
- $25,000 for an identical violation within one year
- $50,000 for wrongful disclosure
- $100,000 and/or 5 years in prison for wrongful violation for obtaining PHI under false pretenses
- $250,000 and/or 10 years in prison if committed with intent to sell or transfer for commercial advantage, personal gain, or malicious harm, includes obtaining or disclosing.

Protecting Patient Privacy Requires Us to Secure Patient Information

Downloading/Copying/Removing



- Employees should not download, copy, or remove from the clinical areas any PHI, except as necessary to perform their jobs.
- *At SUNY New Paltz students are not allowed to remove any PHI from the clinical area.

Faxing

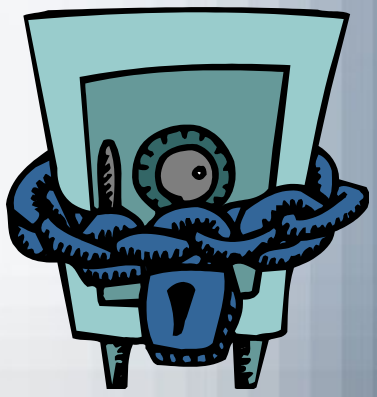
- Faxing is permitted. Always include, with the faxed information, a cover sheet containing a Confidentiality Statement:
  - The documents accompanying the transmission contain confidential privileged information. The recipient of this information is prohibited from disclosing the contents of the information to another party.
  - If you are neither the intended recipient, or the employee or agent responsible for delivery to the intended recipient, you are hereby notified that disclosure of contents in any manner is strictly prohibited. Please notify [name of sender] at [facility name] by calling [phone #] immediately if you received this information in error.

Information that should not be faxed (except in an emergency):

- Drug dependency
- Alcohol dependency
- Mental illness or psychological information
- Sexually-transmitted disease (STD) information
- HIV status

Locating a Fax Machine

- Location should be secure whenever possible,
- In an area that is not accessible to the public, and
- Whenever possible, in an area that requires security keys or badges for entry.



So, what *IS* "e-PHI"?

- **e-PHI** (electronic Protected Health Information) is computer-based patient health information that is **used, created, stored, received or transmitted** using any type of electronic information resource.

- Information in an electronic medical record, patient billing information transmitted to a payer, digital images and print outs, information when it is being sent to another provider, a payer or a researcher.

How do we protect e-PHI?

- Ensure the *confidentiality*, *integrity*, and *availability* of information through safeguards (Information Security)
- Ensure that the information will not be disclosed to unauthorized individuals or processes (**Confidentiality**)
- Ensure that the condition of information has not been altered or destroyed in an unauthorized manner, and data is accurately transferred from one system to another (**Integrity**)
- Ensure that information is accessible and usable upon demand by an authorized person (**Availability**)

Public Viewing/Hearing

- PHI should not be left in conference rooms, out on desks, or on counters where the information may be accessible to the public, or to other employees or individuals who do not have a need to know the protected health information.

Treat a Patient's Information as if it were your own …

Covered Entity Needs **Your** Help in Protecting Our Patients' Privacy.