HIPAA PRIVACY REGULATIONS

Objectives

- Develop a basic understanding of the HIPAA Privacy Regulations
- Understand the impact of the HIPAA Privacy Regulations in your workplace
- Understand ways to protect Patient Health Information
- Apply HIPAA Privacy Regulation requirements to your daily responsibilities

What is HIPAA? HIPAA is:

- The Health Insurance Portability and Accountability Act of 1996
- Complex federal law focused on the healthcare sector
- A response by Congress for healthcare reform
- A law that affects the entire healthcare industry
- A document that outlines civil and criminal penalties for failure to comply
- A civil rights law which gives the patient control over the use of their health information.
- Mandatory

#

Other Important Aspects of HIPAA Include:

- Every workforce member (including employees, volunteers physicians, students, and business associates) is required to ensure the privacy and security of our patients' protected health information (PHI).
- Electronic, written and oral communications containing PHI are protected by HIPAA.
- HIPAA allows us to use patient information for **T**reatment, **P**ayment or healthcare **O**perations (TPO) as defined by HIPAA and required by your job responsibilities.
- Patient approval is required before releasing information for all uses outside of treatment, payment or healthcare operations, with few exceptions.
- Workforce members should use only the minimum amount of patient information necessary to perform their jobs.
- All information that identifies an individual is consider confidential, including:
    - Nursing and physician notes
    - Billing information
    - Other treatment records

Definitions

Portability refers to the part of HIPAA that protects health insurance coverage for workers and their families when they change or lose their jobs.
Accountability refers to many other provisions including HIPAA's privacy regulation.

To Whom Does HIPAA Apply?

- Health Plans, includes health insurance companies
- Healthcare Clearinghouses, includes billing services
- Healthcare Providers, includes doctors, hospitals, laboratories, pharmacies, and

healthcare workers
- Under HIPAA these 3 groups are called Covered Entities

Why is Privacy So Important?

Everyone, especially health care professionals, wants to maintain the privacy of personal information, particularly when it comes to sensitive health care information in electronic form. Although health data is usually stored electronically, your role in maintaining privacy has more to do with how you handle and protect each patient's personal information, rather than with your knowledge of the technical aspects of computers and databases.

Importance of Privacy – An Example:

Laboratory workers frequently encounter situations that could result in a breach of privacy. Here is an example:

> A hospital phlebotomist is asked by her best friend to look up her mother's laboratory results because she didn't understand the test results. The phlebotomist used her access to the hospital information system to get the results. Did the phlebotomist violate HIPAA?

Yes, this is a privacy breach. The phlebotomist's job description doesn't include releasing PHI to anyone other than healthcare providers involved in the care of the patient. She disclosed PHI to a family member without authorization. The mother may not have wanted or authorized her daughter to view her lab results. This phlebotomist would require retraining about the hospital's privacy policies and procedures. She could also be subject to disciplinary action.#

HIPAA Privacy Regulation

- Became law April 14, 2003
- Protects the confidentiality of individual's health data by:
  - Regulating how Protected Health Information (PHI) is used
  - To whom PHI is disclosed, and
  - How and where PHI is maintained
- Requires reasonable security measures to protect individuals' health information
- Establishes accountability for use/release of information
- Gives individuals rights regarding their health information

Consequences of Non-Compliance

The penalties for privacy violations are substantial for both the organization and the individual responsible for the breach. Civil penalties are established on a tier structure based on the level of severity and the intent of the violations. Privacy violations resulting from a lack of appropriate policies, procedure or practices could result in a civil fine of $100 per violation, up to a maximum of $250,000 per year. Criminal penalties for obtaining or using PHI with the intent to sell or use it for personal gain or malicious harm could result in fines up to $250,000 and 10 years in jail. The Office for Civil Rights may also refer breach cases to the state's Attorney General for criminal penalties.

What Information is Protected?

HIPAA protects all health information which:

- Is about an individual, regardless of its form (i.e., oral, paper or electronic)
- Identifies an individual or can be used to identify an individual
- Is related to an individual's past, present or future physical or mental condition, healthcare provided, or payment for the provision of healthcare

This is called **P**rotected **H**ealth **I**nformation or PHI

What Information Can Be Used to Identify an Individual Patient?

PHI is any piece of information that can identify an individual used alone or in combination with other information, including:

- Name
- Address including street, city county, zip code, and equivalent geocodes
- Names of relatives
- Name of employers
- Birth date
- Telephone numbers
- Fax numbers
- Electronic e-mail addresses
- Social Security number
- Medical Records number
- Health Plan Beneficiary number
- Account number
- Certificate/license number
- Any vehicle or other device serial number
- Web Universal Resource Locator (URL)
- Internet Protocol (IP) address number
- Finger or voice prints
- Photographic images
- Any other unique identifying number, character, or code

Scope of the Privacy Regulation

- Limits the use and disclosure of PHI
- Limits who can request PHI
- Provides criteria for de-identifying information
- Sets out administrative requirements
- Establishes mechanisms for reporting violations, includes whistleblower provisions and external complaint processes
- Establishes rights of the individual

Rights of the Individual

- Right of notice: Individuals have the right to know how their PHI will be used, collected, and to whom it may be disclosed
- Right of access: Individuals may access their own PHI upon request
- Right to accounting of disclosures: Individuals have a right to an accounting of disclosures of PHI
- Right to amend: Individuals may request a change to their PHI
- Right to request restrictions: Individuals may request that all or part of their PHI be withheld from specific parties
- Right to confidential communication: Individuals have a right to request and receive communications confidentially
- Right to file a complaint for privacy policy violation issues
- Individuals may have additional rights under state law

Administrative Requirement

- Each covered entity must designate a Facility Privacy Officer who:
    - Oversees and implements the privacy program
    - Works to ensure the facility's compliance of the HIPAA Standards for Privacy of Individually Identifiable Health Information
    - Is responsible for receiving complaints about matters of patient privacy
- All staff must participate in appropriate HIPAA training
- Safeguards must be in place to protect PHI
- Covered entities must implement policies and procedures to comply with the privacy regulations
- There must be a process to handle complaints from individuals about the way their PHI is handled
- There must be a policy in place to discipline employees who fail to comply with privacy policies

#

Safeguards

Reasonable safeguards must be in place to protect individually identifiable information, including PHI from loss, defacement and tampering and to ensure the confidentiality of information. Additionally, each healthcare facility will make certain appropriate administrative, technical and physical safeguards are established:

- To ensure the security and confidentiality of individually identifiable information and records including PHI and records
- To protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.

Physical Safeguard Examples

- Controlling building access with photo-identification/swipe card system
- Keeping offices and file cabinets containing PHI locked
- Turning computer screens displaying PHI away from public view

Administrative Safeguard Examples

- Policies and procedures
- Staff training programs
- Auditing and monitoring compliance with policies and procedures
- Employee confidentiality agreements

Technical Safeguard Examples

- Features are in place which track and audit all electronic information systems access for appropriate usage
- Automatic log-off from the information system after a specified time interval
- Unique user identification with log-on and passwords

Safeguarding – An Example

Betty is going on vacation and has a critical computer report that must be run on her computer. Betty gives Donna her user id and password so that Donna can run the report while Betty is out. Did Betty do the right thing to make sure the critical report is run?

No, your user id and password are unique to you and as such are traceable back to you. When you allow someone else to use your user id and password, in the event of a confidentiality breach, the burden of proof is on you to prove that you were not using your ID. Betty should have asked the Information Systems department to assist in setting Donna up with access to run the report while she was gone.

Protecting Patient Privacy

- Access, use or disclose only the minimum information necessary to perform your designated role
- Do not share confidential information (PHI) with others unless the individuals have the **need to know** this information (i.e., necessary to their position and related to treatment) and have agreed to maintain the confidentiality of the information.
- **Always** dispose of any piece of paper that contains individually identifiable health information in appropriate receptacles. The paper must be handled securely and destroyed by shredding or placing it into the department/units designated recycle bin.
- **Never** print or remove individually identifiable information from the facility without proper authorization.
- **Never** leave PHI where it is accessible to unauthorized persons.
- Ensure that safeguards are in place to protect patient information on medical records maintained at the patient's bedside, outside the room or anywhere else in the facility.
- **Never** give your computer user password or allow it to be used by anyone else. When you have finished always log off of the terminal.
- Install screen savers on PCs whenever possible.
- Position computer screens so PHI is not readable by the public or other unauthorized viewers.

- Position printers, fax and copy machines in protected locations so that printed information is not accessible or viewable by an unauthorized person.
- **Never** discuss PHI in hallways, elevators, cafeterias, etc.
- If reasonable precautions (lowering of voices) are taken to minimize inadvertent disclosures to others, you may:
  - Orally communicate at the nursing or work station
  - Discuss a patient's treatment with other healthcare professionals in a joint treatment area
  - Discuss a patient's condition during training rounds
  - Discuss a patient's condition during pre- and post-conferences

Protecting Patient Privacy – An Example

An adult daughter of an elderly patient is present in the room when his doctor enters to speak with the patient about test results. The patient introduces his daughter to the doctor and then asks the doctor if the test results are back. The doctor begins to explain the results to the patient. Did the doctor violate the patient's privacy by talking about the test results with the daughter present in the room?

No, since the patient asked about the results with his daughter in the room, the doctor can assume that it is appropriate to share the results at that time.

Use the "Minimum Necessary"

All workforce members must limit the amount of patient information to the minimum necessary to accomplish the "intended" work purpose.
Ask yourself the following question before looking at medical records, test results or any other patient information. ***"Do I need to know this information to do my job?"***
Requestors should only receive the requested information.
Do not provide the entire chart or file unless there are valid reasons for the requestor to receive all dates of service.

Notifications

Covered entities are required to provide individuals with a NOTICE OF PRIVACY PRACTICES and have the individual sign an acknowledgement form confirming receipt of the notice.
The purpose of the Notice is to enable an individual to understand what happens to their PHI. The Notice tells individuals why their PHI is needed and how it is being used. The notice should state what information is being collected, how it is being used, disclosed stored, and who to contact with questions or complaints.
It is essential that covered entities faithfully adhere to their own Notice of Privacy Practices.

Authorizations

The privacy regulations give covered entities permission to use and disclose PHI for treatment, payment and health care operations (TPO), without obtaining specific authorization.
A covered entity may disclose PHI to other covered entities, such as another provider, reference laboratories and homecare services, which are providing services to the primary

covered entity.
The service that the other covered entity is providing must fall within TPO.
If the service being provided does not fall within TPO, an authorization from the patient or legal guardian is generally required.
A valid authorization form must state the specific disclosures of PHI to be made, what the information will be used for, and must be signed and dated by the patient.
#

Limiting Use and Disclosure of PHI

A covered entity may use or disclose PHI without getting an individual's authorization in order to:

- Perform and report the requested tests
- Bill for the services performed
- Perform essential functions, including quality assessment, accreditation, and compliance
- Meet legal reporting requirements, including those mandated by public health departments, workers' compensation, law enforcement agencies and the US Department of Health and Human Services

Any uses or disclosures other than those listed above require a written authorization.

Disclosure

The regulation recognizes that there are situations where all of a patient's PHI can be released. These are:

- When releasing PHI to another covered entity for treatment, payment or other healthcare operations, such as quality assessment
- When releasing an individual's PHI to himself or herself or their personal representative
- When an individual has signed an authorization to release the PHI
- When required to do so by law

Business Associate Agreement

A Business Associate is a person or organization, which is not part of the workforce of a covered entity, which is providing services to the covered entity that requires the exchange of PHI.
A legal agreement must be in place between covered entities and their business associates.
This agreement defines the business rules that will be put into effect to ensure the privacy and security of PHI.

Examples of business associates of covered entities if they will require access to PHI may include collection agencies, attorneys, consultants and accountants.
Business associate agreements are not generally required between two covered entities involved in treatment, payment or health care operations.

De-Identified PHI and Limited Data Sets for Research

- Health information is considered de-identified if it cannot be used to identify an individual. Other terms for de-identification are:
    - Anonymous

    - Aggregated
    - Scrubbed
- The Privacy Regulation details the specific information about the individual, which needs to be removed for it to qualify as de-identified.
- When PHI is de-identified it is no longer considered protected.
- Covered entities should try to use de-identified health information whenever possible
- The Regulations do not allow recombining of various portions of de-identified information to re-identify an individual.
- Completely de-identified health information may lose much of its value for research and public health investigations. Thus, the regulations allow for the use of limited data sets for these purposes. These limited data sets are stripped of direct identifiers such as name and street address, but still contain enough individual data to be useful for research and public health investigations.

Summary

- **All** health information that specifically identifies an individual is considered confidential
- Protecting the privacy of patient information is everyone's responsibility
- You are an active part of this privacy program as you use patient information only to perform your job
- Don't intentionally or unintentionally disclose patient information
- Follow proper security guidelines, including log on and password protection; if in doubt, ask the your instructor.
- Accessing patient information without a job-related need to do so is a violation of HIPAA and policy
- HIPAA only allows us to use and disclose PHI for treatment, payment and health care operations - all other disclosures require patient authorization
- It is inappropriate and prohibited to access your own or anyone else's medical record or billing information unless you have a HIPAA recognized purpose (TPO)
- Notify your instructor immediately of any suspected privacy violations or concerns

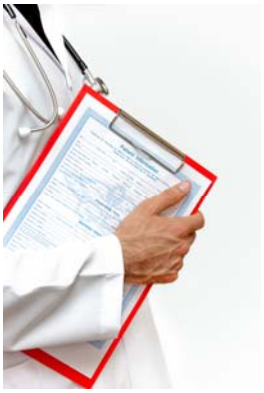
Suggested Photos:













#