

HIPAA TRAINING

West Liberty University
Health Sciences



HISTORY

- HIPAA stands for “Health Insurance Portability and Accountability Act of 1996”
- HIPAA was passed in 1996 as part of a broad congressional attempt at healthcare reform
- This training will address Title II of the Act-Administrative Simplification



PURPOSE

- To increase the efficiency and effectiveness of the health care system through standardization
- To enhance the security and privacy of Protected Health Information (PHI)
- According to the Department of Health and Human Services 1 in 6 patients omit sensitive information when discussing medical history with their physician out of fear of misuse or mishandling.



COMPONENTS

- PRIVACY STANDARDS – April 14, 2003
- Electronic Transactions Standards – Oct 16, 2003
- Security Standards – April 20, 2005
- This training will focus on the Privacy Standards



HIPAA APPLIES TO COVERED ENTITIES

- Hospitals
- Physicians
- Home Health Agencies
- Pharmacy
- Dentists
- Durable Medical Equipment Companies
- Health Plans



PRIVACY STANDARDS

KEY FEATURES

- Protected Health Information (PHI)
- Uses & Disclosures
- Authorization
- Notice of Privacy Practices
- Minimum Necessary
- Patient Rights
- Penalties



PENALTIES

WHY YOU WANT TO READ THIS
PRESENTATION

CIVIL PENALTIES

- \$100 per violation per person up to a maximum of \$25,000 per person per year per standard violation
- These penalties can be assessed against individual employees

CRIMINAL PENALTIES

- Up to \$50,000, 1 year in prison, or both, for inappropriate use of PHI
- Up to \$100,000, 5 years in prison, or both for using PHI under false pretenses
- Up to \$250,000, 10 years in prison or both, for the intent to sell or use PHI for commercial advantage, personal gain, or malicious harm
- These penalties can be assessed against individual employees

PRIVACY RULE

- Regulates the internal use and external disclosure of protected health information (PHI) by organizations and their employees
- For example, PHI cannot be discussed in places like elevators, hallways, the cafeteria, or the smoking areas

EXAMPLE VIOLATION

A nurse sees an acquaintance has checked into the hospital and discovers he is scheduled for surgery. She calls a few of his friends to make sure they are aware of this, thinking they can wish him well or be of some assistance to his family.

WHAT IS PHI?

Personal Health Information

- Oral, written, and electronic communication
- Health and demographic information about an individual that is transmitted or maintained in any form where the information is created or received by a health care provider, health plan, employer or health care clearinghouse
- Includes past, present, and future health information



EXAMPLES OF PHI

- Name
- Address
- Birthdate
- Admission date
- Discharge date
- Date of death
- Telephone numbers
- Fax number
- E-mail address
- Social Security #
- Medical record #
- Account #
- Certificate/license #
- Photographs
- **All clinical data**

PERMITTED USES & DISCLOSURES

- Treatment
- Payment
- Health Care Operations

These are referred to as: “TPO”

OTHER USES & DISCLOSURES

- Some disclosures are mandated by law such as health oversight activities, public health concerns, FDA etc
- ALL OTHER USES OR DISCLOSURES OUTSIDE OF TPO REQUIRE AN AUTHORIZATION

TREATMENT

(Examples)

- To a consulting physician
- To a post discharge provider such as, a rehab unit, skilled unit, or home health agency
- To another department within the hospital

PAYMENT

(Examples)

- Medicare/Medicaid
- Insurance Companies
- Workers' Compensation
- Liability Carrier
- Provision of billing information to a physician who treated the patient at the hospital
- To the billing companies for the emergency room physicians or radiologists

HEALTHCARE OPERATIONS

(Examples)

- Quality assessment and improvement
- Peer review and credentialing activities
- Legal services
- Auditing services
- Business planning and development

AUTHORIZATION

- Authorization must be obtained for ALL uses and disclosures other than TPO or those mandated under law.
- Authorizations must include:
 - Description of the information
 - Name of person/entity to release to
 - Expiration date
 - Information regarding right to revoke
 - Date and signature

PRIVACY NOTICE

- Every patient must receive a copy of the healthcare provider's or institution's privacy notice the first time they receive services (Starting: April 14, 2003)
- The notice must be posted in areas easily seen by patients
- The notice must be posted on the official website

PRIVACY NOTICE REQUIREMENTS

- Be in plain language
- Contain a description and example of TPO
- Contain a description and example of other uses and disclosures not requiring Authorization
- Include statements about an individual's rights
- Include statements about the duties of the provider
- Describe the complaint process

MINIMUM NECESSARY

The privacy rule requires covered entities to use or disclose only the “**minimum necessary**” PHI to accomplish the intended purpose of the use, disclosure, or request



INTERNAL REQUIREMENTS

- Identify workforce who need access to PHI
- For each job code, limit access based on a need-to-know basis
- Employees of the healthcare service are obligated to use the access they have available to only perform their job duties.

EXTERNAL REQUIREMENTS

- Limit access to what is needed to accomplish the purpose for which the request was made
- Do not send a requestor an entire medical record if they ask for insurance information or a particular lab result

EXAMPLE VIOLATION

- You go to lunch with your friend from another department. At lunch your friend says, “ We have really been busy this morning. Dr. Right saw 20 patients this morning”. You ask if Edward Stellin is Dr. Right’s patient and your friend replies, “yes, didn’t you know he had a cholecystectomy?”

PATIENT RIGHTS

- Receive written notice of privacy practices
- Request restrictions on uses & disclosures
- Access, inspect & copy their PHI
- Request amendment or correction of their PHI
- Receive an accounting of disclosures of their PHI
- Request confidential communications

CONFIDENTIAL COMMUNICATIONS

- A patient has a right under HIPAA to request alternate methods of communication
- The hospital must honor those requests if they are reasonable

RIGHT TO INSPECT AND COPY

- Patients have the right to inspect and copy their medical information
- This includes medical and billing records, but excludes psychotherapy notes

RIGHT TO AMEND

- Patients have a right to request an amendment to their record as long as the information is kept by the hospital
- Any requests for amendments must be in writing and submitted to Medical Records
- Hospital may deny the request to amend the information

DENY REQUEST TO AMEND

- If the request is not in writing
- If the portion of the record was not created by that Institution or healthcare service originally
- If the original record is accurate and complete

RIGHT TO REQUEST RESTRICTIONS

- Patients have a right to request a restriction or limitation on the medical information the hospital uses or discloses about them for TPO
- Hospital is not required to agree to the restriction
- If hospital does agree to the restriction, they must comply with the restriction unless the information is needed to provide the patient with emergency treatment

ACCOUNTING FOR DISCLOSURES

- Under HIPAA, patients have a right to request an accounting of all disclosures we have made of their PHI
- We do not have to list those for TPO
- We must track all others disclosures
- We do have to disclose any inappropriate disclosures

INAPPROPRIATE DISCLOSURES

- If results are reported to a physician who is not that patient's physician
- If information is faxed to the wrong fax number
- If we discover through an audit that inappropriate access has occurred
- If information is left unattended and unauthorized personnel review it

EXAMPLE VIOLATION

- There are 2 doctors with the same name – Dr. Julius **H.** Wrong and Dr. Julius **W.** Wrong. Patient of Dr. Julius **H.** Wrong presents for lab testing and he is incorrectly registered to Dr. Julius **W.** Wrong. Lab reports results to Dr. Julius **W.** Wrong instead of Dr. Julius **H.** Wrong.

REPORTING INAPPROPRIATE DISCLOSURES

- All inappropriate disclosures must be reported to the Privacy Officer
- It will be the responsibility of the Privacy Officer to log all inappropriate disclosures
- Inappropriate disclosures will be tracked by employee and appropriate disciplinary action will be taken

HOSPITAL REQUIREMENTS

- Designate a privacy officer with primary responsibility for ensuring compliance with the regulations
- Establish training programs for all members of the workforce
- Implement appropriate policies & procedures to prevent intentional and accidental disclosures of PHI

HOSPITAL REQUIREMENTS

- Establish a system for receiving and responding to complaints regarding privacy practices
- Implement appropriate discipline for violations of the privacy guidelines
- Make reasonable efforts to limit information to the minimum necessary to accomplish a person's job

EMPLOYEE OBLIGATIONS

- Report any inappropriate disclosures or breaches of patient confidentiality to the Privacy Officer
- Sign a confidentiality statement annually
- Keep patient PHI confidential at all times
- Access information on a “need to know” basis

ENFORCEMENT

- THE PUBLIC – The public will be educated about their privacy rights and will not tolerate violations to their privacy.
- OFFICE OF CIVIL RIGHTS – They will provide guidance and monitor compliance.
- DEPARTMENT OF JUSTICE – They will be involved in criminal and privacy violations.

Additional Tips

- Accessing information
- Faxing information
- Practical information

ACCESSING RECORDS

- Records of patients should only be accessed if you have a reason to do so to perform your job duties
- You do not have the authority to access any other record just because you have the computer access. In other words, if you have access to PCI, you cannot look up your father-in-law's records unless you need to do so to perform your job duties
- All access is monitored and audit trails do exist
- Employees have been terminated based on those audit trails

ACCESSING RECORDS

- Very important to sign off the computer when you walk away from it so others can't use your password for inappropriate access
- Any access under your password is considered yours
- If you feel someone else has your password, contact Information Systems to have it changed
- Do not share your password with anyone

ACCESSING RECORDS

- We are no longer allowing employees access to their own record or the records of their children
- Must now go through the same process as any other patient
- Will be required to go to Medical Records to obtain records
- Some records of your child are now protected under the law and even a parent does not have access. Examples include, certain psych records and HIV testing

FAXING PHI

- Whenever you are faxing PHI outside of the facility, a cover sheet must be used
- Use a cover sheet when faxing within the facility when the fax is directed towards a specific employee
- The cover sheet must be the OVHS&E cover sheet which includes appropriate HIPAA language
- Do not use any unauthorized cover sheets

FAXING PHI

- When faxing, double check the number entered prior to sending the fax
- If you realize you have faxed to the wrong number contact them immediately and retrieve the information sent

FAXING

- Fax records only when it is absolutely necessary for the further treatment of the patient
- Fax only those records that must get there immediately

OTHER STEPS TO PROTECT THE PRIVACY OF OUR PATIENTS

- Do not leave the records of patients laying around in unsupervised areas
- If you print PHI out destroy it immediately after you are done with it
- If you take copies of PHI to a meeting and pass them out make sure you collect all copies at the end of the meeting and discard them appropriately
- Any copies of PHI should be shredded

PRACTICAL STEPS

- Dictation and phone calls should occur in private areas
- Cell phones should only be used in emergency situations and must be used in private areas
- Conversations among employees regarding patients must occur in private areas

PRACTICAL STEPS

- Close exam room doors whenever you are reviewing information with the patient or when you are performing a test or procedure
- Use common sense – if the roles were reversed would you feel that your privacy was being adequately protected

MESSAGES

- If you call a patient and must leave a message, leave the minimum amount of information possible
- For example, “This call is for Lee Smith, please call the Admitting Office at “
- If you call someone and receive another member of the household do not answer any questions such as, what test are they having done or what is wrong with them etc.

NEED TO KNOW

- Information regarding a patient should only be given to employees who have a need to know
- OR Schedules, Admission lists etc are only intended for those who need that information to perform their job duties
- As employees we are not automatically entitled to information

HOW TO REPORT

- Inappropriate disclosures or breaches of patient confidentiality should be reported to one of the following:

Privacy Officer

Department Manager

Compliance Hotline (8181)

HIPAA GOLDEN RULE

MAINTAIN PATIENT INFORMATION IN
THE SAME MANNER YOU WOULD
WANT SOMEONE TO MAINTAIN YOUR
PATIENT INFORMATION

FINAL THOUGHTS

- REMEMBER – A Breach of confidentiality can be costly to the organization and to you personally
- WILL RESULT IN DISCIPLINARY ACTION – MOST LIKELY TERMINATION OF EMPLOYMENT

- Print the next slide: quiz
- Complete the quiz
- Return the quiz to your clinical instructor/supervisor

Quiz: HIPAA

Name: _____

Date: _____

- True or False 1. HIPAA stands for Health Insurance Protection, Action, and Accountability.
- True or False 2. One purpose of HIPAA is to enhance the security and privacy of Protected Health Information (PHI).
- True or False 3. The Privacy Standards component went into effect in 2008.
- True or False 4. HIPAA applies to hospitals, pharmacies, health plans, and home health agencies, but NOT to physicians.
- True or False 5. Discussing Protected Health Information (PHI) in the cafeteria over lunch is a violation of the Privacy Rule.
- True or False 6. PHI includes any personal information about past, present, or future health information in oral, written, or electronic communications.
- True or False 7. PHI includes ONLY clinical data, it DOES NOT include admission, discharge, or death dates.
- True or False 8. Disclosure of PHI is permitted for Treatment, Payment, or Health Care Operations (TPO) purposes.
- True or False 9. Patient authorization MUST be obtained for ALL uses and disclosures of PHI INCLUDING TPO and those mandated under law.
- True or False 10. The patient has the right to inspect and copy their medical information excluding psychotherapy notes.

SCORE: _____