Health Insurance Portability and Accountability Act **(HIPAA)**

A Common Sense Approach to the Privacy and Security Rule

TRAINING MODULE I

HIPAA: Overview

In 1996 President Clinton signed the Health Insurance Portability and Accountability Act (HIPAA). This law ensures the continuation of healthcare coverage for individuals as they change jobs or become unemployed. However, in order to continue healthcare coverage health information must be moved; and to make it easier among providers to share information, the law seeks to simplify the administration of health insurance by requiring that common transactions, such as submitting a claim on the patient's behalf, be in a standard format for all healthcare organizations and payers. But, as health information becomes easier to share, it also becomes easier for information leaks and abuses, especially when sharing by electronic means. Therefore, the HIPAA law also aims towards combating waste, fraud, and abuse in health insurance and healthcare.

HIPAA: Definitions

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of information outside the UABHS operating entity holding the information.

Protected Health Information (PHI): Individually identifiable health information. This is information that is a subset of health information including demographic information collected from an individual such as name, address, age, race, date of birth, and is created or received by a health care provider, health plan, employer, or health care clearinghouse, and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care, or payment for the provision of health care to an individual.

Healthcare Operations: Conducting quality assessment and improvement activities; credentialing, competency and training evaluation activities; underwriting, premium rating and other activities relating to provider contracts; conducting compliance, medical review, legal services and auditing functions; business planning and development; and business management and general administrative activities, including but not limited to customer service, resolution of internal grievances, and due diligence.

HIPAA: Privacy

Protecting patient's privacy with confidentiality

HIPAA privacy standards go in to effect on April 14, 2003. The purpose of these standards is to establish a uniform way for protecting the privacy of patient information. The methods used to establish this uniformity are (1) use and disclosure standards and (2) patient rights. These standards will give patients the right to adequate notice of the uses and disclosures of their protected health information and control of who will see their protected health information. As well as, establish their right to notice of their rights and the covered entities (health care provider, health plan, health care clearinghouse) duties in relation to the information. These standards will also limit covered entities communications with or about patients involving protected health information to those who need the information in order to provide treatment, payment, and health care operations. Such communications will involve verbal discussions, written communications and electronic communications. Only those people and computer process with an authorized **need-to-know** will have access to the protected information.

Fines and Penalties for Non-Compliance

The Office of Civil Rights of the U.S. Department of Health and Human Services (DHHS) is responsible for overseeing HIPAA Compliance.

$ **Civil Penalties** are fines of up to $100 for each "inadvertent violation" of the law per person, up to a limit of $25,000 for violating each identical requirement or prohibition. For instance, if a hospital released 100 patient records illegally, it could be fined $100 for each record, for a total of $10,000.

Criminal Penalties for "wrongful disclosure" can include both large fines and JAIL TIME. These penalties can be as high as a $250,000 fine or prison sentences of up to 10 years. For example:

- Gaining access to health information under false pretenses
- Releasing patient information with harmful intent or selling the information

Why Does this Affect You?

You are a "**Covered Entity**" and must comply with HIPAA because you are either a:

- ❖ Healthcare Provider (University Hospital, TKC, CEFH, physicians and others who electronically bill for services).
- Clearinghouse (processes nonstandard data elements of health information into standard data elements).
- Health Plan that provides or pays the cost of medical care (VIVA Health).

I. Uses and Disclosures

General Rule

Protected Health Information (PHI) must be used and disclosed only as permitted by HIPAA.

Minimum Necessary Standard

When HIPAA permits use or disclosure of PHI, providers should disclose or use only the minimum amount of PHI needed in order to do their jobs. However there are some exceptions, minimum necessary does not apply to:

- Releases to or requests by a health care provider for treatment
- Anything for which a patient authorization is signed
- Disclosures required by law
- Incidental uses or disclosures (ex. Using sign-in sheets in waiting rooms, and engaging in confidential conversations that are overheard by others, despite reasonable measures to prevent such disclosures)

Treatment, Payment, and Healthcare Operations (TPO)

Protected Health Information may be:

- Used for TPO
- Disclosed to other providers for treatment
- Disclosed to other covered entities for payment
- Disclosed to other covered entities that have a relationship with the patient for certain healthcare operations such as quality improvement, credentialing and compliance.

Psychotherapy Notes

Psychotherapy notes may not be used or disclosed unless the patient signs an authorization.

What are psychotherapy notes?

Psychotherapy notes are notes that the mental health professional writes (in essence the therapist's impressions about the patient) in order to document or analyze the contents of conversation during a private, group, joint, or family counseling session.

Psychotherapy notes do not include "summary information" such as chart notes; medical notes; progress notes; treatment summaries; symptoms; summary of theme of psychotherapy session; diagnosis; and medications prescribed and their side effects.

Psychotherapy notes must be kept separate from the patient's medical record.

Absent an authorization, only the originator of the notes may use them for treatment.

Uses & Disclosures without an Authorization

PHI may be used or disclosed without an authorization under the following circumstances:

- Public health agencies for purposes such as controlling or preventing disease or collecting vital statistics
- Public health or government authorities for law enforcement purposes, such as reporting on victims of abuse, neglect or domestic violence
- Health oversight agencies for activities authorized by law
- Judicial and administrative proceedings, such as compliance with a court order or subpoena
- Law enforcement officials seeking information for the purpose of identifying a suspect, witness, or victim of a crime
- Coroners, medical examiners, and funeral directors to identify a deceased person or determine a cause of death
- Organ donation
- Worker's compensation

Research

Covered entities are permitted to use or disclose PHI for research if the Institutional Review Board (IRB) has approved the research and one or more of the following conditions exist:

1. Patient Authorization
2. Decedent Research
3. Preparatory Research
4. Limited Data Set
5. IRB grants a waiver of required authorization

Other Uses & Disclosures

Facility Directories, unless patient opts out, may disclose a patient's name, location and general medical condition to those asking for the patient by name

Protected Health Information may be disclosed to individuals involved in the care or payment for care unless the patient objects

Marketing and Fundraising

Covered entities are prohibited from:

- Using or disclosing PHI for marketing purposes without the patient's expressed authorization
- Selling patient/enrollee lists to third parties

However, providers can communicate with patients about treatment options or the covered entities own health-related products and services, and common health care communications such as; disease management, wellness programs, prescription refill reminders and appointment notifications, recommending alternative treatments, therapies, or health care products

Limited protected health information may be used for fundraising if the patient gives instruction on how to opt out

II. Patient Rights

Patients have the right to:

- A Notice of Health Information Practices
- Request Access to their PHI
- Request Accounting for Use and Disclosures
- Request Amendment and Correction (subject to approval by the covered entity)
- Request Confidential/Alternate communication
- Request Restriction on use of PHI (subject to approval by the covered entity)
- File Complaints

III. Required Business Documents

Under HIPAA law, covered entities are required to have the following business documents:

1. Notice of Privacy Practices
2. Authorization Form
3. Accounting for Disclosures
4. Business Associate Agreements

Notice of Privacy Practices

- This document gives patient's notice of their rights with respect to PHI and Privacy practices of covered entities
- It requires providers to make good faith efforts to obtain the patient's written acknowledgement at the time of receipt of the Notice of Privacy Practices, except in emergency circumstances.

Each patient must receive a **Notice of Privacy Practices** prior to the initial visit on or after April 14, 2003. UAB Health System's is titled *Notice of Health Information Practices*

Authorization Form

This document is required for all uses and disclosures not otherwise permitted by HIPAA

Accounting for Disclosures

This document is a record of disclosures for the past 6 years

No record is required for treatment, payment, healthcare operations, authorizations nor incidental disclosures

Business Associate Agreements

This document binds subcontractors who use PHI to the HIPAA Privacy standards

IV. HIPAA Privacy Policies

Under HIPAA law, covered entities are required to develop and implement policies for the following:

- Use and disclosure of Health Information which includes;
  - Authorization Form
  - Notice of Information Practices
  - Business Associate Agreement
- Use and Disclosure of Health Information for Marketing
- Use and Disclosure of Health Information for Research
- Patient Health Information Rights

HIPAA Security

"A covered entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information." Examples of the appropriate safeguards that should be implemented and practiced in order to protect PHI are:

- To carefully scrutinize shadow charts, individual databases, stand-alone servers, and drafts for security requirements
- Require authorization for access to information
- Implement entity authentication through mechanisms such as automatic log off; and
- Termination of personnel procedures

<u>Ways to protect patient privacy</u>

- Do not leave printed documents where unauthorized persons can see them
- When faxing, dial the number carefully and verify receipt if at all possible
- Shred PHI documents that are no longer necessary and are not the subject of any current or potential government review
- Position computer screens so that they cannot be seen by unauthorized persons
- Do not share your passwords
- Report suspected or known breaches of confidentiality to your manager, the privacy hotline or HSIS

Question?

I am not a physician or a nurse. Do I need to be concerned about protecting patient privacy and confidentiality? After all, I never look at patient medical records.

-**YES!** Because you are an employee of a covered entity and work in a healthcare facility, you should always be on the alert for situations that may compromise patient confidentiality and privacy

-**YES!** Because patients are asserting their rights to protect their confidential medical information through mechanisms such as lawsuits and you can incur civil and criminal penalties for noncompliance.

Let's Review Our Understanding of HIPAA!

UAB HEALTH SYSTEM

MS. HIP and UABHS

Ms. Hip, looking for information on high blood pressure, pulls up the UAB Health System web site.

- UABHS Notice of Health Information Practices.
- UABHS Articles on Blood Pressure available for review.

Ms. Hip registers her name and e-mail address for future mailings or notifications on high-blood pressure and other health topics.

- No HIPAA restrictions because information is not PHI.

Ms. Hip arrives at The Kirklin Clinic for her scheduled appointment.

- Ms. Hip is asked to sign an acknowledgement that she has received the Notice of Health Information Practices.
- Tracking of Acknowledgements.

Ms. Hip reviews the Notice and requests The Kirklin Clinic not to disclose her medical condition to her children because she does not want them to worry. Further, she does not want her medical information to be used by the clinic for anything other than treatment.

- Right to Request Restrictions, but no Right to Receive.
- Unit Manager and Patient Rep. contacted for discussions with Ms. Hip.
- TKC agrees not to disclose to children (except if there is an emergency), but refuses to limit use to treatment- need for payment and healthcare operations.
- Restrictions Requested Form documented in tracking.

Ms. Hip tells her physician, Dr. UAB, that she and her son attended outpatient-counseling sessions at CPM. Dr. UAB believes this may be relevant to Ms. Hip's high blood pressure and wants to see the medical record.

- Ms. Hip must sign an Authorization prior to release of the medical records of the counseling sessions.
- The physicians may release portions of the medical record to the consulting physician, other than the counseling sessions, without an Authorization.

Dr. UAB writes a prescription for high blood pressure medication and phones it into TKC Pharmacy. Ms Hip sends her husband to the TKC Pharmacy to pick up the medication.

- HIPAA authorizes a pharmacist to make a reasonable inference of the patient's best interest in allowing another individual to pick up a prescription.

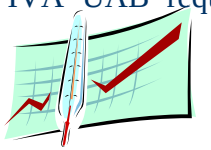
On the way home, a tractor hits Ms. Hip's car. Ms. Hip is rushed to University Hospital's Emergency Department, unconscious and in critical condition.

- Emergency Department Staff initiate immediate treatment. Ms. Hip regains consciousness and her condition stabilizes.
- The treating physician documents the emergency treatment situation.
- In an emergency situation, acknowledgement may be obtained as soon as practicable.

The police request the Emergency Department for Ms. Hip's medical records.

- The medical records will be released if the police have a court order or subpoena.

Patient Access and Utilization Management obtain registration information from Ms. Hip and call VIVA UAB to verify eligibility and obtain authorization for the Emergency Department Records. VIVA UAB requests a copy of the medical records.



- PHI may be transmitted to VIVA UAB, based on Notice of Information Practices

---

Ms. Hip's children rush to the Hospital and are sent to the waiting room, pending Ms. Hip's transfer from the Emergency Department to Jefferson Tower. The Hospital pages the family of Ms. Hip over the speaker system.

- HIPAA requires reasonable efforts to maintain the confidentiality of oral communication. Family pages are reasonable.
- The team may discuss condition with children if emergency; otherwise, treatment team must ask Ms. Hip to retract her restriction since she previously requested that her medical information not be disclosed to her children.

After being informed that Ms. Hip will need home health care, Social Services contacts a home health agency chosen by Ms. Hip. The agency requests Ms. Hip's proposed treatment plan.

- PHI may be transmitted to post-discharge care providers as part of the treatment plan per the Notice of Information Practices.

After being discharged, Ms. Hip re-reads the Notice of Health Information Practices and submits a written request for a copy of all her records.

- The Hospital HIM Department and TKC review the request and determine that all medical and billing records can be released, with the exception of her psychotherapy notes, which the treating physician determined should not be seen by Ms. Hip at the present time.
- Within 30 days of the request, the Hospital and TKC send copies of the records to Ms. Hip, along with a bill for the copying costs.
- The Hospital sends a letter to Ms. Hip informing her that she may not see the psychiatric records, based on her physicians order, but that she can request a review by another physician.

UABHS Development Officer requests patient lists from the Hospital so that she may send information to them about the fundraising efforts for the North Pavilion.

- The Hospital forwards only demographic information and dates of service.
- The Development Officer must include a description of how the individual may opt out of receiving any further fundraising communications.

Note- TKC *patient information cannot be used for Hospital Fundraising*.

Ms. Hip calls the Hospital to complain about being contacted for the North Pavilion fundraising project.

- The Hospital refers Ms. Hip to the Hospital Privacy Coordinator who informs Ms. Hip that she may submit a written complaint to the Privacy Coordinator for a response from UABHS.

Along with the complaint, Ms. Hip requests an accounting of the entities to which PHI has been disclosed.

- The Hospital prepares a response informing Ms. Hip that she may opt out of future fundraising.
- The Hospital checks the Accounting database and determines that the only non-TPO disclosures were to Development Officer. This information is transmitted to Ms. Hip.

Several months later, Ms. Hip dies at home under mysterious circumstances. The coroner requests the Hospital and TKC for Ms. Hip's medical records.

- The PHI may be released to the coroner for purposes of determining a cause of death.

For HIPAA questions or to report a suspected HIPAA violation contact:

Robin Mobley
1917 Outpatient Clinic
HIPAA Project Manager
934-9152
(1917 use only)

Or

Carlos Brown
UAB Hospital
Corporate Compliance/Privacy Manager
934-2990

Corporate Compliance & Privacy Hotline
934-4446

Test on Next Page

PLEASE PRINT TEST BEFORE ANSWERING QUESTIONS

TURN-IN TO ROBIN MOBLEY
RM#226 OR MEDICAL RECORDS MAILBOX

An Introduction to Confidentiality and Privacy under HIPAA
Nursing, Clinical, And Medical Staff Test

Name: _____

Employee/Social Security #: _____

Job Title: _____

Campus Mailing Address: _____

Date: _____

Score: _____

1.What area is addressed by HIPAA?
- a. Notice of Privacy Practices
- b. Business Associates
- c. Protected Health Information
- d. All of the above

2. What is considered to be a "covered entity" under HIPAA?
- a. The Kirklin Clinic, Callahan Eye Foundation Hospital, and UAB Hospital
- b. Physicians
- c. Health plans such as VIVA
- d. All of the above

3. What are the two kinds of sanctions under HIPAA?
- a. Criminal Sanctions
- b. Civil Sanctions
- c. A and B
- d. None

4. What organization is charged with enforcing HIPAA's Privacy Regulations?
- a. Joint Commission
- b. The Office for Civil Rights in the Department for Health and Human Services
- c. The Healthcare Financing Administration
- d. The Federal Bureau of Investigation

5. What form of personally identifiable health information is protected by HIPAA's privacy rule?
- a. Paper
- b. Electronic
- c. The spoken word
- d. All of the above

6. The newspaper has reported that someone famous has come to the hospital, and you're curious to know if this is true. Should you ask around or look for records about this person?
- a. Yes
- b. No

7. Providers have until April 14, 2004 to comply with the privacy regulations
- a. True
- b. False

8. HIPAA's privacy rule covers not just a patient's health-related information, such as his or her diagnosis, but also other identifying demographic information such as social security number and telephone numbers.
- a. True
- b. False

9. **Which of the following are some common features designed to protect confidentiality of health information contained in patient medical records?**
    a. Locks on medical records rooms
    b. Passwords to access computerized records
    c. Rules that prohibit employees from looking at records unless they have a need-to-know
    d. All of the above

10. **A friend is concerned because his girlfriend is in the hospital. He asks you to find out anything you can. Should you try to find information for your friend?**
    a. Yes
    b. No

11. **When is the patient's authorization to release information required?**
    a. When patient information is going to be shared with anyone for reasons other than treatment, payment, or healthcare operations
    b. To release psychotherapy notes
    c. Both A and B

12. **You are working elsewhere in the hospital when you hear that a neighbor has just arrived in the ER for treatment after a car crash. You should**
    a. Contact the neighbor's spouse to alert him or her about the accident
    b. Do nothing and pretend you don't know about it
    c. Tell the charge nurse in the ER that you know how to reach the patient's spouse and offer the information if needed

13. **If you suspect someone is violating the organization's privacy policy, you should**
    a. Confront the individual involved and remind him or her of the rules
    b. Watch the individual involved until you have gathered evidence against him or her
    c. Report you suspicions to your immediate supervisor of the organization's privacy or compliance officer, as outlined in your organization policy

14. **For nurses, physicians and clinical staff who intentionally misuse a patient's protected health information, the penalty is**
    a. Fines up to $100
    b. Fines up to $25,000
    c. Fines up to $250,000 and/or imprisonment for a term up to 10 years
    d. None of the above

15. **Protected Health Information (PHI) is considered confidential if it is related to:**
    a. A person's past, present or future physical or mental health condition
    b. A patient's present condition only
    c. A patient's past and present condition only