
# Understanding the Basic Concepts of HIPAA

# PRESENTED BY MNVS

SANDRA HILL, MSN, RN, CNML

Chief Administrative Officer

# PURPOSE

- This course is designed to introduce you to the basic HIPAA requirements and to describe how those rules impact your medical practice.

# Objectives

- Define HIPAA & the 3 main pieces
- Recognize the “covered entities” that must comply
- Describe what is “Protected Health Information”
- Explain security measures to comply with HIPAA rules

# Terms

- HIPAA – Health Insurance Portability and Accountability Act
- CE – Covered Entity
- BA – Business Associate
- BAA – Business Associate Agreement
- PHI – Protected Health Information
- HHS – Health and Human Services
- OCR – Office of Civil Rights
- DOJ – Department of Justice

# HIPAA

- (HIPAA) Health Insurance Portability and Accountability Act enacted 1996
- Final Implementation April 14, 2013
- Administered by HHS
- Enforced & Implemented by OCR

# What is HIPAA?

- HIPAA is a Federal Law that has special privacy, security, enforcement rules that health agencies must follow.
  - Privacy Rules make sure a patient's health info is protected & not given out without permission
  - Security Rules make sure a patient's personal info is stored and electronically transmitted safely.
  - Enforcement Rules established and implemented by OCR & DOJ

# Overall Purposes of HIPAA

- To protect and enhance the rights of consumers by providing them access to their personal identifiable health information and controlling the inappropriate use of that info.
- To improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection.

# Patient

- Gives more control to the patient over his or her health information
  - How their info may be used
  - Limits amount of info released
  - Gives patient the right to examine & obtain a copy of their health record & request corrections

# Healthcare Providers

- Sets boundaries on the use and release of health records
- Establishes safeguards to protect the privacy of health info
- Holds violators accountable
- Protects our professional reputation
- Avoids loss of Medicare & Medicaid

# Does HIPAA Change the Way We Do Our Work?

- Makes it a law that health care agencies keep PHI private and secure.
- Requires staff to be informed of HIPAA regulations and their responsibilities.

# Does HIPAA Change the Way We Do Our Work?

- HIPAA requires that health care agencies give their patients info about their rights in the form of a *Notice of Privacy Practices*.

- Health care agencies will ask patients with whom they can share their PHI on a *PHI Communication Resource Form*

# Site Specific Guidelines

- To meet HIPAA regulations, each health system will have written policies and procedures/guidelines on how HIPAA will be carried out in their facility.
- A HIPAA Officer/Director/Risk Manager must be assigned for regulatory purposes.

# Federal vs State standards

- If states have higher standards they override the basic standards set for HIPAA by Health and Human Services.

# Fines and Legal Penalties if you do not obey the laws

- Federal fines of $100 per accidental violation ($25,000 annually).
- Maximum fine of $250,000 for malicious violation
- Federal prison sentence up to 10 years for selling PHI or maliciously using the info to harm someone

# Sanction Levels

- *Level 1* - Violation is accidental.

  Ex: Disclosing PHI by leaving a computer terminal unattended without logging off.

- *Level 2* - Violation is purposeful disregard of policies.

  Ex: Using another employee's password to look at patient records without a need to know.

- *Level 3* - Violation is intentional and malicious with complete disregard to HIPAA standards.

  Ex: Selling PHI to a local newspaper.

# HIPAA Violation Complaint

- Facilities will not be audited for compliance, but sites will be assessed with complaints.
- Internal and external process and guidelines for the patient and employee to file a complaint must be in place.

# Exceptions of HIPAA

- Emergency situations
- Public health issue
- Judicial and administrative proceedings
- Law enforcement purposes
- Reports of abuse
- Organ donation

# Exceptions of HIPAA

- Funeral Directors
- Unconscious patient
- Subpoenas
- Worker Compensation
- Neglect or domestic violence
- Serious threats to safety and to health

# Covered Entity (CE)

- Individuals and organizations that have primary responsibility to protect personal identifiable health info:

  1. *Health Plan* – Insurance Co, Medicare…
  2. *Health Care Clearing House* – an entity that provides billing services, etc.
  3. *Health Care Providers* – person or entity that provides and bills for health care services in an electronic form

# Covered Entities Must:

- Develop a Privacy Notice
- Develop related policies and procedures
- Train employees to understand the privacy procedures – For HIPAA standards, students are considered employees.
- Appoint a Privacy/HIPAA Officer
- Secure and protect medical records
- Establish a complaint process

# HIPAA Requires Privacy Notice

- Notice of privacy practices to all patients written in simple language.
- How PHI will be used and disclosed for Treatment, Payment, and health Operations.
- How to file a complaint
- Consent to use and disclose PHI for (TPO) or Acknowledgement of being offered a Notice

# Patient Rights

- To know how their PHI will be used and disclosed
- To request additional protection e.g. Insurance
- To request a copy of their medical records
- To request an amendment to their medical records
- To have an accounting of disclosures of PHI
- To refuse to sign the acknowledgement

# Protected Health Information (PHI)

Privacy Rule Protects:

*Individually Identifiable Health Information*

- Past, present or future physical or mental health condition
- Provision of health care to the individual
- Past, present, or future payments for the provision of health care to the individual

# Business Associate (BA)

- A person or company that provides services to a covered entity
- CPA, attorney, billing company, medical record shredding company, computer consultant, fax/copy machine repair…
- Students and their schools

# Business Associate Contract

- Must have Agreement that provides assurances for privacy & assigned use of patient's PHI
- BA will safeguard the PHI

# Reasonable HIPAA Safeguards

- Not intended to impede customary and essential communications and practices
- Identify & protect against reasonably anticipated threats to security
  - Computer Password/Individual Password
  - Locked Forms & doors
  - Do not disable firewalls
  - No Jokes on computer=virus

# "Minimum Necessary" Use and Disclosure

- Develop policies and procedures to define & minimize the amount of PHI used, disclosed, and requested.
  - Internal use – Restrict access and sharing of information – "Need to Know" basis
  - External use – Establish allowable routine, recurring disclosures, or request for disclosures to minimum amount

# Minimum Necessary Standard

- "Minimum Necessary" does not apply:
  - Request by health care providers for treatment purposes
  - Disclosures to the patient
  - Pursuant to a patient's authorization
  - Disclosure to HHS for complaint investigation
  - Required by law or HIPAA compliance

# Minimum Necessary Standards

- Disclosure to friends and family--We can discuss PHI with family and relatives, if:
  - a) The patient agrees
  - b) Patient has had the chance to object and does not
  - c) Reasonable e.g., patient brings a spouse into room
- White boards, bulletin boards, etc:
  - Use of these boards to show location or status of a patient is allowed, but take reasonable precautions to avoid accidental disclosures.

# Research

- Individual patient authorization
- Hospital Research Board Authorization
- Institutional Review Board (IRB)
- Research provisions are very complex. You might need to seek legal counsel.

# Practical Application of HIPAA

- Development of policies and procedures
- Development of employee annual training
- Employee/student orientation within 15 days of hire
- Safe Procedures:  Fax, phone, schedule book, computer screens, passwords
- Seek Patient authorization: Fax, phone

# Practical Application of HIPAA

- *HIPAA Signed Notice*
  - Document good faith effort if refused
- *Communication Resource Form* of PHI
  - List of people who can receive info
  - Patient directory publication permission
  - Clarification of phone messages

# Practical Application of HIPAA

- Protection of verbal PHI:
  - Use of name, very private or quiet discussion of patient's condition in public area.
- Protection of written PHI:
  - Closed medical files in shared area, locked file cabinets, locked offices, computer passwords.
- Minimum Necessary:
  - Define the "Minimum Necessary" of PHI release & reasonable reliance of appropriate request of info.

# Protect Patient's Privacy

- Only look at info you need.
- Don't talk about patients in public areas.
- Don't discuss other's patients
- Protect computer terminals.
- Protect paper records. No notes left.

# Accidental HIPAA Violation

- An outsider overhears workers talking about a person in an elevator, hallway, cafeteria, or front office.
- Workers leave private info lying open in public places or desks or trash.
- A worker forgets to log out and leaves a computer on and alone.

# Intentional HIPAA Violation

- Give medical records or any PHI to others who don't have permission to see them.
- Share PHI with your family members, friends, and newspapers who have no legal right to it
- Copy PHI and take it home
- Make changes in the patient info on the computer that you don't have permission to make
- Share your computer password with coworkers or others
- Look at info in paper or computer medical records that you don't have permission to see

# Frequently asked Questions

- Can medical practitioners access patient's medical info in the course of their training?
- Yes.  Health care operations definition provides for learning under supervision. Minimum necessary.

# Frequently asked Questions

- Are business associates required to restrict their uses and disclosures to the minimum necessary?

- Yes, BA contract limits the uses and disclosures to the minimum necessary.

# Frequently asked Questions

- Can a physician's office FAX patient medical info to another physician or med office?

- Yes. For treatment purposes with reasonable safe guards i.e., confirming the current fax number and the fax machine is in a secure location.

# 1-True or False

- You will no longer be able to call patients from a waiting room by their name.  You will have to use a number system or pager.

- False-Unless a patient asks that we not call them by name from the waiting room, we can continue to do so.

# 2-True or False

- We will no longer be able to put any patient names or charts outside of the hospital doors for identification.

- False-Unless a patient has requested that we do not publish his/her name in the Patient Directory, we can put the name outside the door.  The chart can be turned with the name facing the wall.

# 3-True or False

- We will have to make all the hospital rooms private to avoid discussing treatment with another patient or family member in the room.

- False-HIPAA Privacy Standards do not require structural changes to the facilities.  We should take care in pulling the curtains and speaking in a soft voice when having a private conversation with a patient.

# 4-True or False

- **Next to loose talk**, the current area of greatest risk for inappropriate release of PHI is *faxing* records to the incorrect location.

- True-It is critical that fax numbers be verified and carefully entered so that medical records do not end up sent to the wrong location.

# Pulling it all together

- The following are a few quick case examples for review to allow you to put the HIPAA regulations into real life situations.

# Case Example 1

- Mrs. Johnson is a patient you transported to your local hospital. You receive a phone call from her granddaughter wanting to know how she is doing and what happened to her. What do you do?

# Case example 1 answer

- Ask the granddaughter her name, check the PHI *Communication Resource Form* to see if the granddaughter is listed.
- If not listed, you can give a general condition, but not specific PHI. You can direct her to someone listed on PHI for specific PHI. If the patient requests “not to publish info” then you may not provide any info.
- Check specific site policies and procedures

# Case Example 2

- Julie Smithson calls your office to ask about her father's bill.  Her father told her he doesn't know why he received a bill.  Medicare was suppose to have taken care of it.
- She is trying to help clear the confusion for her father.  She asks you to find out what the bill is for and if Medicare is going to pay it.
- Can you discuss this info with her?

# Case Example 2 Answer

- First check the PHI *Communication Resource Form* to see if the daughter is listed.
- If yes, then you may talk with her about the bill.
- If no, then you need to explain that for patient confidentiality reasons , you are unable to discuss any information without her father's authorization.

# Case Example 3

- Margaret is a receptionist and has access to the schedule of patients coming in for appointments each day.
- One day Margaret notices that Connie, one of her daughter's friends, has an appointment in PT that week for LBP. When she goes home that evening she tells her daughter that she will be seeing Connie later in the week at the clinic.
- Is she violating privacy rules?

# Case Example 3 Answer

- Yes, Margaret is violating privacy rules when she tells her daughter about Connie's scheduled appointment.

# Case Example 4

- Sue is an EMT student in the ER.  One day a fellow college classmate is admitted to the hospital.
- Sue checks the chart and finds out that he was admitted with a diagnosis of cancer
- When Sue gets home she calls all his friends to tell them he is in the hospital with cancer and to collect money for flowers.
- Do Sue's actions violate HIPAA privacy?

# Case Example 4 answer

- Yes, even though she might have had good intensions but:
  - She searched the patient's chart.
  - She disclosed to a third party that the patient had been admitted.
  - She also revealed PHI by disclosing the patient's diagnosis without his consent.
  - Did she have a "need to know" this pt's info?

# HIPAA Training Completed

Go to HIPAA Test and complete.