Introduction to HIPAA for Health Care Professionals

FOOT HEALTHCARE ASSOCIATES

Introduction

- This educational module is intended to help employees understand the fundamentals of HIPAA at clinical sites.
- Many sites or agencies will expect you to complete an orientation to their specific approach to HIPAA policies.

What is HIPAA and Why Should I Care?

- **The Health Insurance Portability and Accountability Act (HIPAA) is a federal law designed to improve the efficiency and effectiveness of the health care system.**
- **Part of HIPAA directly affects your clinical work and the operations of any facility where you will train.**
- **Understanding the fundamentals of HIPAA will prepare you to step into training sites with a clear understanding of how to comply with requirements for respecting the privacy of protected health information (PHI).**

Content

I. The Importance of Protecting Patient Health Information

II. General HIPAA and Privacy Rule Overview

III. Permitted Uses and Disclosures

IV. Patients' Rights to Control their Health Information

V. Administrative Requirements

VI. General HIPAA Security Rule Overview

The Importance of Protecting Patient Health Information

Employees with access to patient data may use or disclose it only on a "need to know" basis:

- Keep this information confidential.
- Access or use this information only as required to perform your job.
- Provide the minimum necessary information when responding to information requests.
- Do not discuss this information with others unless it is administratively or clinically necessary to do so.
- Do not use any electronic media to copy or transmit information unless you are specifically authorized to do so.

The Importance of Protecting Patient Health Information

Additional examples of actions to protect patient privacy:

- At nursing stations, keep computer monitors that display patient information turned away from public view.
- Log off from patient records before leaving a data terminal.
- If you must leave for a few moments, do not leave records face up on your desk or work area.
- Place fax machines used to receive confidential records in locations with appropriately limited access.
- Avoid elevator and hallway consultations involving patients.

Consequences of Violations

Inappropriate disclosure of confidential information is subject to discipline, up to and including discharge from employment. For licensed professionals, it is also subject to discipline by licensing and credentialing bodies

There are civil and criminal penalties for violations of patient privacy:

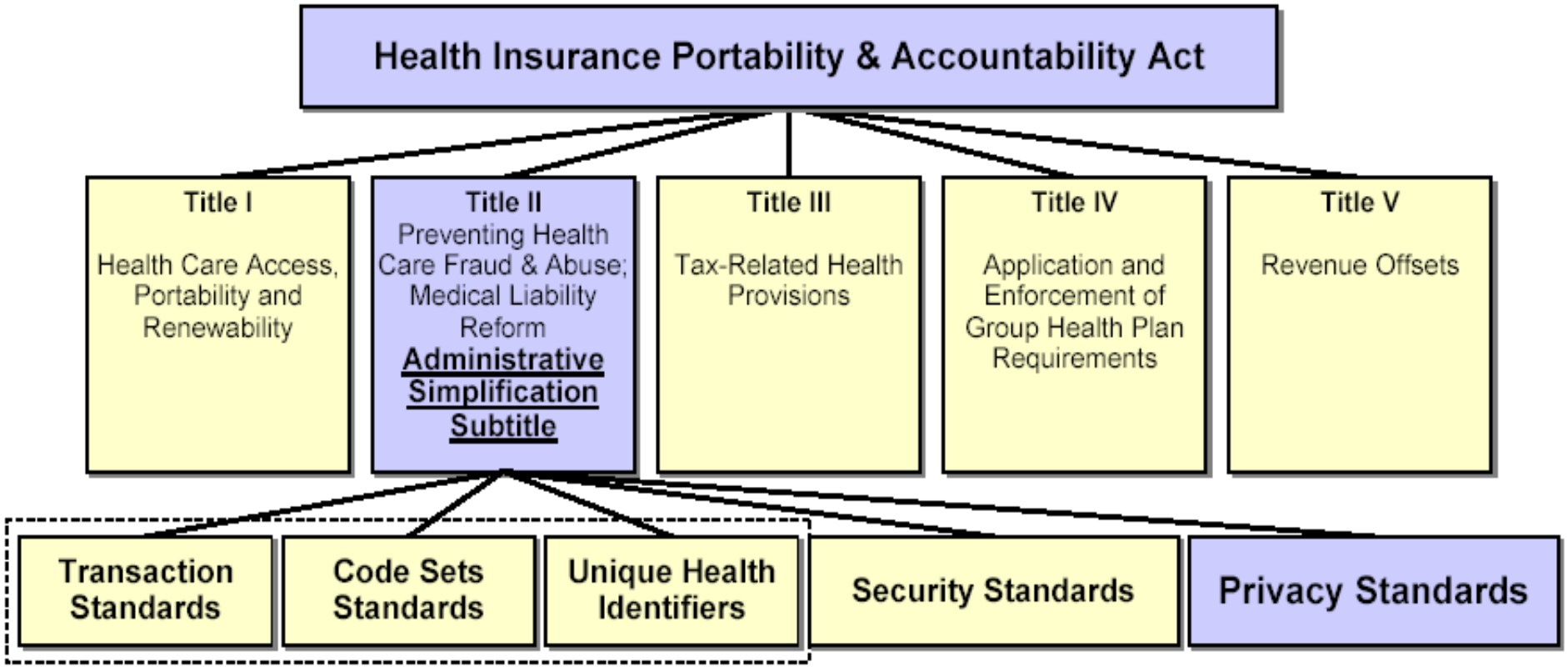
- Fines up to $25,000 for multiple violations of the same standard in a calendar year
- Fines up to $250,000 and/or imprisonment up to 10 years for deliberate misuses of individually identifiable health information.

HIPPA rules are not a barrier to good care:

- **The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients.**
- **Staff and students are free to communicate as required for quick, effective, and high-quality health care.**
- **The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.**

HIPAA and Privacy Rule Overview:

The Health Insurance Portability and Accountability Act (HIPAA) has many parts. Most relevant to employees in the health professions are the “Administrative Simplification” provisions including national standards for electronic health care transactions, codes, identifiers, security, and the privacy of personal health information.



The Privacy Rule applies to protected health information (PHI).

Protected health information (PHI) is "identifiable" health information acquired in the course of serving patients. Any of the following data make health information "identifiable":

- Name
- Social security number
- Street and email addresses
- Employer
- Telephone and fax numbers
- Member or account numbers
  - (e.g. medical record number, health plan identification number)
- Relatives' names
- Date of service, birth or death
- Fingerprints, photographs, voice recordings
- Certificate or license numbers
- Any other linked number, code, characteristic (e.g. device identifiers, serial numbers)

The Privacy Rule applies to written, electronic, and oral protected health information (PHI)

The Privacy Rule: Parents and Minors

HIPAA generally defers to state law concerning the relative rights of parents and minors. In this module, the terms "individual" or "patient" mean:

- Parents and legal guardians may generally exercise the HIPAA rights of their minor children;
- Patients 18 or older, or with emancipated or "mature minor" status, may exercise their own rights under HIPAA.
  - If you are in doubt about a patient's status or have questions about the legal definition of emancipation or "maturity," check with management.
- A minor patient may exercise HIPAA rights regarding matters involving diagnosis or treatment relating to certain conditions (e.g., sexually transmitted diseases, drug or alcohol dependency, and pregnancy).

Permitted Uses and Disclosures of PHI

An agency may use or disclose PHI for the following purposes:

- In order to treat a patient.
- Justifying payment for treating a patient.
- Certain administrative, financial, legal, and quality-improvement activities that are necessary to “run the business” (such activities are called “health care operations”).

Additional Permitted Uses and Disclosures of PHI

If the disclosure complies with and is limited to what the law requires, agencies are permitted to disclose PHI:

- To public health authorities and health oversight agencies
- To coroners, medical examiners, and funeral directors
- For organ procurement
- To respond to court orders and subpoenas

Permitted Uses and Disclosures of PHI

There are certain disclosures that agencies may make if the patient is given the opportunity to agree or object:

- A patient's location and condition (in general terms) if the patient is asked for by name or for disaster relief purposes.
- PHI relevant to care, or to family/close friends who are designated by the patient.

Permitted Uses and Disclosures of PHI

Written permission or authorization from the patient is required to use or disclose PHI for purposes other than treatment, payment, health care operations, or as required by law or for public health reasons.

- E.g. Photos/Videos
- Testimonials

PHI and **Research**

Specific procedures may allow PHI to be used or disclosed for research purposes:

- Records can use de-identification.
- Written authorization may be obtained from the patient for research use or discloser.
- The Institutional Review Board (IRB) may grant a waiver of written authorization.
- Only data needed to prepare work for research purposes only may be disclosed.
- Special provisions may allow for research using a decedent's PHI.

General Data Disclosures

An agency may use or disclose demographic information and the dates of treatment for the purpose of raising funds for its own benefit, without an authorization.

- Example: "Between January and June we treated 47 patients under 18, 20% of whom had family incomes under $25,000 per year.

General data disclosures

An agency must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of uses, disclosures, or requests.

Incidental Disclosures

An incidental disclosure that occurs as a by-product of an otherwise permitted use or disclosure is permitted:

- If it cannot be reasonably prevented.
- If it is limited in nature.
- To the extent that reasonable safeguards exist.

Permitted Uses and Disclosures to Carry Out Treatment, Payment, and Health Care Operations

An entity may use or disclose PHI for its own "Treatment," "Payment," or "Health Care Operations":

- **"Treatment"** generally means the providing, coordinating, or managing health care and related services among health care providers or by a health care provider with a third party; consultation between health care providers regarding a patient; or the referral of a patient for health care from one health care provider to another.
- **"Payment"** encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill coverage responsibilities, and to provide benefits under the plan.
- **"Health Care Operations"** are certain administrative, financial, legal, training, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.

Disclosures of PHI for Treatment, Payment, and Health Care Operations of Another Entity

This is appropriate for:

- Treatment activities of a health care provider.
- Payment activities of the entity that receives the PHI.
- Several specific uses included in the health care operations of the entity that receives the PHI, if both the sending and the receiving entities either have or had a relationship with the individual who is the subject of the PHI and the PHI is related to this relationship. The permitted disclosure may be for the purpose of
  - Health care fraud and abuse detection or compliance,
  - Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, or contacting of health care providers and patients with information about Treatment alternatives.
  - Reviewing the competence or qualifications of health care professionals, evaluating practitioner or health plan performance; conducting training programs for students or practitioners; or accreditation, licensing, or credentialing activities.

"Public Good" Uses and Disclosures

An agency may use or disclose PHI without the written authorization of the individual in the situations listed below:

- **Uses and disclosures required by law.**
- **Uses and disclosures for public health activities** (i.e., public health, child abuse and neglect, FDA, communicable diseases, employment workplace medical surveillance).
- **Disclosures about victims of abuse, neglect, or domestic violence.**
- **Uses and disclosures for health oversight activities.**
- **Disclosures for judicial and administrative proceedings.**
- **Disclosures for law enforcement purposes.**
- **Uses and disclosures about decedents** (i.e., to coroners and funeral directors).
- **Uses and disclosures for cadaveric organ, eye, or tissue donation purposes**
- **Uses and disclosures for research purposes.**
- **Uses and disclosures to avert a serious threat to health or safety.**
- **Uses and disclosures for specialized government functions** (i.e.. military and veterans activities, national security and intelligence activities, protective services for the president and others, medical suitability determinations, or correctional institutions and other law enforcement custodial situations).
- **Disclosures for workers' compensation.**

"Public Good" Uses and Disclosures

State Law and other Federal Laws that are more protective of individual's privacy should be followed. Agencies are required to track most disclosures and to provide individuals with a listing of them upon their request.

Authorization Requirements

HIPAA requires the agency to obtain a written authorization to disclose or release any PHI that is not for treatment, payment, or health care operations, or otherwise permitted by the rules

Examples of disclosures requiring written authorization under HIPAA: Schools, camps, airlines, hotels, aid organizations, outside attorneys

These authorizations must contain the following elements:

- A description of the information to be used or disclosed.
- Who is authorized to make the use or disclosure.
- To whom the disclosure may be made.
- A description of each purpose of the disclosure.
- An expiration date or an expiration event.
- Signature of the individual and date.
- Required statements:
  - The individual's right to revoke the authorization and directions how to revoke.
  - The ability or inability to condition treatment or payment.
  - The risk that redisclosure by the recipient may occur.

Additional Written Authorizations

Agencies must typically obtain written authorization to disclose or release patient information in situations beyond what HIPAA requires.

Examples of practices that typically requires permission or consent to release information:

- Photographs and videos for treatment and training.
- Transports.
- Sharing patient information with outside providers at the patient's request or at the request of another provider.
- Second opinions.
- Making requests for patient information from other providers.

Clinical research is uniquely affected by the regulations.

From a clinical investigator perspective, the new regulations will control access to existing health information (medical/database record reviews) and handling of identifiable information created as part of clinical research.

There are specific methods that allow PHI to be used or disclosed for research purposes:

- All data are de-identified (according to the specific standards of the Privacy Rule).
- A limited data set is collected and released (according to the specific standards of the Privacy Rule).
- A patient gives a written authorization that his or her data may be used and/or disclosed.
- The Institutional Review Board (IRB) may grant a waiver of written authorization.
- Data are collected for preparatory work for research purposes only (according to the specific standards of the Privacy Rule).
- Special provisions are in place for research on a decedent's PHI.

Incidental Disclosures

An incidental disclosure that occurs as a by-product of an otherwise permitted use or disclosure is permitted:

- If it cannot be reasonably prevented.
- If it is limited in nature.
- To the extent that reasonable safeguards exist.

Examples:

- Keep patient information on white boards/locator boards to a minimum.
- Reduce unnecessary incidental disclosures during check-in processes and in waiting rooms.
- Take care to limit the amount of information disclosed on an answering machine.
- Do not discuss patients in public areas.
- Consider location when posting patient schedules and storing patient charts.
- Keep voices low when discussing patient issues in joint treatment areas.
- Position workstations so screen does not face public areas; consider using screen filters.

Notice of a Person's Rights to Control His or Her PHI

An agency must distribute to each patient at the first treatment encounter, and obtain written acknowledgment of receipt of, a "Right to receive Notice of Privacy Practices":

- Describing how the agency may use and disclose PHI.
- Describing the rights the individual has to control his or her health information.

Notice of a Person's Rights to Control Their PHI

Patients should receive a listing of disclosures required by law, public health, health oversight, child abuse reporting, FDA reporting, communicable disease exposure, wound or injury reporting, response to legal process, law enforcement, coroner/medical examiner, organ procurement, research protocols where the IRB has waived the individual's authorization requirement, or workers' compensation.

Notice of a Person's Rights to Control Their PHI

People have a right to request confidential forms of communication. Agencies must accommodate reasonable requests to receive confidential communications.

People have a right to request restricted uses and disclosures of PHI:

- Permitting such restrictions not required.
- Requests for restrictions should be made in writing to the institution's privacy officer.

Notice of a Person's Rights to Control Their PHI

People have a right to inspect and obtain a copy of their health information. Individuals have the right to inspect and obtain a copy of health information in the medical or billing record.

People have a right to request amendment to medical and billing records.

People have a right to file a formal complaint about violations of privacy with the agency or the Department of Health and Human Services.

The Notice of Privacy Practices

The Notice of Privacy Practices describes how the agency may use and disclose PHI and describes the rights the individual has to control his or her health information. The agency must distribute the notice to each patient at the first treatment encounter and obtain written acknowledgment of receipt.

Tracking Disclosures or the "Accounting of Disclosures Log"

An individual has a right to receive a listing of certain disclosures.

The listing must include disclosures made to individuals or entities outside of agency for the following purposes:

- Required by law
- Public health activities
- Health oversight activities
- Child, elder, or handicapped abuse reporting
- FDA reporting
- Communicable disease exposure
- Wound or injury reporting
- Response to legal process
- Law enforcement activities
- Coroner or medical examiner
- Organ procurement
- Research protocols where the IRB has waived the individual's authorization requirement
- Workers' compensation

"Accounting of Disclosures Log"

The listing must include a description of:

- To whom information was disclosed–When it was disclosed
- What was disclosed
- Why it was disclosed

Right to Request Amendment

Individuals have the right to request amendment to PHI included in their medical and billing records.

The patient may approach the author of the entry, point out the error, and ask the author to correct it.

Uncontested changes requested to the author of the entry can be corrected by the author.

If the author does not agree with the request, then the patient may contact the facility's privacy officer, who may conduct a review of the relevant record, consult with the treating physician, evaluate the individual's request, and consult with other hospital professionals, as appropriate.

Administrative Requirements: Business Associates Overview

- A Business Associate is a person or entity to whom an agency discloses PHI so that the person or entity may carry out, assist with, or perform a function on behalf of the agency (e.g., billing).
- The agency is required to have "satisfactory assurance" that any business associate will "appropriately safeguard" PHI received or created by the business associate in the course of performing services for the agency.
- The agency must document the satisfactory assurances through a written contract.
- The business associate provision does not apply to providers who receive information for treatment purposes.

Practical Examples of Appropriate Behavior Under HIPAA

The following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

- **Orally coordinate services at hospital nursing stations.**
- **Discuss a patient's condition over the phone with the patient, a provider, or *family member.**
- **Discuss lab results with a patient or other provider in a joint treatment area.**
- **Discuss a patient's condition or treatment regimen in the patient's semi private room.**
- **Discuss a patient's condition during training rounds in an academic or training institution.**

HIPAA Security Rule

The HIPAA Security Rule provides that Practices must:

- Implement security awareness and training for all members of its workforce (including management).
- Implementation specifications:
  - Security reminders & Periodic security updates.
  - Protection from malicious software: Procedures for guarding against, detecting, and reporting malicious software.
  - Log-in monitoring: Procedures for monitoring log-in attempts and reporting discrepancies.
  - Password management: Procedures for creating, changing, and safeguarding passwords.
  - Encrypting and securing of outgoing Patient data
  - Securing Hardware/Harddrives and data contained on electronic devices (

Personal HIPAA Compliance Checklist

While working within the Practice I will remember to ask the assigned Privacy Officer:

- Whether I need to review the site's specific HIPAA policies.
- When and where patients must be given HIPAA notices.
- Site-specific HIPAA implementation policies and Security measures.

When reviewing records or discussing patients I will be mindful of the privacy rules.

If I have any questions about the appropriateness of a request for information, I will check with my on-site supervisor or the Compliance Officer.

Review

Core HIPAA Principles

- **Privacy Rule:** Protect patient information (PHI) in all forms—verbal, written, and electronic
- **Security Rule:** Safeguard electronic PHI (ePHI) through administrative, physical, and technical measures.
- **Minimum Necessary Standard:** Access or share only the information needed to perform your job.
- **Patient Rights:** Patients can request access to their medical records and must authorize most disclosures.
- **Reporting:** Immediately report any suspected privacy or security incident to your Privacy or Security Officer.

Everyday HIPAA Best Practices

- Never discuss patient information in public or common areas.
- Always **lock your computer screen** when leaving your desk.
- Verify fax numbers and email addresses before sending PHI.
- Use **secure messaging or encrypted email** when sharing PHI electronically.
- Store paper charts or printed PHI in **secure areas** when not in use.
- Dispose of PHI only in approved shredding bins.
- Keep **passwords private**—never share them, even with coworkers or IT staff.

Review

Cybersecurity Essentials

- **Phishing Awareness:** Don't click suspicious links or open unexpected attachments. When in doubt, verify with IT.
- **Strong Passwords:** Use strong mix of upper/lowercase letters, numbers, and symbols.
- **Multi-Factor Authentication (MFA):** Always enable it when available.
- **System Updates:** Allow automatic updates and restarts to patch vulnerabilities.
- **Email Security:** PHI must only be sent through secure, HIPAA-approved systems.
- **Device Safety:** Never use personal USB drives/devices for clinic data.
- **Wi-Fi:** Connect only to clinic-approved, secure networks.
- **Data Backup:** Follow your clinic's backup and recovery protocols.

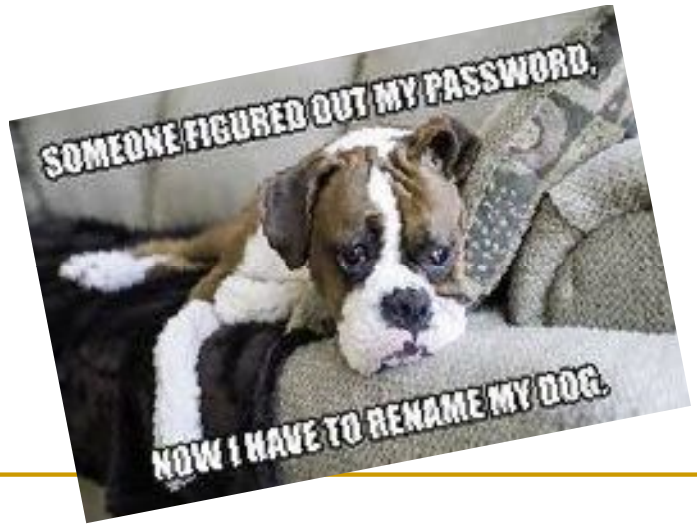
What To Do If Something Happens

- If you suspect a **breach**, **ransomware attack**, **lost/stolen device**, or **misdirected email**, report it **immediately** to your HIPAA Privacy/Security Officer or IT department for mitigation.
- Quick reporting helps reduce potential exposure and legal risk.

Protecting patient data is not just compliance—it's patient trust. Every employee plays a role in maintaining privacy and security every day.

TEST!!!!!!

- Must be printed, completed and turned back into the Manager. (scan/email or physically hand in)
- Please write your name/date and sign.



THANKS FOR PAYING ATTENTION!!