HIPAA/HITECH

STAFF TRAINING

Overview

- Our Commitment to Patient Privacy
- HIPAA Privacy and Security Requirements
- How We Use Patient Information
- How We Protect Patient Information
- Role of Privacy Officer and Security Officer
- Your Responsibilities as an Employee

Our Commitment to Patient Privacy

- Patient Privacy is important to us
- Patient Privacy is protected by federal and state laws
- As a provider, we must comply with all laws and regulations
- Our Notice of Privacy Practices explains how we use information
- Designated personnel to assure patient privacy:
  - Privacy Officer
  - Security Officer
- Policies and Procedures to safeguard Patient information
- Corrective actions and self-reporting of information breaches

What is Protected Health Information?

Protected **H**ealth **I**nformation (PHI) is individually identifiable health information, in any form or medium, that relates to the person's:

- Health care or condition
- Provision of healthcare
- Provision of payment for healthcare
- Any demographic information that can identify the person (name, dates, telephone number, insurance number, SSI number, account number, photo, email address, etc.)

General rule: **Any** information that can be used as a link to a person's health information.

Health Information and Privacy Law

- **HIPAA**

  Health **I**nsurance **P**ortability and **A**ccountability **A**ct of 1996

  - **Privacy Rule** (April 2003) protects access to, and uses and disclosures of, an individual's protected health information (PHI). The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

  - **Security Rule** (April 2005) requires physical and technical safeguards to protect the confidentiality, integrity, and availability of PHI. The Security Rule protects health information in electronic form, and requires entities covered by HIPAA to ensure that electronic protected health information is secure.

Security of Patient Information

- **HITECH**

  Health **I**nformation **T**echnology for **E**conomic and **C**linical **H**ealth Act of 2009

  - **Breach Notification Rule** (August 2009) requires covered entities and their business associates to provide notification following a breach of unsecured protected health information

Who is Subject to HIPAA and HITECH?

- "**Covered Entity**"
  - Any healthcare organization that stores, processes, or transmits health information electronically

- **"Business Associates"**
  - Organizations who perform services that involve the use or disclosure of PHI on the behalf of a covered entity

Uses and Disclosures

- **Use - The sharing or use of PHI <u>within an entity that maintains such information</u> (typically for Treatment, Payment, or Operations)**
  - Processing requisitions
  - Transmitting claims
  - Evaluate services (quality assurance)
- **Disclosure - The release, transfer, or provision of access to PHI <u>outside the entity holding the information</u>**
  - Transmitting patient information to another provider
  - Transmitting claim information to billing vendor
- **Allowable Uses and Disclosures -** for purposes of Treatment, Payment, or Operations, public policy, where required by law

Penalties for Non-Compliance

- $100 fine per day for each unmet standard (up to $25,000 per person, per year, per standard).
- $50,000 fine + one year in prison for improper disclosure of health information.
- $100,000 fine + five years in prison for obtaining health information under false pretenses.
- $250,000 fine + ten years in prison for using health information for personal gain.

The United States Office of Civil Rights is responsible for conducting HIPAA audits and investigating HIPAA violations

Disciplinary action, up to and including termination of employment, for failure to follow policies and procedures

Penalties for Non-Compliance

- 2009: CVS ordered to pay $2.25 million for disposing PHI in unsecured trash dumpsters
- 2011: Cignet Health to pay $4.3 million for denying patients timely access to records
- 2011: UCLA to pay $865,000 when employees accessed electronic records of celebrities.

Penalties for Non-Compliance

2012 Massachusetts provider settles HIPAA case for $1.5 million

- Theft of an unencrypted personal laptop containing the electronic protected health information (ePHI).
- The information contained on the laptop included patient prescriptions and clinical information.
- Failed to take necessary steps to comply with the requirements of the HIPAA Security Rule.

Penalties for Non-Compliance

2012: Alaska DHSS settles HIPAA security case for $1,700,000

- A portable electronic storage device (USB hard drive) possibly containing electronic PHI was stolen from the vehicle of a DHHS employee.
- Did not have adequate policies and procedures in place to safeguard electronic PHI.
- Had not implemented device and media controls or devices were not encrypted as required by the HIPAA Security Rule.

Penalties for Non-Compliance

2012: HHS settles HIPAA case with Blue Cross Blue Shield Tennessee for $1.5 million

- 57 unencrypted hard drives stolen from leased facility.
- Contained names, SSI , diagnoses, birth dates of one million individuals.
- Did not have adequate physical safeguards.

More Examples of Non-Compliance

2013: HHS announces first HIPAA breach settlement involving less than 500 patients

Hospice of North Idaho settles HIPAA security case for $50,000

Unencrypted laptop containing PHI of 441 patients was stolen

More Examples of Non-Compliance

2010: University of Rochester Medical Center notifies over 800 patients of possible breach after surgeon lost a flash drive with patient information

2012: Dakota County (Minnesota) medical examiner investigator's personal laptop stolen - laptop was not password protected

2012: CHRISTUS St. John Hospital notified the New Hampshire Attorney General's Office of a breach involving unencrypted patient information on a lost memory stick

How We Use Patient Information

HIPAA allows for the use or disclosure of PHI for purposes of **Treatment**, **Payment,** and **Operations**

As a provider of healthcare services, we use patient information in the following ways:

- Receive clinical information and orders from physicians and other providers **(Treatment)**
- Provide information to physicians and other providers **(Treatment)**
- Bill for our services **(Payment)**
- Internal processes-quality assurance, analysis, monitoring **(Operations)**

Patient authorization is not necessary for purposes of Treatment, Payment, or Operations

“Minimum Necessary” Rule

Must make reasonable efforts to limit use or disclosure of PHI to the minimum necessary amount to accomplish the intended purpose of the use of the information.

Ask: “What information is needed for this release?”

- **Accessing, using, or disclosing PHI beyond the minimum necessary use is a violation of HIPAA.**

Minimum Necessary Rule does not apply to:

- Requests for treatment or laboratory services
- Disclosures to the patient
- When authorized by the patient
- When required by law

Individual (Patient) Rights

Under HIPAA, Patients have the Right to:

1. See or inspect clinical record and obtain copies; if denied, to request a review of denial
2. Change or amend information believed to be incorrect
3. A list of disclosures for 6 years after 4/14/03
4. Restrict uses and disclosures
5. Request provider communicate in ways to protect privacy
6. Receive a paper copy of Notice of Privacy Practices

Our Responsibilities

1. Assign responsibility for privacy and security.
2. Establish procedures for handling “PHI”.
3. Provide physical security.
4. Provide technical security.
5. Establish rules for protecting patient privacy.
6. Allow patients access to medical records.
7. Respond to complaints.
8. Publish a Notice of Privacy Practices.
9. Ensure that Business Associates protect patient privacy.
10. Train the workforce.

Notice of Privacy Practices

- Patients are provided with our **Notice of Privacy Practices** (NPP)
- The NPP informs our Patients:
  - How their health information will be used to provide services and bill for services
  - Of the uses and disclosures that we may make
  - Of their rights to access and amend their medical information
  - About our responsibilities with respect to PHI
  - How to ask questions or file a complaint

How We Protect Patient Information

- Notify patients how we will use and disclose their information (Privacy Notice)
- Train our workforce
- Well-defined policies and procedures
- Physical and technical safeguards
- Limit access to patient information, and only to what is minimally necessary to perform job
- Business Associate Agreements to safeguard patient information
- Monitor for compliance with laws, policies, and procedures
- Report and investigate actual or potential breaches of information
- Implement corrective actions, including discipline
- Privacy Officer, Security Officer, and Compliance Officer provide oversight and guidance

Improper Use or Disclosure

- Any unauthorized or improper Use or Disclosure of PHI must be promptly reported to the Privacy Officer.
  - Can be intentional or accidental
- The Privacy Officer is responsible for assuring a thorough investigation and imitating corrective actions.
- All improper uses and disclosures must be tracked and, in some cases, reported.

Examples:

- Employee gains access to records of a friend or family member
- Sending patient information to the wrong patient
- Password is shared and user accesses patient information

Breaches of Patient Information

- A "**Breach**" is any unauthorized acquisition, access, use, or disclosure of unsecured or unencrypted PHI.
- Common examples:
  - Lost or stolen unencrypted laptop, PDA, USB drives, CD-ROMs, DVDs, tapes, removable drives, etc.) that could contain patient information
  - Documents containing PHI discarded in trash
  - Access to paper or electronic PHI by an unauthorized party
  - PHI emailed outside of our network (use of personal email account should never be done)

Important: Report any actual or potential breach immediately to Privacy Officer Security Officer or your supervisor.

Your Responsibilities

1. Always safeguard patient information (oral, written, electronic)
2. Follow Minimum Necessary Rule - Is the information necessary for your job?
3. Refer complaints and patient requests immediately to Privacy Officer, Security Officer, or Compliance Officer
4. Report any actual or potential violations of policies and procedures and practices promptly to the Privacy Officer, Security Officer, or Compliance Officer
5. Be familiar with and adhere to our HIPAA Policies and Procedures

Where do you find more info?

1. Call or e-mail the Jeff Chesebro, Director of Operations or April Conant, Privacy Officer
2. Visit the Health and Human Services (HHS) Website and FAQ - http://www.hhs.gov/ocr/privacy/