HIPAA Training

Community Physical Therapy

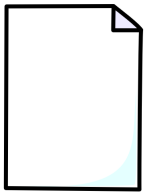
August, 2016

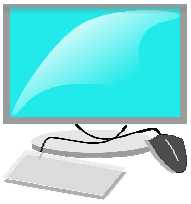
Objectives

- During this presentation you will learn:
  - About the Health Insurance Portability and Accountability **("HIPAA") Privacy and Security Rules;**
  - About the **HIPAA identifiers** that create **protected health information ("PHI");**
  - How to recognize situations in which confidential and protected health information can be mishandled;
  - About practical ways to protect the privacy and security of sensitive information, including PHI; and
  - That employees will be held responsible if they improperly handle confidential or protected health information.

Forms of Sensitive Information

- Sensitive Information exists in various forms…
  1) Printed
  2) Spoken
  3) Electronic





It is the responsibility of every employee to **protect the privacy of sensitive information** in ALL forms

Examples of Sensitive Information

- Social Security numbers
- Research data
- Computer passwords
- Individually identifiable health information
- Credit card numbers
- Driver's license numbers
- Personnel information


The improper use or disclosure of sensitive information presents the risk of identity theft, invasion of privacy, and can cause harm and embarrassment to those involved. Breaches of information privacy can also result in criminal and civil penalties for both CPT and those individuals who improperly access or disclose sensitive information, as well as disciplinary action for responsible CPT employees

HIPAA Privacy & Security Rules

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law designed to protect a subset of Sensitive Information known as protected health information (PHI).

In 2009, HIPAA was expanded and strengthened by the HITECH Act (Health Information Technology for Economic and Clinical Health). In January of 2013, the Department of Health and Human Services issued a final rule ("Final Rule") implementing HITECH's statutory amendments to HIPAA.

Section 1

HIPAA Privacy Rule Overview

Covered Entities Have a Duty to Protect PHI

A "covered entity" is any person or organization that furnishes, bills, or is paid for health care services in the normal course of business. Pursuant to HIPAA, individually identifiable health information is considered "protected health information," or PHI. CPT divisions that use or disclose PHI are governed by HIPAA requirements.

PHI defined

- PHI is generally defined as:
  - Any information that can be used to identify a patient – whether living or deceased – that relates to the patient's past, present, or future physical or mental health or condition, including healthcare services provided and payment for those services.

Employees may access PHI only when necessary to perform their job-related duties.

Any of the following are considered identifiers under HIPAA

- Patient names
- Geographic subdivisions (smaller than state)
- Telephone numbers
- Fax numbers
- Social Security numbers
- Vehicle identifiers
- Email addresses
- Web URLs and IP addresses
- Dates (except year)
- Names of relatives
- Full face photographs or images
- Healthcare record numbers
- Account numbers
- Biometric identifiers (fingerprints or voiceprints)
- Device identifiers
- Health plan beneficiary numbers
- Certificate/license numbers
- Any other unique number, code, or characteristic that can be linked to an individual.

Reality

Affinity Health Plan, Inc. discovered and reported to HHS that it had returned leased photocopiers to the leasing agents without first erasing the data contained on the copier hard drives that included PHI. The breach was estimated to have affected 344,579 individuals. Following an investigation, Affinity entered into a settlement agreement with HHS providing for a $1.2 million payment and a corrective action plan.

In general, HIPAA violations are enforced by the Department of Health and Human Services (HHS). However, pursuant to HITECH, state attorneys general are also permitted to bring civil actions and recover monetary awards that may be shared with harmed individuals.

Copiers: erase all data from hard drives.

Faxes: confirm authorization instructions; verify telephone numbers before faxing; when possible, use pre-programmed numbers.

Devices: encrypt; enable and use password protection.

reality

A court ordered Walgreens to pay $1.44 million to a customer whose PHI was impermissibly accessed and disclosed by a pharmacy employee. The employee suspected her husband's ex-girlfriend gave him an STD, looked up the ex-girlfriend's medical records and confirmed her suspicion, and shared the information with her husband. He then texted his ex-girlfriend and informed her that he knew about her STD.

Multiple state courts have ruled that HIPAA establishes a standard of care to which healthcare provider offices need to adhere, and liability for negligence may arise when that standard of care is breached.

Access Must be Authorized

An employee may only access or disclose a patient's PHI when this access is part of the employee's job duties.

Except in **very** limited circumstances, if an employee accesses or discloses PHI without a patient's written authorization or without a job-related reason for doing so, the employee violates CPT policy and HIPAA.

Unauthorized Access

It is never acceptable for an employee to look at PHI "just out of curiosity," even if no harm is intended (i.e., retrieving an address to send a 'get well' card).

It also makes no difference if the information relates to a "high profile" person or a close friend or family member – ALL information is entitled to the same protection and **must be kept private**.

These rules apply to all employees, including health care professionals as well as support staff.

Be aware that accessing PHI of someone involved in a divorce, separation, break-up, or custody dispute may be an indication of intent to use information for personal advantage, unless the access is required for the individual to do his job. Such improper behavior will be considered by CPT when determining disciplinary action against violators.

Breaches

- A breach occurs when information that, by law, must be protected is:
  - Lost, stolen or improperly disposed of (i.e. paper or device upon which the information is recorded cannot be accounted for);
  - "hacked" into by people or mechanized programs that are not authorized to have access, or
  - Communicated or sent to others who have no official need to receive it (e.g. gossip about information learned from a medical record).

reality

Facing the most severe level of HIPAA's criminal provisions – up to 10 years in prison and a $250,000 fine – because the violations involved access and use of PHI for personal gain, an employee af the Seattle Care Alliance agreed to plead guilty and serve a 16 month prison sentence and pay back both the impacted credit card companies and the patient from whom he stole the PHI. The employee accessed and used the [patient's name, birth date, and Social Security number from the medical record to fraudulently obtain four credit cards. He then charged about $9,000 in the patient's name.

Individual employees, and not just the "covered entities" for whom they work, are subject to HIPAA's sanctions.

Employees Must Report Breaches

- Part of your responsibility as a CPT employee is to **report privacy or security breaches involving PHI to your supervisor AND the HIPAA Privacy Officer, Nancy Rowan at 630-417-4245 or Nancy.rowan@cptrehab.com**

Employees, volunteers, students or contractors of CPT may not threaten or take any retaliatory action against an individual for exercising his/her rights under HIPAA or for filing a HIPAA report or complaint, including notifying if a privacy or security breach.

Penalties for Breaches

Breaches of the HIPAA Privacy and Security Rules have serious ramifications for all involved. In addition to sanctions imposed by CPT, such breaches may result in civil and criminal penalties.

Statutory and regulatory penalties for breaches may include:

Civil Penalties: $50,000 per incident up to $1.5 million per incident for violations that are not corrected, per calendar year

Criminal Penalties: $50,000 to $250,000 in fines and up to 10 years in prison

Quick Review

- Sensitive information exists in may forms: printed, spoken, and electronic.
- Sensitive information includes Social Security numbers, credit card numbers, driver's license numbers, personnel information, computer passwords, and PHI.
- There are a number of state and federal laws that impose privacy and security requirements
- Two primary HIPAA regulations are the Privacy Rule and the Security Rule.
- When used to identify a patient and when combined with health information, HIPAA identifiers create PHI.
- An employee must have a patient's written authorization or a job-related reason for accessing or disclosing patient information.
- Breaches of information privacy and security may result in both civil and criminal penalties, as well as CPT sanctions. Employees must report such breaches.

Section 2

HIPAA Privacy Rule Program Components

1) Patient Rights

HIPAA sets forth the following individual rights for patients.

- To receive a copy of the Entity's notice of Privacy Practices.
- To request restrictions and confidential communications of their PHI;
- To request corrections of their healthcare records.
- To file a complaint with a healthcare provider or insurer and the U.S. Government if the patient believes his or her rights have been denied or that PHI is not being protected.
- To receive notice of a breach of their unsecure PHI.

2) Minimum Necessary

Generally, a patient's authorization is required for the use or disclosure of PHI. When a use or disclosure of PHI is permitted, via patient authorization or otherwise, HIPAA requires that only the amount of PHI that is the MINIMUM NECESSARY to accomplish the intended purpose be used or disclosed.

Disclosure of PHI

HIPAA regulations permit use or disclosure of PHI for:

- Providing medical treatment
- Processing healthcare payments
- Conducting healthcare business operations
- Public health purposes as required by law

Employees may not otherwise access or disclose PHI unless:

- The patient has given written permission
- It is within the scope of an employee's job duties
- Proper procedures are followed for using data in research
- Required or permitted by law

Note: the Final Rule now protects PHI of a deceased individual for period of 50 years following the death of that individual

Quick Review

Under HIPAA, patients have the right to:

- Receive a copy of the Entity's Notice of Privacy Practices
- Receive a copy of their healthcare records in electronic form
- Ask for corrections to their healthcare records
- Receive an accounting of when and to whom their PHI has been shared
- Restrict how their PHI is used and shared
- Authorize confidential communications of their PHI to others
- Receive notice of a breach of their unsecured PHI
- File a HIPAA complaint

Section 3

HIPAA Security Rule

HIPAA Security Rule

The HIPAA Security Rule concentrates on safeguarding PHI by focusing on the confidentiality, integrity, and availability of PHI.

Confidentiality means that data or information is not made available or disclosed to unauthorized persons or processes

Integrity means that data or information has not been altered or destroyed in an unauthorized manner.

Availability means that data or information is accessible and useable upon demand only by an authorized person.

Mobile Devices

No employees are allowed to view or store PHI on a mobile device.

Password Control

Many security breaches come from within an organization and many of these occur because of bad password habits.

- Use strong passwords where possible (at least 8 characters, containing a combination of letters, numbers and special characters).
- Change your passwords frequently (45-90 days) to prevent hackers from using automated tools to guess your password.

Communications in Public Areas

- Be aware of your surroundings when discussing Sensitive Information, including PHI. Do not discuss Sensitive Information or PHI in public areas such as in cafeterias, departments or public places outside of work.

Use caution when conducting conversations in:

- Semi-private rooms
- Corridors
- Elevators and stairwells
- Open treatment areas.

Appropriate Disposal of Data

- Hard copy materials such as paper or microfiche must be properly shredded or placed in a secured bin for shredding later.
- Magnetic media such as diskettes, tapes, or hard drives must be physically destroyed or "wiped" using approved software and procedures. Contact the CPT HIPPA Officer for further information.
- CD ROM disks must be rendered unreadable by shredding, defacing the recording surface, or breaking.

Sensitive information and PHI should never be placed in the regular trash!

Physical Security

Equipment such as PCs, servers, mainframes, fax machines, and copiers must be physically protected.

- Computer screens, copiers, and fax machines must be placed so that they cannot be accessed or viewed by unauthorized individuals.
- Computers must use password-protected screen savers.
- PCs that are used in open areas must be protected against theft or unauthorized access.

Questions?

- If you have further questions, please contact Nancy Rowan, The CPT HIPPA Officer, at 630-417-4245 or at Nancy.rowan@cptrehab.com