The Health Insurance Portability and Accountability Act

Basic HIPAA Training

Who Needs Training and Why

- Employees who come in contact with "Protected Health Information" are Federally required to attend training
  - Departments listed later
- This presentation is designed to
  - Familiarize you with
    - HIPAA regulations
    - Our policies and procedures regarding protected health information (PHI)
  - Ensure Federal compliance
- Our policies are located in Human Resources

Summary of the Law

- To establish basic privacy and security protection of health information.
- To guarantee individuals the right to access their health information and learn how it is used and disclosed
- To simplify payment for health care.

What Exactly is HIPAA?

- Public Law 104-191 (1996)
- Overseen by: Department of Health & Human Services (HHS) and enforced by Office for Civil Rights (OCR)
- Regulations on:
  - Privacy of health information
  - Security of health information
  - Notification of breaches of confidentiality
  - Penalties for violating HIPAA

What is Protected by HIPAA?

- Protected Health Information (PHI)
  - Any Individually Identifiable Health Information (IIHI)
    - Created or received by a health care provider, health plan, or health care clearinghouse
    - Relating to the past, present of future physical or mental health or condition of an individual (including information related to payment for health care)
    - Transmitted in any form or medium—paper, electronic and verbal communications

What is Protected by HIPAA?

- Examples of PHI:
  - Medical charts
  - Problem logs
  - Photographs and videotapes
  - Communications between health care professionals
  - Billing records
  - Health plan claims records
  - Health insurance policy number

What is Protected by HIPAA?

- Health information protected if it directly or indirectly identifies someone.
  - Direct identifiers: individual's name, SSN, driver's license numbers
  - Indirect identifiers: information about an individual that can be matched with other available information to identify the individual.

Direct and Indirect Identifiers

1. Name
2. Geographic subdivisions smaller than a State
   - Street Address
   - City
   - County
   - Precinct
   - Zip Code & their equivalent geocodes, except for the initial three digits
3. Dates, except year
   - Birth date
   - Admission date
   - Discharge date
   - Date of death
4. Telephone numbers
5. Fax number
6. E-Mail Address
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web universal resource locations (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable data
18. Any other unique identifying number, characteristic, or code

What is Protected by HIPAA?

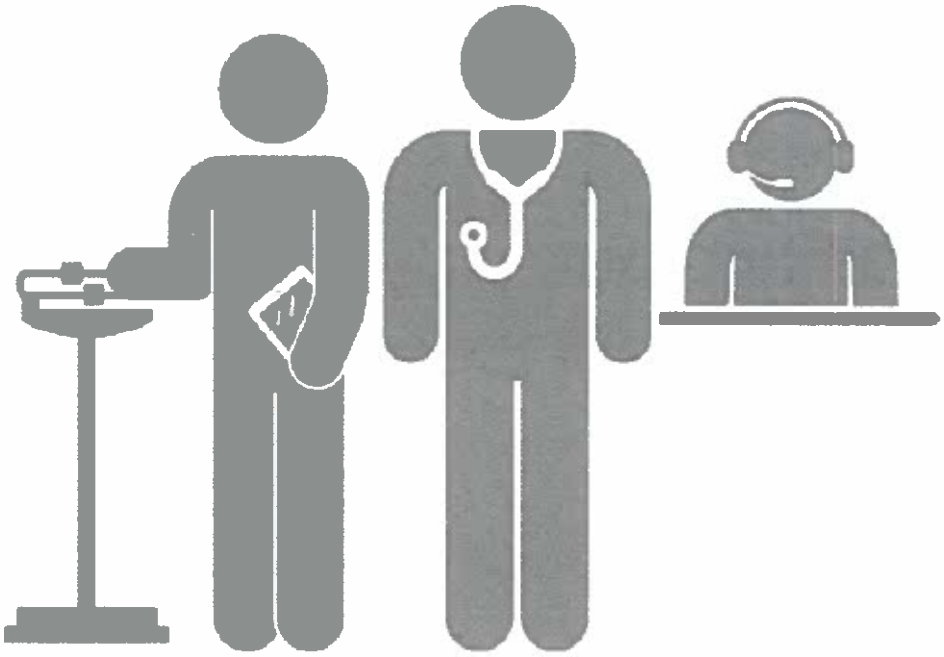
- If any direct or indirect identifiers are present, the information is PHI and subject to HIPAA protection.

- Information can be "deidentified" – but the Privacy Officer must review to ensure all direct and indirect identifiers have been properly removed.

Who is Subject to HIPAA?

CCH "covered entity" components:

- All employees, contracted individuals, and vendors of CCH



How HIPAA Protects PHI

- Limits who may use or disclose PHI.
- Limits the purposes for which PHI may be used or disclosed
- Limits the amount of information that may be used or disclosed (Minimum Necessary rule)
- Requires use of safeguards over how PHI is used, stored and disclosed

Who May Use PHI?

- You are only given access to PHI if you need it in order to perform your job
- You must agree to protect the confidentiality of the information
- You are subject to discipline if you violate CCH's privacy policies and procedures.

How May PHI May Used?

- General Rule:
  - Workforce members may use or disclose PHI **only** for permitted uses without an individual's specific written authorization.

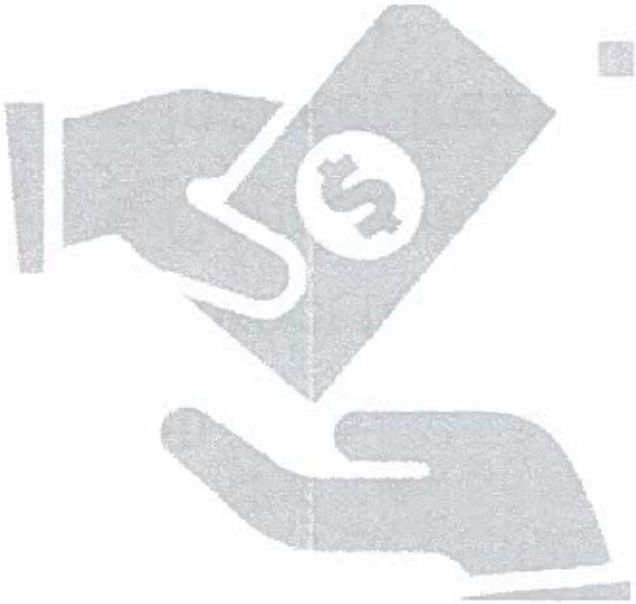
Permitted Uses For PHI

- "TPO"
  - Treatment
  - Payment
  - Health care operations
- Specified public policy exceptions (public health and law enforcement)
- Any other use requires individual written authorization

Treatment

- Providing, coordinating & managing health care
- Includes:
  - Direct treatment of patient
  - Consultation among health care providers
  - Indirect treatment (for example, laboratory testing)
  - Patient referral from one provider to another

Payment



- Activities by a health care provider to obtain reimbursement for health care
  - Includes: billing, eligibility/coverage determination, medical necessity determinations
- Activities by health plan to pay claims

Health Care Operations

- Activities directly related to treatment and payment -- such as credentialing, auditing, utilization review, quality assessment, training programs
- Supporting activities, such as computer systems support
- Administrative and managerial activities, such as business planning, resolving complaints, and complying with HIPAA.

Minimum Necessary Rule

- The use or disclosure of PHI is limited to the **minimum amount necessary** to accomplish the purpose
- Does not apply to treatment
  - Can use whatever information you think you need for treatment purposes
- Any other purpose, must consider: what is the minimum amount of information needed to perform the task?

Safeguarding PHI

- People consider health information their most confidential information, and we must protect it accordingly
  - Do not access PHI that you do not need
  - Do not discuss PHI with individuals who do not need to know it.
  - Do not provide PHI to anyone not authorized to receive it
- Misusing PHI can result in discipline, legal penalties and loss of trust

Safeguarding PHI

- When using PHI, think about:
  - Where you are
  - Who might overhear
  - Who might see

Safeguarding PHI

- Avoid:
  - Discussing PHI in front of others who do not need to know.
  - Leaving records accessible to patients or others who do need to see them
  - Positioning monitors where others can view them
  - Using printers located in public or unsecured areas

Safeguarding PHI

- Follow safe practices for your computer system ID and password
  - Use strong passwords
  - Keep your use ID and password confidential and secure
    - if you need to write it down, keep it in your wallet
  - Do not allow anyone else to access the computer system under your ID

Safeguarding PHI

- Only access electronic PHI from a workstation certified for HIPAA or PHI access.
- Only save electronic PHI to a HIPAA-designated server
  - Do not save on computer's hard drive, CD, floppy disk, USB thumb drive or other removable media
- Do not leave computer station unattended without locking it first

Safeguarding PHI

- Do not engage in risky practices with computers used to access PHI
  - Do not surf the internet
  - Do not open attachments to e-mail unless from a trusted source
  - Do not install applications unless approved by CCH IT Department

Safeguarding PHI

- Do not unnecessarily print or copy PHI
- When faxing PHI, use a fax cover page
- Do not send PHI in email unless first cleared by your supervisor
- Dispose of PHI when it is no longer needed
  - use shredding bins for paper records
  - When retiring electronic media used to store PHI, ensure the media is “cleansed” according to IT Department standards

Safeguarding PHI

- Report unusual activity to your supervisor immediately
  - You observe questionable practices
  - You find PHI in inappropriate areas
  - You suspect unauthorized use of your user ID/password
  - A patient/health plan participant complains to you about a privacy issue

Why should we care about the HIPAA rules?

CCH

- Disciplinary action up to and including termination of employment

Civil Penalties

- Up to $1.5 million per year per violation

Criminal Penalties

- Up to $250,000, imprisonment of up to ten years, or both

Lawsuits

- Invasion of privacy/negligence

REMEMBER!

HIPAA can be summarized by saying "Need to know!"