HIPAA Security, Privacy and Breach of PHI Training

What is HIPAA?

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

Comprehensive federal legislation regarding health insurance which is comprised of four key areas:

1. **Portability**
    - Created to ensure access to health coverage and allows for continuity in health coverage: Protects health insurance coverage for workers and their families when they change or lose their jobs
    - Prevents denial due to a pre-existing condition(s): Prevents discrimination against employees and their families due to a pre-existing medical condition(s)

2. **Accountability**
    - Healthcare fraud is a federal crime
    - Fines and/or jail time may apply
        - Civil penalty for inadvertent violation = fines of $100/ per incident up to $25,000/per year for each similar offense
        - Criminal penalties could equal fines up to $250,000 and/or jail time, and increase with the degree of the offense
    - Individuals and organizations face sanctions

3. **Privacy**
    - Provides the first comprehensive federal protection for the privacy of an individual's health information, verbal, written, or electronic
    - Gives individuals more control over their health information, and sets boundaries on the use and disclosure of their health information
    - HIPAA's privacy rule focus on the safeguarding of patients' **P**rotected **H**ealth **I**nformation (aka Personal Health Information) or PHI
    - All other uses or disclosures require the individual's written authorization or must be "de-identified"
    - Disclosures must be limited to the amount of PHI reasonably necessary to achieve the purpose of the disclosure ("minimum necessary")

4. **Security**
    - Establishes safeguards that must be achieved to protect the privacy of PHI
    - Holds violators accountable with civil and criminal penalties that can be imposed if they violate an individual's privacy rights
    - Secured, locked containers must be used to dispose of any paper copies of PHI, or items must be shredded immediately

5. **Electronic Transactions**
    - Standardizes electronic health care transactions: The following functions are subject to the standardized electronic formats and codes set requirements:
        - Claims
        - Status/inquiry
        - Referrals
        - Authorizations
        - Enrollment/disenrollment
        - Premium Payments
        - Eligibility
        - Billing
    - Faxing PHI:
        - Avoid faxing PHI information unless it is urgent
        - When sending a fax that contains PHI:
            - ✓ Confirm the fax number with the recipient and call to notify the recipient that the fax was sent
            - ✓ Request a verbal verification from the recipient that the fax was received
            - ✓ In the event of a misdirected fax, make sure that it is returned or destroyed
            - ✓ Include a fax cover page (found on Pulse SharePoint), that includes recipient's name, phone and fax number, date and time of fax, number of pages transmitted, and the following warning at the bottom:

        "The information contained in this facsimile is PRIVILEGED AND CONFIDENTIAL information intended only for the use of the individual or entity named above. If you have received this communication in error, please notify us immediately by phone and return the original facsimile to us at the address above via the United States Postal Service."

        - When receiving a fax that contains PHI:
            - ✓ Place faxes that contain PHI in a secure location, do not print and leave them so they are accessible
            - ✓ As with all PHI handle and store in a secure manner

- Workstations:
    - All employees are required to follow the "Clean Desk Policy"
        - ✓ Maintaining a neat work environment during business hours
            - ♦ Only keep items on your desk you need for the day
            - ♦ Non-essential items should be stored away when not in use
        - ✓ Refrain from cluttering the work area with Post-It or other handwritten notes displaying sensitive information
        - ✓ Discard sensitive items you no longer need, by either shredding it or placing it in the secured bins for shredding
        - ✓ Remove or secure any proprietary or sensitive information when you leave your desk. You should make a quick check prior to leaving your area and secure this information in your desk
        - ✓ When you leave your desk in the evening remove all sensitive documents, or lock your office

    - Keep files, records and other documents that contain PHI in drawers or file folders when not in use
    - CD's, diskettes, flash drives, or any other electronic storage device that contains PHI or other confidential information must be properly stored or destroyed when no longer needed. Simply deleting information may not be enough to ensure that information cannot be retrieved and improperly disclosed. Electronic media must be submitted to the hardware department for destruction

    - Employees may not send PHI through email without encrypting.

6. **Phone Call Verification**: (RCM department)
    - It is critical that callers be identified with reasonable certainty before any PHI is disclosed over the phone
    - The following process must be used to identify the caller:
        - Name of the subscriber
        - Member/certificate number
        - Address, including street, city, state and zip code
        - Home or work phone number
    - Member's legal representative:
        - Must provide a fax or mail appropriate proof of representation (Power of Attorney or Guardianship documents)
    - Agent or Broker on behalf of the member
        - Request their agent/broker number
        - Request responses to the questions listed above, if at least 2 of the responses match the member information, you may provide assistance

HIPAA TERMS

- **Covered Entity –** Those entities who are subject to HIPAA:

- Health Plans: Includes HMO's, health insurers, self-insured group health plans, Medicare, and Medicaid
- Healthcare Clearing Houses: An entity that processes health information from a healthcare provide to a payer
- Healthcare Providers who transmit any health information electronically in connection with certain transactions

- **Protected Health Information (PHI) –** made up of 2 components – Health Information and individually Identifiable Health Information. PHI is a culmination of data that is specific to individual patients.
    - Health Information: information that relates to the past, present, or future physical or mental health of the individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare. The data can be used to identify:
        - ✓ A patient
        - ✓ A patients health
        - ✓ Healthcare services received
    - Individually Identifiable Health Information is a subset of Health Information, and is information that can be used to identify the individual:
        - ✓ Name
        - ✓ Address
        - ✓ SSN
        - ✓ Medical record number
    - Minimum necessary for use and disclosure of PHI
        - ✓ Employees must limit their access of PHI to the minimum amount that is needed to perform a job function.
        - ✓ Notify your manager if you believe that in the course of your duties, you are approached with a non-routine situation.

- **Business Associate –**is a person or entity, that acts on behalf of a Covered Entity or provides services to the Covered Entity, and who has access to a Subscriber's or Member's PHI.

- **Treatment, Payment and Healthcare Operations (TPO) –** Uses and Disclosures by a Covered Entity of a Member's PHI for purposes of treatment, payment or healthcare operations do not require authorization from the member.

    - Examples of items that fall under TPO are:
        - ✓ Processing and payment of claims
        - ✓ Communications with providers about a member
        - ✓ Business management and general administrative activities

- **De-Identified**- PHI that does not identify the member, and there is no reasonable basis to believe such information can be used to identify the member. In order to be "de-

identified" all identifiers, including but not limited to name, address, social security number, phone number, birth date, fax number, e-mail address, etc must be removed.

What is a Security Breach?

An act from outside an organization that bypasses or contravenes security policies, practices, or procedures. A similar internal act is called security violation.

Step 1 – Discovery

- A breach of PHI will be deemed "discovered" as of the first day Pulse knows of the breach or, by exercising reasonable diligence, would or should have known about the breach.
- If a potential breach is discovered; it is very time sensitive and must be immediately reported.

Step 2 – Internal Reporting

- If you believe that a potential breach of PHI has occurred, you must immediately notify you supervisor, who will notify the HIPAA Compliance Officer (HCO).
- Please provide all of the information you have available to you regarding the potential breach, including names, dates, the nature of the PHI potentially breached, the manner of the disclosure (fax, email, mail, verbal), all employees involved, the recipient, all other persons with knowledge, and any associated written or electronic documentation that may exist.
- Notification and associated documentation may itself contain PHI and should only be given to the HCO.
- Please do not discuss the potential breach with anyone else, and do not attempt to conduct an investigation.

Step 3 – Investigation

- Upon receipt of notification of a potential breach the HCO shall promptly conduct an investigation.
- The investigation shall include interviewing employees involved, collecting written documentation, and completing all appropriate documentation.
- The HCO shall retain all documentation related to potential breach investigations for a minimum of six years.

Step 4 – Risk Assessment and recommendation

After the investigation is complete, the HCO will perform a Risk assessment. The purpose of the Risk Assessment is to determine if a use or disclosure of PHI constitutes a breach and requires further notification to the Covered Entity. The HCO

shall appropriately document the Risk Assessment and make a recommendation on whether notification to the Covered Entity of the potential breach would be prudent.

A "reasonable judgment" standard will be applied to the Risk Assessment, which shall be fact specific, and shall include consideration of the following factors:

- Did the disclosure involve Unsecured PHI in the first place?
- Who impermissibly used or disclosed the Unsecured PHI?
- To whom was the information impermissibly disclosed?
- Was it returned before it could have been accessed for an improper purpose?
- What type of Unsecured PHI is involved and in what quantity?
- Was the disclosure made for any improper purpose?
- Is there the potential for significant risk of financial, reputational, or other harm to the individual whose PHI was disclosed?
- Was immediate action taken to mitigate any potential harm?
- Do any of the specific breach exceptions apply?

Step 5 – Final Determination

The HCO and Executives of Pulse shall have final authority to determine whether a breach of unsecured PHI occurred and what, if any further action is warranted.

Step 6 – Notification to Covered Entity

In the event it is determined that notice to the Covered Entity is warranted, the HCO shall promptly prepare and transmit a Covered Entity ("CE") Notice.

- **Content: The CE Notice shall include:**
    - Identification of each individual whose Unsecured PHI is believed to have been breached, the date of the disclosure, the facts and the circumstances surrounding the disclosure, and all associated documentation.
    - The CE Notice shall include all other available information known to Pulse that the Covered Entity will be required to include in its own Notice to the individual(s).
    - If additional information regarding the breach is later discovered by Pulse, that information will be promptly provided to the Covered Entity.
    - The CE Notice shall be sent first class mail, return receipt requested, and the receipt and a copy of the CE Notice shall be kept with related documentation.

- Upon receipt of the CE Notice from Pulse, it is the obligation of the Covered Entity to notify affected individuals, HHS, and/or the media unless otherwise specifically agreed upon by contract.

- **Timing of Notification**

  Pulse shall notify the Covered Entity "without unreasonable delay" but no later than 60 days after discovery of the breach.

  - Unjustified delay – If it appears to the HCO that the investigation will not be completed within a reasonable time, the Covered Entity will be notified before completion of the investigation.

  - Law Enforcement delay – A delay in notification is permissible if a law enforcement official states that a breach notification would impede a criminal investigation or cause damage to national security.
    - In that event, the law enforcement statement must be in writing and must specify the length of the delay required.
    - If the request for a delay in notifications oral, Pulse must document the statement and request written confirmation within 30 days.

Step 7 – Documentation

All phases of the process must be documented in detail on a case-specific basis, in a manner sufficient to demonstrate that all appropriate steps were completed. All supporting documentation associated with the potential breach shall be kept on file for a period of six years.