Health Insurance Portability and Accountability Act (HIPAA) Training

HEALTH NETWORK ONE

What is HIPAA

HIPAA is the acronym for the Health Insurance Portability & Accountability Act of 1996.

- It is a law that provides protection standards for patient confidentiality and its health information. It also provides security standards for electronic systems and for the transmission of health information in electronic format.

HIPAA's Title II aims for "Administrative Simplification" of the health insurance system in three ways:

- Electronic data sent from a doctor or hospital to an insurance payer, or delegated representative must be in approved electronic format.
- Data systems must be secure, so information will not get into the wrong hands
- People who handle patient health information must protect the privacy and rights of the patients.

Who is covered by HIPAA

- Health Plans
- Healthcare Providers and Institutions: physicians, hospitals
- Health care Clearinghouses: Central Institutions that establish transactions electronically.
- HIPAA requires that covered entities use or disclose PHI in a limited way. Under the HIPAA minimum necessary standard, HIPAA-covered entities are required to make reasonable efforts to ensure that access to PHI is limited to the minimum necessary information to accomplish the intended purpose of a particular use, disclosure, or request.

Protected Health Information (PHI)

- PHI is individually identifiable health information collected from an individual, created or received by a covered entity and
    - Is related to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or to the past, present, or future payment for the provision of health care to an individual;
    - That identifies the individual or could identify the individual.
    - That could be transmitted or maintained electronically, or through any other medium.
- Protected health information (PHI) has two components:
    - Health information and Information about a specific, identifiable person
- There are rules about how PHI may be used so it is important to know what they are and apply them consistently!

Example of an individual's Identifiers

- Remember, PHI only applies to Individually Identifiable Health Information; both components must be present.
- Information that can be used to identify, contact, or locate an individual.
  - Names
  - Geographic Data
  - All elements of dates
  - Telephone Number
  - Fax Numbers
  - Email address
  - Social Security Number
  - Medical Record Numbers
  - Health Plan Beneficiary Numbers
  - Account Numbers
  - Certificate/License Numbers
  - Vehicle identifiers and serial numbers including license plates
  - Device Identifiers and Serial Numbers
  - Web URLs (Uniform Resource Locater)
  - Internet Protocol Addresses
  - Biometric Identifiers (e.g. retinal scan, fingerprints)
  - Full face photos and comparable images
  - Any unique identifying number, characteristic or code

PHI Formats

- PHI can exist in written, oral, or electronic format.
- Examples of verbal PHI:
    - When we talk to doctors and office staff.
    - When we deal with pharmacies or insurance companies.
    - When we talk to patients themselves.
    - When we deal with inquiries from government officials.

Examples of an Individual's Health Information

- Information that describes a medical condition, such as a diagnosis or diagnosis code.
- Information that identifies a medical procedure or treatment, like a procedure code.
- A prescription
- A medical chart
- Vital signs or medical test results
- The record of a doctor's appointment
- A medical claim form
- A patient's eligibility information, membership in a health plan, or insurance information.

PHI Safeguards

- The improper use or disclosure of sensitive information presents the risk of identify theft, invasion of privacy, and can cause harm.
- Breaches can also result in criminal and civil penalties for both the ACE and those individuals who improperly access or disclose sensitive information.

We must safeguard all patients' PHI whether it is in written, electronic, or oral form. The following pages cover some of the methods that we should use to Safeguard PHI, including these:

- Oral, Telephone and Voice Mail Safeguards
- Mail Safeguards
- Fax Safeguards
- Computer Safeguards
- E-Mail Safeguards

PHI Safeguards (Cont.)

Oral, Telephone/Voice-mail safeguards:

- Do not talk about an individual's PHI in public areas within the workplace, such reception area or break room, or outside of the workplace.
- Do not play back voice mail messages with the speakerphone button on.

Mail Safeguards:

- Make sure that open mail containing PHI is not left sitting in a public area.

Fax Safeguards:

- Always use a cover sheet that includes a confidentiality statement.
- Double-check the fax number you are sending the information to.
- Whenever possible, use a fax directory or call the recipient immediately before and after sending the fax, to ensure that it is expected, and is picked up promptly.

PHI Safeguards (Cont.)

E-Mail Safeguards:

- Emails containing PHI must be sent secured and encrypted.
- As an information security measure, do not use your personal emails to receive or share the confidential and protected health information of our members.
- Please follow the guidelines below when sending PHI via email:
  - Include the minimum necessary of PHI to complete the purpose of the message.
  - Ensure that the address of the recipient is correct and that the document included in the message (if any) is correct.
- Encrypt all emails to external persons outside the company.
- Do not send PHI in email unless email is encrypted.
- Never put any PHI in the subject line of emails.

PHI Safeguards (Cont.)

Computer Safeguards: Password Management

- Create a unique, strong password or PIN for each account or device and keep your credentials secure.
    - Don’t use personal or easy-to-guess information when creating a password.
    - Make a password complex by adding numbers, multi-case letters (upper and lower), and symbols.
    - Mix numbers into the center of your password.

Password Policy Guidelines

- A minimum of 8 characters long and contain at least a mix of THREE of the following FOUR Properties
    - Lowercase letters (a-z)
    - Uppercase letters (A-Z)
    - Numbers (0-9)
    - Symbols (!”Â£$%^&*)
- Strong password example: B5rCo5#44E4, M1c3nm3n,Goo*stov

PHI Safeguards (Cont.)

Password Management Don’ts:

- Reveal your password to anyone.
- Share your password to your supervisor, Service Desk employee, or a family member.
- Allow anyone else to use your User ID and password.
- Reveal your password on questionnaires or security forms.
- Store your passwords in a file on any computer system.
- Re-use the same password
- Write your passwords down and store them anywhere in your office.
- Place your passwords into email messages or other forms of electronic communication.

Remember: Change all passwords frequently and keep your passwords secret.

Privacy Rule

Purpose:

- Protects the confidentiality of PHI in all formats (paper, verbal, and electronic).
- Grants the members understanding and control of how their PHI is used.
- Ensures that PHI is used for health purposes only.
- Establishes that PHI can only be disclosed for treatment, payment, or health care operations (TPO) or with the consent (valid authorization) of the individual.
- Establishes individual's rights with respect to their health information.
- Establishes the notification process for HIPAA Breaches.

What does the Privacy Rule require providers and health plans to do?

- Notify the individuals about their privacy rights and how their information can be used and disclosed.
- Adopt and implement processes in their practices, hospitals, or plan.
- Train their employees to understand the privacy processes.
- Designate a responsible person to ensure that the privacy processes are applied and followed.
- Secure patient records contain PHI so they aren't readily available to those who don't need to see them.

Security Rule

Purpose:

- Protects patients' electronic PHI (ePHI)
- Ensures the confidentiality, integrity, and availability of all ePHI created, received, maintained, or transmitted
- Protects against impermissible uses or disclosures of ePHI that are reasonably anticipated

What does the Security Rule require providers and health plans to do?

- Develop reasonable and appropriate security policies
- Ensure the confidentiality, integrity, and availability of all ePHI you create, get, maintain, or transmitted
- Identify and protect against threats to ePHI security or integrity.
- Protect against impermissible uses or disclosures.
- Analyze security risks in your environment and create appropriate solutions
- Review and modify security measures to continue protecting ePHI in a changing environment
- Ensure employee compliance

Permitted Uses and Disclosures of PH145 CFR 164.502

The use and disclosure of PHI is permissible:

- For TPO: treatment, payments and healthcare operations.
- When a valid written authorization exists from the individual, authorizing the use and disclosure of his/her PHI to a third party (representative).
- To a family member or friend that is involved with the medical care or payment of the medical care of the individual and the individual has the opportunity to accept/object the use or disclosure.
- For health oversight activities.
- When it is required by law.
- For law Enforcement Purposes or National Security.
- For judicial and administrative proceedings.
- For Forensic Pathologist, Judges and Funeral Directors.
- To avert a serious threat to health or safety .
- Among others.

Accounting for Disclosures

- We must be able to tell patients if their PHI is given to other parties.
- We are not required to account for disclosures if the patient authorized the disclosure.
- The Office of the Privacy Official handles all these requests.

Reporting Privacy or Security Concerns

The following require immediate notification to the HIPAA Team at:
HIPAA@healthsystemone.com

- Sensitive, confidential or proprietary information (excluding PHI) is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties.
- Unauthorized use of the ACE' information system has taken place, or is suspected of taking place.
- Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed.
- Any and all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like which may be indicative of a computer virus infection or similar security problem.

Unintended use or disclosure of PHI or any HIPAA breach must be reported as soon as it is known to the email address above.

Privacy Breach Assessment

- The use or disclosure not authorized of PHI for HIPAA is presumed to be a breach unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised.
- Risk Analysis to determine if the PHI was compromised can include:
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
  - The unauthorized person who used the PHI or to whom the disclosure was made.
  - Whether the PHI was actually acquired or viewed.
  - The extent to which the risk to the PHI has been mitigated.

Examples of PHI Breach

- Unauthorized disclosure of PHI to a third party in paper or electronically (without a valid authorization).
- Lost, stolen or improper disposition of documents with PHI.
- Access to PHI when its not required for job duties.
- Access of PHI for an improper purpose by an unauthorized person.
- Send unprotected PHI outside the company (e.g. without encryption) and an unauthorized person has access to the information.
- Discuss PHI (such medical results, diagnosis and conditions) with the individual in public areas, where others can hear the conversation.
- Disclose PHI in a manner not permitted by HIPAA.

Treatment, Payment, Operations

HIPAA allows the office to do routine things with PHI. These routine things are summarized with the terms “Treatment, Payment and Operations” (TPO).

Treatment: All that is done as part of a patient’s medical care, such as:

- Health care appointments
- Lab testing
- Filling a prescription at the drug store
- Referring a patient to a counselor or specialist
- Reminding a patient about health care or appointments
- Participating in the prior approval process with doctors and hospitals to determine the appropriate treatment for a patient.

Treatment, Payment, Operations (Cont.)

Payment: All the activities related to paying for a person's health care, such as:

- Determining if an individual is eligible for a program.
- Coordinating claims with other payers.
- Reviewing medical records to decide if a procedure should be paid.
- Verifying insurance eligibility or coverage limits.
- Discussing claims with providers in person, by correspondence, or on the phone.
- Sending a remittance document to providers identifying the patients and procedures that are being paid and denied.

Treatment, Payment, Operations (Cont.)

Operations: All the activities done to operate divisions that may provide health care services, such as:

- Auditing
- Rate-setting for contracted providers
- Policy determination for programs
- Fraud and abuse detection
- Employee training
- Legal services
- Contract provider assignment activities

Patient Authorization

We must have written authorization from the patient, or the patient's personal representative, before we can use or disclose PHI for any purpose, with these exceptions:

- Treatment, Payment, and Health Care Operations, or
- As permitted or required by law without authorization

Psychotherapy notes and HIV/AIDS-related data are especially sensitive. **DO NOT RELEASE** them without notifying the Privacy Official.

Individual's Rights under HIPAA

- **Right of Access:** The Privacy Rule required Covered Entities (e.g. health plans) to provide individuals, upon request, the right to inspect or obtain a copy of their PHI in one or more "designated record sets" maintained by or for the covered entity. (45 CFR 164.524)
    - A covered entity must act on a request for access no later than 30 days after receipt of the request. An extension of 30 days can be made notifying the individual making the request.
    - The plan can send a copy of the PHI directly to a third person designated by the individual, if such request is made in writing, providing the name and address of the third Party.
- **Right to Amend or Correct PHI:** Individuals have the right to have covered entities amend their PHI in a designated record when that information is inaccurate or incomplete. (45 CFR 164.526)
    - Covered entities must respond to a request for an amendment within 60 days.

Individual's Rights under HIPAA (Cont.)

- **Right to Disclosures of Accounting of PHI**: Individuals have a right to an accounting of the disclosures of their PHI by a covered entity or the covered entity's business associates except the disclosures made for one the following reasons:

    - Treatment, payment, or healthcare operations (TPO), pursuant to a valid authorization, to the subject of the information, for national security purposes, to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody, incident to otherwise permitted or required uses or disclosures. (45 CFR 164.528)

    - Request of an accounting of disclosures of PHI must be acted on no later than 60 days after receipt of the request. An extension of 30 days can be made notifying the individual making the request.

Individual's Rights under HIPAA (Cont.)

- **Request of Restrictions:** Individuals have the right to request that a covered entity restrict uses or disclosures of PHI for treatment, payment or health care operations (TPO), disclosures to persons involved in the individual's health care or payment for health care, or disclosures to notify family members or others about the individual's general condition, location, or death. (45 CFR 164.522 (a)).
    - The plan is under no obligation to agree to requests for restrictions. However, if the plan does agree, it must comply with the agreed upon restrictions, except for purposes of treating the individual in a medical emergency and the restricted PHI is needed to provide the emergency treatment.
- **Confidential Communications:** The plan must permit members to request an alternative means or location for receiving communications of PHI by means other than those that the plan typically employs, (45 CFR 164.522 (B))
    - For example: A member can request that the health plan communicate with the individual through a designated address or phone number.
- Health Plans must accommodate reasonable requests if the individual indicates that the disclosure of all or part of the PHI could endanger the individual.

Releasing a minor's PHI to a parent

- One of the permitted releases without authorization applies to releasing the PHI of a minor child to their parent(s).
- You can answer a parent's questions about his/her minor (age 17 and under) child without requiring a written consent. However, as in all situations, be helpful but provide only the information that is requested, and nothing more.

PHI of a Deceased Individual

- The Final Rule limits the period of protection of PHI of a deceased individual to 50 years. This is a protection term, not a record retention period.
- The Final Rule also allows the disclosure of PHI of a deceased individual to a family member or close friend who was involved in the individual's care or payment of healthcare prior to the individual's death, unless doing so is inconsistent with any prior expressed preferences of the individual.

Minimum Necessary Rule

HIPAA requires that when you use or disclose PHI, you must follow the “Minimum Necessary Requirement”. This means that you must use or disclose only the information requested or needed. Applies to all forms of communication: paper, fax, oral, and electronic communication of PHI.

- The minimum standard requirement does not apply to:
  - Disclosures to, or requests, by a health care provider for treatment purposes.
  - Disclosures to the individual who is the subject of the information.
  - Uses or disclosures made pursuant to an individual’s authorization.
  - De-identified information.
  - Uses or disclosures required by law.
  - Among others.

Additional Requirements for Privacy

- Substance Abuse Information
- Mental Health related data
- HIV-AIDS related information

Requirements for confidentiality of substance abuse related information have been in place since the early 1970's. The principles established then were expanded to include all identifiable heath information with the enactment of HIPAA.

Currently, these three categories of PHI are emphasized in the Privacy practices that are recommend for all covered entities because these health issues may carry additional social repercussions to an individual.

Penalties for Non-Compliance

As covered entities, we are required to sanction members of our workforce (employee, contractor, etc.) and business associates, up to termination.

- There are legal penalties — fines and even jail time — for people who violate HIPAA rules.
    - Civil penalties imposed by the Office of Civil Rights
    - Criminal penalties imposed by the Department of Justice
        - These penalties apply to managers and the company in general if we fail to establish policies and provide training to staff.
        - The penalties apply to staff if you ignore the law, especially if you deliberately give someone's private information to another person that is not supposed to see it.

Remember: Management of PHI

- Follow the procedure for the proper disposal of sensitive information using locked recycling drop boxes.
- Keep laptops, smartphones, USBs and any other memory or document containing PHI in a secure place.
- Never leave PHI on your desk in plain sight.
- Make sure not to leave documents that contain PHI in printers or fax machines.
- Use strong passwords. Keep your user ID and passwords confidential and secure. Never share your password or user name (User ID).
- Do not access PHI that you do not need to access.

Wrap up! Hippa@healthsystemone.com

- PHI & Sensitive information exists in many forms: printed, spoken, and electronic.
- PHI & Sensitive information includes Social Security numbers, credit card numbers, driver's license numbers, and computer passwords.
- 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.

Report ethical, compliance, fraud, waste, and abuse violations in a confidential manner at:

SIU@healthsystemone.com | 1-866-321-5550


HEALTH NETWORK ONE