HIPAA Privacy and Security Training

Provided By the Office of Audit, Compliance, and Privacy

Learning Objectives

- Explain basic rules for using and disclosing *protected health information,* or PHI.
- Define the rights afforded to patients under HIPAA.
- Identify the requirements for safeguarding PHI.
- Identify your role in protecting the privacy and security of PHI and other sensitive information.
- Specify the consequences associated with non-compliance.
- Appropriately report privacy and security incidents.

Don't be the Weakest Link!

Welcome to Penn Medicine. We appreciate the contributions you make to our work and to our community. One of the key values of Penn Medicine is protecting patient privacy. Every member of the workforce must work together to ensure the best in patient care and protection. We are only as strong as our weakest link and we rely on you – and everyone else in Penn Medicine – to meet our goals and be true to our values.

What are HIPAA and HITECH?

- HIPAA is a federal law enforced by the Department of Health and Human Services that regulates health care services.
- The HIPAA Privacy and Security Rules regulate the use, collection, sharing, and protection of patient information while also providing patient rights.
- HITECH significantly enhanced the requirements of the Privacy and Security Rule by creating new obligations and expanding others.
- These rules protect Protected Health Information (PHI), which includes information that:
    - Can reasonably identify an individual
    - Is created or received by Penn through its operations of providing health care
    - Relates to the past, present, or future physical or mental health or condition of that individual.

Using and Disclosing PHI

- Under HIPAA, it is permissible to share PHI consistent with the signed patient authorization form.
- There are certain cases where patient authorization is not required under HIPAA, the most common being:
    - **Treatment** of a patient
    - Obtaining **Payment** for services
    - For **Healthcare Operations** purposes, such as administrative activities, business management, and planning and quality effectiveness.
- However, in these cases, there may be circumstances that still require authorization in writing, such as. taking photos or video of the patient.
- There are specific rules regarding research that apply under HIPAA, that usually require written patient authorization, as well as Institutional Review Board approval.
- Other uses and disclosures that are allowed without patient authorization include:
    - Marketing: Providers may communicate with a patient about products and services to assist in their care, but communications paid for by third parties require patient authorization.
    - Fundraising: Certain PHI may be used for fundraising and development purposes. All fundraising activity must be coordinated through the Development Office.
    - Public Health Purposes: PHI may be shared to public health authorities for authorized public health purposes.
    - Health Care Oversight: Governmental agency oversight activities that require access to PHI are allowed under HIPAA so long as the activities are within the scope of the agecy's authorized function.
    - Law Enforcement Purposes: HIPAA regulates how much PHI we may share with law enforcement depending on the situation. If you receive a request for PHI from a law enforcement official, you must contact your Entity Privacy Officer. If you receive a subpoena or court order requesting PHI, the Office of General Counsel must be involved.
    - Emergency Circumstances: There may be cases when you need to share PHI to prevent or lessen a serious and imminent threat to the health and safety of a person or the public. This is allowable under HIPAA.
    - Friends and Family: PHI may be shared with a patient's friends and family if they are involved in the patient's care. We at Penn Medicine must exercise professional judgment in the circumstances to reasonably determine that the patient does not object to the disclosure.
- The **Minimum Necessary Rule** limits access to PHI to a "need-to-know" basis only. Access is granted only to the information required to perform your job function. This rule does not apply in circumstances of sharing information for treatment purposes.

- **Clinical systems will be monitored to ensure that employees accessing PHI of patients is appropriate – meaning, part of their job functions**. Employees who access PHI for personal or other, non-work-related purposes, will face discipline, up to and including termination.

Additional Requirements

- Business Associates are vendors that perform functions for or on behalf of UPHS that involve the use, access to, or maintenance of PHI. They are directly responsible for HIPAA compliance and must sign Business Associate Agreements that outline the requirements for protection of data.
- Patients also have rights under HIPAA and HITECH, which include the following:
    - Access and review their own medical information when properly requested
    - Request an amendment to information they believe is inaccurate
    - Include a statement in their own record (if they disagree with a clinician's documentation)
    - Request an accounting record of certain disclosures
    - Request confidential communication by reasonable means
    - Request certain restrictions of sharing PHI.

Information Security

- Secure configuration is required on all devices that may access Penn Medicine data. Such protections include operating system patches, antivirus software, password protection, and prohibition of malicious software and exploitative network traffic. Any equipment that does not meet security requirements cannot be trusted to handle sensitive data like PHI and will be removed from the network.
- Data destruction is essential when disposing of information that is no longer necessary. Paper documents containing sensitive information must be shredded. Request the assistance of your IT Support Team for proper disposal of electronic equipment such as computers, laptops, printers, tablets, smart phones, printers, and scanners.
- Social engineering is any trick used to try and access confidential information. Examples of this unexpected contact via a phone call, email, or a web link requesting sensitive information. Always report any suspicious activity to the IS Service Desk.
- Accounts and passwords must be unique to each person to ensure only authorized individuals have access to networks and systems. Passwords should not be shared or predictable, and must be reset regularly. Strong passwords include special characters, and longer passwords tend to be more secure than shorter ones.
- Emails containing PHI require extra vigilance, as insecure emails can result in data breaches and legal liabilities. Free, public email systems may not be used to communicate PHI. Bulk email forwarding to an external mail service is not permitted. UPHS maintains some additional security measures for protecting PHI in email, such as an encryption filter that scans outbound email and encrypts detected sensitive content or typing "encrypt" in the subject line of a message to encrypt an email.
- Discussion or sharing of sensitive internal information, such as PHI, in a public forum such as Twitter, Facebook, or other social media is unacceptable behavior and is prohibited. Workforce members, including volunteers, are prohibited from sharing PHI in addition to pictures of or stories about patients. UPHS uses web filters to block malicious and inappropriate websites.
- Sensitive data should always be stored with appropriate protections such as encryption, especially when stored on tablets, laptops, flash and USB devices, and other mobile storage devices. Encryption technologies modify data so that unauthorized users are unable to access it. Your IT support team or local service provider can assist with appropriate encryption methods and guidance.
- Physical security is also essential to protect information. Turn off devices and make sure your work area is secure before leaving. Use cables or other physical devices to secure a computer to a station. Do not leave ID cards, keys, laptops, phones, storage devices, or sensitive paperwork lying around. Call security if you are concerned about unknown people or unusual activity in your area.

Scenarios

- Frank, an environmental services worker, is walking through the hallway in between assignments and notices a piece of paper on the floor. He picks it up, quickly examines it, crumples it, and throws it in a nearby trash can.
    - The piece of paper Frank picked up off the floor contained medical information of a patient.
    - The paper should have been shredded to reduce the risk of patient information being misplaced or exposed.
- While at her desk, Maria, a Patient Services Representative, answers a phone call. Without hesitation, she responds to the caller's request – "That's so nice of you that you want to check on how your cousin is doing. Give me a moment to pull up the chart and check on her test results".
    - Even though people may have good intentions, they still may not be authorized to receive patient information. Maria needs to politely tell the caller that they cannot share patient information without the proper permissions.
- While at work, Tamika, a Business Administrator, receives an email that her account has been locked. The email urgently prompts her to click on a link in the email to unlock it.
    - Information Services will not use the email to directly troubleshoot accounts at Penn. Email messages like this typically indicate an outside attack. This is called **phishing**, which is an attempt to trick the user into revealing personal information and/or downloading a virus and/or revealing personal information. These types of emails can have severe consequences, such as exposing user accounts or sensitive data to outside attacks.
- Conrad, a resident at Penn, takes his health system issued iPad home to review some patient notes he documented during the day. After dinner, his wife asks if she can use the iPad to look up some recipes. Conrad enters his password and hands the iPad to his wife.
    - If you share a device from work with a family member or other individual, make sure they are unable to view any ePHI or other confidential information. In addition, be especially careful of suspicious apps, which may weaken security.
- Rosalyn is a researcher and is traveling home to Minneapolis to visit friends and family. She is planning to review patient-related data during her trip. Before leaving work, she downloads all the necessary data to her personal laptop, and heads off to the airport to catch her flight to Minnesota.
    - Sensitive data must not be stored on devices without approved security measures like encryption, passwords, and other protections. This includes all devices and hosts such as desktops, laptops, tablets, smartphones, personal email accounts, USB devices and unsecured DVDs, CDs, and cloud storage.

Understanding Breaches and Notification Obligations

- A breach is an impermissible acquisition, access, or use or disclosure of unencrypted PHI, unless there is proof that there is a low likelihood that the data is compromised.
- Unsecured PHI is PHI that has not been rendered unreadable, unusable, or otherwise indecipherable to unauthorized individuals. The best way to secure PHI is to encrypt it.
- **If a breach of PHI has occurred, you must report it to your manager, Entity Privacy Officer, or Penn Privacy Office IMMEDIATELY.**
- By law, if a breach has occurred, the following must be notified:
    - Affected patients without unreasonable delay
    - The Department of Health and Human Services, if greater than 500 individuals are affected.
- Consequences associated with non-compliance are as follows:
    - Disciplinary action, up to and including termination
    - Criminal and Civil penalties
    - Monetary fines, both for the organization and for liable individuals.
    - Reputational harm and loss of patient trust.

Doing Your Part

- Only access, use, and share PHI as needed to perform your job function.
- Always ask questions if you are unsure. Your Entity Privacy Officer is your first line of contact.
- Report suspected violations.
- Remember we are all patients too. Consider how you would want your own privacy and data protected.

Assessment

1. A patient was treated in the HUP emergency room over the weekend. The following Tuesday, the patient visits his primary care physician for follow up. The patient's physician calls and wants to discuss the care the patient receives over the weekend with a nurse working in the emergency room. After verifying that the caller is in fact that patient's physician, is the HUP Emergency Room nurse allowed under HIPAA to provide the physician with PHI about this patient?
    a. Yes, and the information she discloses is not subject to the Minimum Necessary rule because the information is for treatment purposes.
    b. No, she cannot disclose any protected health information about this subject.
2. A department manager wishes to hire two new companies, one to handle medical records and a second to run the department's website, especially the management of incoming medical questions by visitors who provide their names. The situation calls for:
    a. A business associate agreement between each company and Penn, because each is performing an operational service for the department involving PHI.
    b. A business associate agreement for the medical records vendor, but not for the website company.
    c. A written authorization from the patients whose data will be seen by these companies.
3. Beth is a cardiac patient who cannot drive. She lives with her daughter Sarah, who consistently brings Beth in for her doctor's visits. Beth, Sarah and her doctor routinely discuss Beth's course of treatment. A day after Beth's last visit, Sarah calls the office to ask for a clarification about the instructions written by the physician during the last visit. The doctor should:
    a. Check the chart to see if Beth has signed an authorization, as only a written authorization allows him to discuss Beth's medical treatment with her daughter.
    b. Not answer the question. The doctor should only speak to the patient, Beth, and not to a member of the family.
    c. Answer the question if he reasonably believes that the caller is the daughter and only to the extent that the answer is necessary for Sarah to assist in the treatment of Beth.
4. Kevin, a patient, is considering getting a second opinion regarding a diagnosis from his doctor. He calls the office and asks for a copy of his medical records. The office representative may
    a. Provide him with the records.
    b. Ask him to fill out an access request form and then send his records.
    c. Not provide him the records, as he should have confidence in the diagnosis his current physician has provided.

5. Mark, a business administrator, receives a phone call from a man from the Department of Health and Human Services describing that they need to see charts of all patients from the last week, as part of an oversight review. Mark should:
    a. Request by fax or mail proof of identity and authority for the request and consult his entity HIPAA Privacy Officer.
    b. Provide only the records he thinks are appropriate for such a request.
    c. Provide copies of the records as soon as possible, as these are allowable disclosures under the HIPAA Privacy Rule.
6. Reed, a nurse, urgently needs to speak to Abbi, an internist, about a dosage question for a patient. Reed can only find Abbi in the patient waiting room and knows she has a busy schedule. Reed may:
    a. Ask the doctor to step aside to an area where other patients are not within earshot and ask the question, using the patient's name to avoid risk of medical errors.
    b. Ask the question with a low voice and describing the patient well enough for the doctor to know to whom he is referring, but without using the patient's name or other information that could reasonably identify the patient.
    c. Either of the above.
7. You are out to dinner with your aunt and she asks you if you've seen her sister LeeAnn in the radiation center, as she heard she was getting treatments. You should:
    a. Politely acknowledge her concern for her sister, but let her know you are not permitted to share that information.
    b. Disclose to her that Mary has been receiving treatments but that you cannot provide any details.
    c. Share the details of Mary's situation with her since it's her sister and you know she's concerned.
8. You've just found out that a fellow volunteer you are close with is out for 3 weeks on a leave of absence. You are concerned about her, so you decide to check in the system to determine what's going on. This is an acceptable practice because you have access to the system and your intent is good.
    a. True
    b. False
9. Penn Medicine, as part of its process to ensure compliance with HIPAA, can and does monitor system usages to help in the identification of inappropriate access to PHI.
    a. True
    b. False