HIPAA

Non-Employee Annual HIPAA Training

Shepherd Center

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996

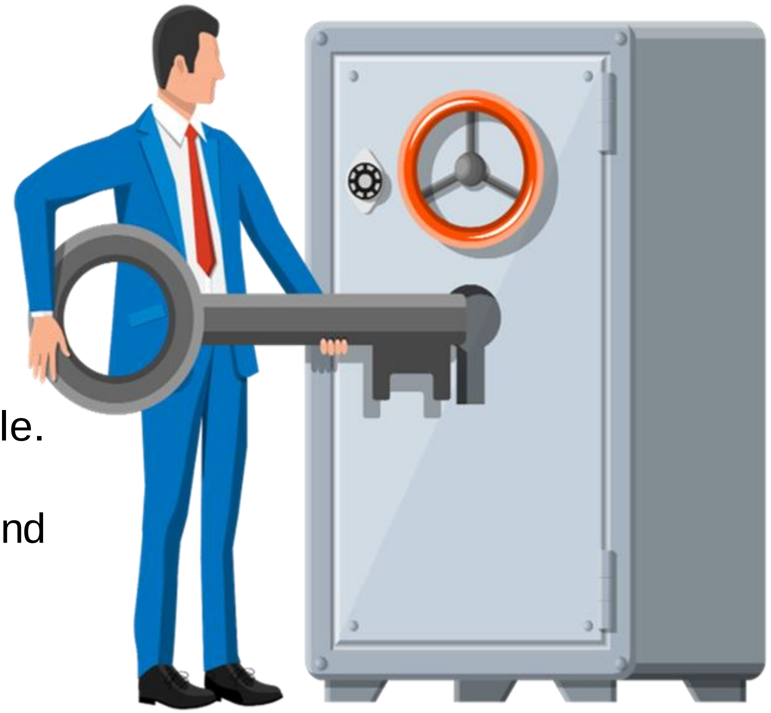
As an individual who has access to protected healthcare information, you are responsible for adhering to the HIPAA law.

The 1996 HIPAA regulations created:

- Protections for the privacy and security of healthcare data.
- Safeguards to prevent unauthorized access to protected healthcare information.
- Additional protections for electronic healthcare records.

This training module will give you an understanding of the HIPAA Privacy and Security Rule.

You are individually responsible—and accountable—for recognizing how HIPAA Privacy and Security requirements apply to your assigned work area.



HIPAA

Course Overview

HIPAA Privacy Rule

HIPAA Security Rule

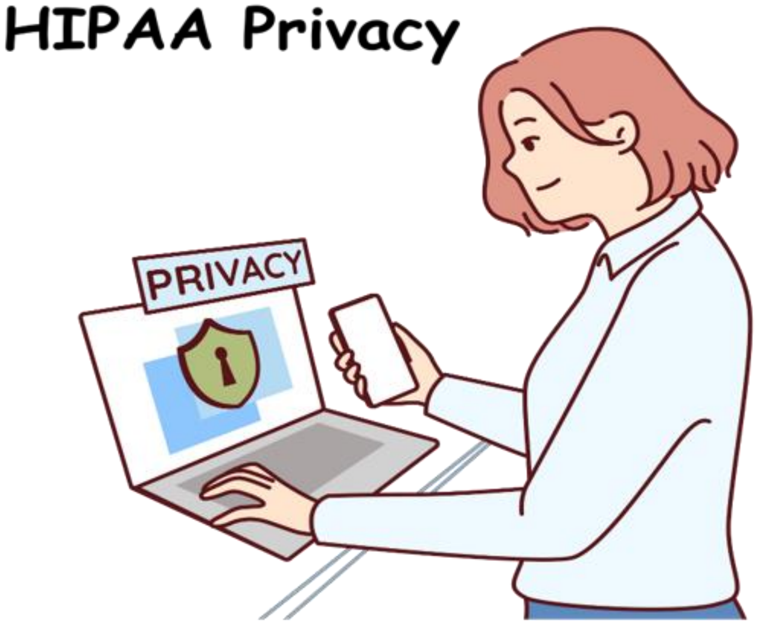
Enforcement & Breach Notification

Assessment

Shepherd Center

Why is HIPAA Privacy Important?

Shepherd Center supports enhanced patient privacy of health information. The HIPAA Privacy Rule is carefully balanced to provide strong privacy protections while ensuring access to and quality of health care delivery.



HIPAA Privacy Rule

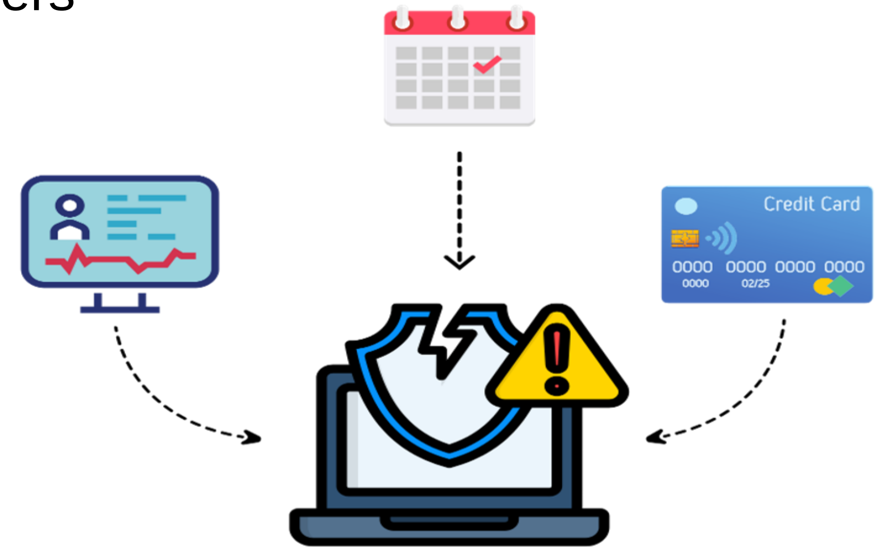
Protected Health Information (PHI)

What is PHI?

Information about health status, provision of health care, or payment for healthcare that we create or collect that contains personally identifiable information (PII) and can be used to identify a specific individual.

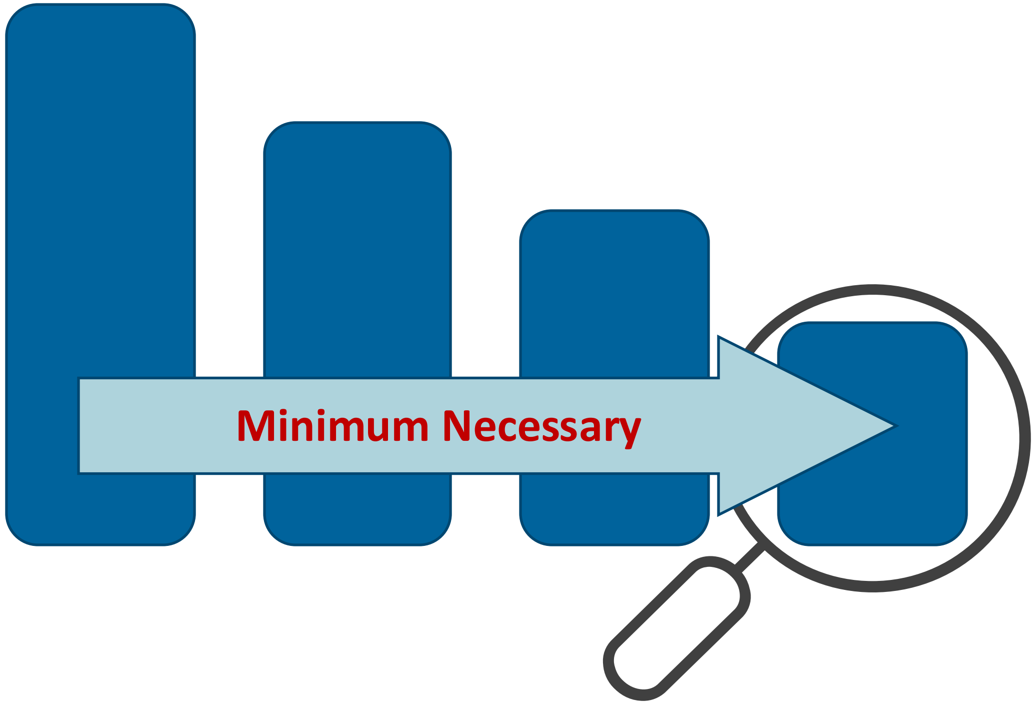
PII includes:

- Names of individuals and relatives
- Postal addresses
- Dates
- Telephone and fax numbers
- E-mail addresses
- Social Security numbers
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certification/license numbers
- Automobile VIN and serial numbers
- Device identifiers and serial numbers
- URLs and IP addresses
- Biometric identifiers
- Full face photographic images



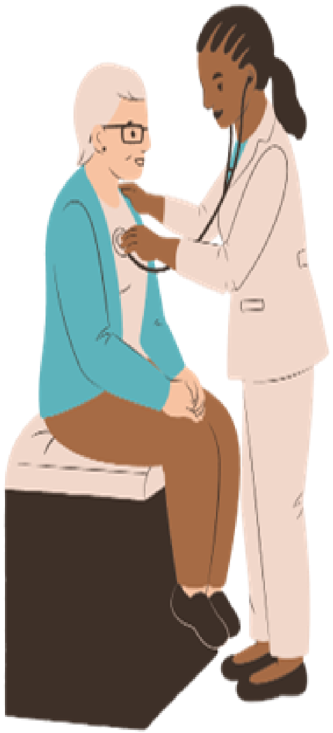
Shepherd Center

Minimum Necessary Rule



It is important to ONLY use the MINIMUM amount of information necessary to perform any assigned task.

Treatment, Payment or Operations (TPO)



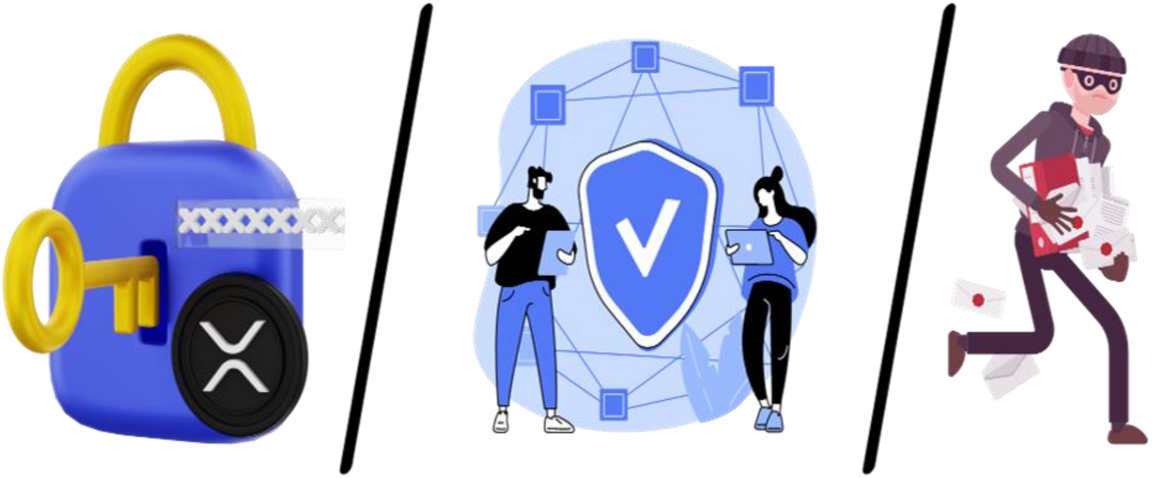
HIPAA does permit the use and disclosure of PHI as it pertains to Treatment Payment and Operation.

- **Treatment:** Coordination or management of healthcare, consultation between providers
- **Payment:** Billing & collections
- **Operations:** Education, quality assurance and audits

HIPAA Privacy Violations

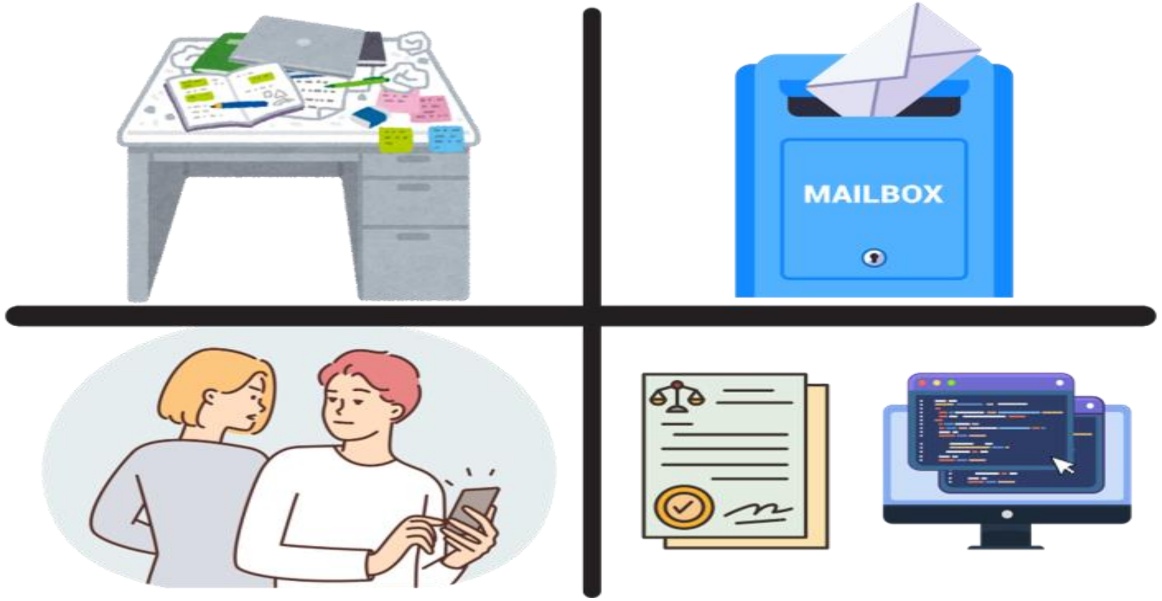
Examples of a HIPAA Violation include:

- Accessing health records to which you were not entitled
- Disclosing PHI to family, friends, or coworkers without prior authorization
- Stealing someone else's PHI in order to sell or misuse it.



HIPAA Privacy Violations Continued

- Misplacing PHI
- Exposing PHI in non-private areas such as the elevator or the cafeteria
- Communicating PHI via means not approved by the patient
- Leaving PHI records open on electronic devices & paper PHI lying around



Around the Office Tips

- Keep PHI out of clear view of the public (e.g., desks, whiteboards, or copiers/fax machines).
- Do not discuss PHI when it might be overheard by others who do not have a legitimate business need to know.
- Dispose of documents and electronic media containing PHI in secured containers or by shredding.

Key Take Aways & What To Do When Things Don’t Go As Planned

- Understand what PHI is and be aware of the many ways it can be breached
- Have a clear understanding of Shepherd Center’s policies and the guidance they provide in protecting PHI
- Ask for assistance whenever you are unsure of what to do

Shepherd Center

What to do if you have HIPAA Privacy questions, issues or concerns:

Ask your Direct Leader/Supervisor

or

Contact our HIPAA Privacy Officer at 404-350-1281

or

Contact our Compliance Program Administrator at 404-350-7737

Be prepared to provide the following info, if applicable:

1. When, where, and how the conduct occurred, or is occurring;
2. Persons involved in the conduct; and
3. Specific nature of the conduct

HIPAA Security Rule

The HIPAA Security Rule defines the standards required for **securing** electronic PHI (e-PHI).

Anyone who comes into contact with e-PHI must follow our *administrative, technical, and physical* safeguards to protect the confidentiality, integrity, and availability of healthcare information.

HIPAA Security Rule

Administrative Safeguards

Implementing the Security Rule requires a variety of important administrative safeguards. These safeguards detail the reasonable policies and procedures we use to limit access to and protect e-PHI.

Security Management Process

- We implement policies and procedures to prevent, detect, contain, and correct security violations.

Security Officer

- We designate a security officer who develops and implements our required policies and procedures.

Incident Procedures

- We report even suspected security incidents without delay.

Contingency Plan

- We take precautions to back up PHI in our care, so that we can respond to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain e-PHI.

Mitigation

- We take practical steps to mitigate the harmful effects caused by inappropriate disclosure of PHI.

Awareness and Training

- We train all team members on the importance that security plays in helping us remain HIPAA compliant, document training completion, and implement ongoing reminders to ensure security stays on the forefront of day-to-day operations.

Physical Safeguards

You can minimize the risk of unauthorized access to PHI by following physical security practices in your workplace.

Physical Safeguards apply to:

- Facility Access
- Workstations
- Devices and Media

Facility Access

- Always keep office doors and cabinets locked.

- Do not allow anyone to follow you into a secure location.

- Ensure that everyone who enters a secure area swipes their own badges.

- Report suspicious tampering with equipment or the presence of unauthorized individuals to security.

Workstations

- Always follow our policies for accessing e-PHI.

- Do not use your computer for activities unrelated to your job duties.

- Do not alter or modify physical components to your workstation.

- Physically secure your laptop and other mobile equipment with security cables or in locked drawers.

- Report suspicious use of your computer or unauthorized access of sensitive information to security.

Devices and Media

- Never leave your laptop or smartphone unattended in the office, in your car, or when traveling.

- Follow our approved processes for disposal of digital media that has accessed e-PHI, such as CD-ROMs or USB thumb drives.

- Contact IT for assistance in backing up data before moving any equipment that accesses e-PHI; ensure that movement is documented.

- Do not transmit or make copies of PHI using your personal devices (such as taking pictures of information using your smartphone).

- Appropriately store and dispose of any recordings, such as security camera footage or voice calls taped for quality purposes.

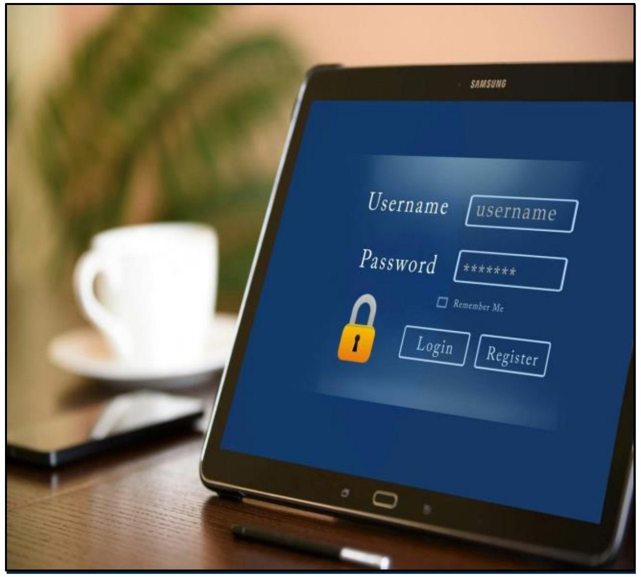
Technical Safeguards

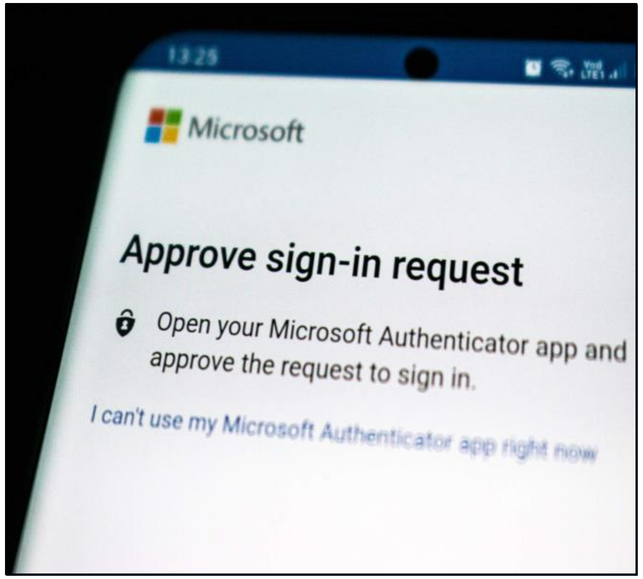
Implementing appropriate technical safeguards allows us to protect electronic protected health information (ePHI) from unauthorized access, disclosure, or use.

Locking computer screens when not in use

Multi-Factor Authentication (MFA) for remote login

Password protection on all devices.



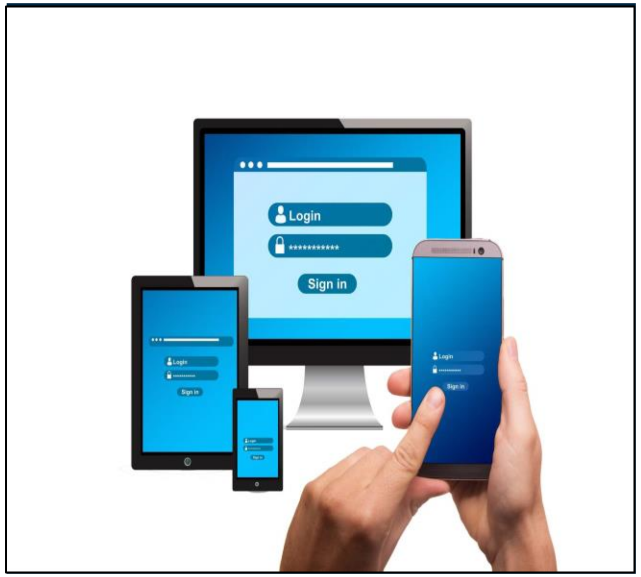


Microsoft

Approve sign-in request

Open your Microsoft Authenticator app and approve the request to sign in.

I can't use my Microsoft Authenticator app right now



Cybersecurity Tips

- Be careful with emails or messages from unknown senders, especially if they ask for money or personal information. Verify the legitimacy of the sender especially if it seems 'too good to be true.'
- Avoid clicking on suspicious links or downloading unknown files.
- Never share your passwords or login credentials with anyone who doesn't have authorized access.
- Always verify websites and sources of information are legitimate.
- When in doubt ALWAYS check with Shepherd Center’s IS department.

Enforcement & Breach Notification

Any impermissible release, acquisition, use, or disclosure of PHI can bring significant risks to our organization, ranging from fines to criminal penalties. These monetary penalties and legal sanctions exist to discourage incidents from occurring and provide consequences for those who violate HIPAA rules and regulations.

We're legally accountable to HIPAA regulations, but we also follow privacy and security best practices to protect customers and patients. It's the right thing to do!

When You Break The Law…

- The Office for Civil Rights, the government agency charged with enforcing the privacy and security regulations, is very active in investigating complaints and reported breaches.

- To remain HIPAA compliant, our organization must apply appropriate sanctions against individuals who fail to comply with privacy and security policies and procedures.

- This means that you could be individually fined and face criminal charges for violating HIPAA regulations.

Internal Actions

- Verbal Warning
- Termination of contract

Civil Actions

Monetary Fines

Criminal Actions

Imprisonment

Shepherd Center

What to do if you have HIPAA Security questions, issues or concerns:

If you receive what is believed to be malicious files or email or suspect that a computer is infected, it must be reported immediately to Information Security via phone (404-603-4357) with the following information *(if known):*

1. Source of infection.
2. Symptoms of system infection (ransomware notice, slow performance, strange emails).
3. Potential recipients of infected material.
4. Malicious software name if detected by anti-malware.

Shepherd Center

END OF MODULE

TAKE THE ASSESSMENT

Shepherd Center

A Passing Score of 80% or more is **REQUIRED**

Click on the button to take your ASSESSMENT >>>

HIPAA Assessment

This is a trustworthy file so click “Ok” on the next prompt!