HIPAA Privacy & Security

Orientation Module for Students - Advanced Practice Providers - Residents - Faculty

Greater Green Bay Health Care Alliance

ggbha.org

Updated 02/28/2025

HIPAA Privacy & Security

This module is designed to prepare you for your clinical or residency experience. The goal of this module is to teach you the importance of keeping our patients' protected health information (PHI) safe from inappropriate uses and disclosures. This includes electronic protected health information (ePHI).

After completing all **five modules and you understand the information presented**, you will need to complete the '**Confidentiality Agreement and Acknowledgement of Orientation Modules**' form. Please give the completed form to your school coordinator or faculty member, **not** the healthcare facility. The school will retain your signed/dated form.

The five learning modules need to be completed annually by students/advanced practice providers/residents/faculty.

HIPAA Privacy & Security

While completing this module, please know YOU are responsible for understanding the information presented.

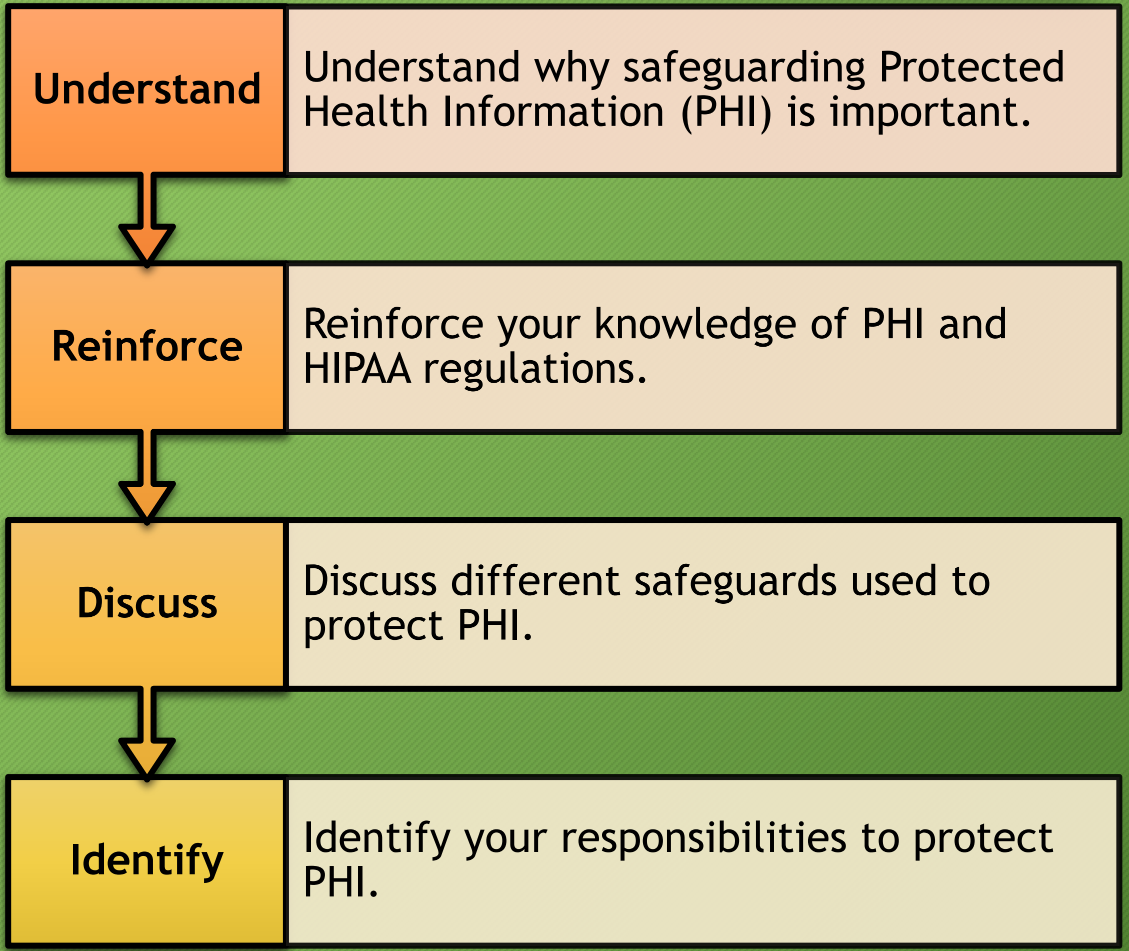
If you have any questions, please contact your instructor/school/facility for answers prior to submitting your final ‘Confidentiality Agreement and Acknowledgement of Orientation Modules’ form.

Learning Outcomes

GOAL:

Focus on Safeguarding

Patient Health Information (PHI)



Understand	Understand why safeguarding Protected Health Information (PHI) is important.
Reinforce	Reinforce your knowledge of PHI and HIPAA regulations.
Discuss	Discuss different safeguards used to protect PHI.
Identify	Identify your responsibilities to protect PHI.

What is PHI? Protected Health Information

Protected Health Information (PHI) is any piece of information in an individual’s medical record that was created, used, or disclosed during the course of diagnosis or treatment that can be used to personally identify them.

Examples of PHI Protected Health Information

1. Name
2. Address (including subdivisions smaller than the state such as street address, city, county, or zip code)
3. Any dates (except years) that are directly related to an individual, including birthday, date of admission, etc.
4. Telephone number
5. Fax number
6. Email address
7. Social Security number
8. Medical record number
9. Health plan beneficiary number
10. Account number
11. Certificate/license number
12. Vehicle identifiers, serial numbers, or license plate numbers
13. Biometric identifiers such as fingerprints or voice prints
14. Photos

Forms of PHI – Protected Health Information

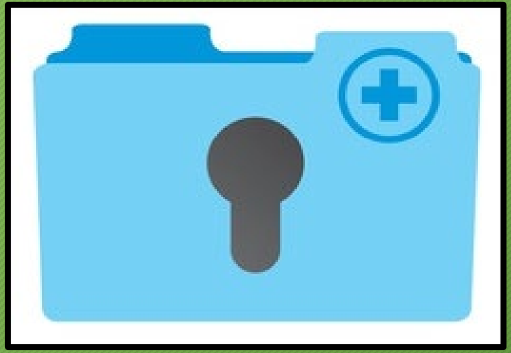
When we talk about safeguarding our patient's Protected Health Information (PHI), remember that PHI comes in many forms.

1. **VERBAL** – Discussing PHI should be done in a manner that protects the PHI as much as possible by speaking quietly or in private areas when possible.
2. **PAPER** – Paper documents that contain PHI should never be left unattended in a location that patients or others have access to or may oversee.
3. **ELECTRONIC** – Electronic PHI (ePHI) includes everything from your desktop or laptop computer, cell phones, and tablets, to CDs and USB drives or medical devices that contain PHI.

Loss or Theft of PHI

Because PHI is valuable, health care systems are often targeted for theft and hacking by cybercriminals.

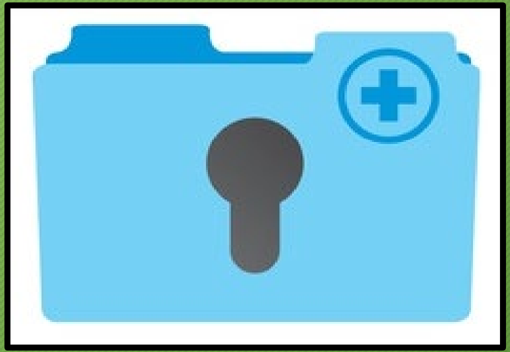
PHI is valued much higher than other types of data, fetching up to $50-100 per record, more than 10 times the price of credit card data.



Loss or Theft of PHI

Loss or theft of PHI may lead to:

1. Loss of patients' trust.
2. Identity theft.
3. Millions in settlement agreements and even more costs to fix security issues.



Theft of PHI

Healthcare is the #1 Target of Attackers

Cyber Safety = Patient Safety

Cyber Security Facts

97%

- Percent of healthcare organizations have confirmed being targeted by some form of cyberattack.

730 Systems

- 730 health systems were victims of a cyber attack in 2023.
- 135 million patient records affected.

$77.5 Billion

- Ransomware cost healthcare organizations $77.5 billion since 2016.

End of Life

- 96% of hospitals claim they were operating with end-of-life operating systems or software with known vulnerabilities, including medical devices.

Cyber Safety Zone

Social Engineering

- Don’t take the bait!
- Does the URL match the sender? (i.e., if the sender is Jackson Equipment, links should go to www.jacksonequip.com, not www.klnkjklajf.net
- Does the message illicit some type of quick action such as “respond immediately” or “quick action is required?”

Loss or Theft of Equipment or Data

- Know your:
  - Organizational policy regarding taking equipment or information home.
  - Organizational encryption policy when sharing data via email.
- Use a secure Wi-Fi or VPN when accessing organizational data or sharing PHI.

Cyber Safety Zone

Insider Accidental or Malicious Data Loss

- Follow your instinct, always report what does not look or feel right to you.
- Beware of social engineering techniques like phishing. These emails intentionally focus on human emotion, using words like, “Your immediate action is needed.”
- Read thoroughly and proceed with caution.
- Participate in security awareness training within your respective organizations.

Why Records are Valuable

“Cyber criminals are selling information on the black market at the rate of $50 for each health record, compared to $1 for a stolen credit card or social security number.” – FBI Cyber Division

Criminals can use data to:

- Submit false medical claims (and obtain free medical care).
- Purchase prescription medication illegally.
- Resell the record on the black market.
- Medical ID thieves may bill your health plan for fake or inflated treatment claims. Criminals are often doctors or other medical personnel who know how the insurance billing system works.

Protecting PHI

Two caregivers are standing in a patient's doorway, discussing the patient's health condition and treatments. Is this a privacy incident?

Decide your answer before proceeding to the next slide.

Protecting PHI

Correct Answer:

YES – This is a privacy incident. Never discuss a patient out in the open where others can hear you. Do it in a private location.

Protecting PHI

You have become particularly fond of a patient for whom you are caring. She has been in the hospital for a week. You heard she is going home today and want to share the good news with friends and family members via social media. Is this acceptable?

Decide your answer before proceeding to the next slide.

PROTECTING PHI

Correct Answer:

NO – Sharing this news on social media is a privacy incident. The HIPAA Privacy Rule **prohibits the use of Protected Health Information on social media networks.** This includes images of patients or videos that could result in a patient being identified.

***Prior to the start of the clinical rotation, review the institutional policies of your school and the clinical agency regarding social media and HIPAA. HIPPA violation fines can range up to $50,000+.**

PROTECTING PHI

You happen to see a family friend being admitted to the hospital. You want to call your family members to tell them what you just observed. Is this acceptable?

Decide your answer before proceeding to the next slide.

Protecting PHI

NO – This is not acceptable. Telling others about your family friend being admitted to the hospital would violate this patient’s privacy rights.

Unauthorized Health Information

Releasing unauthorized health information is also a violation. This refers to releasing the wrong document that has **not** been approved for release. A patient has the right to release only parts of their medical record.

Examples could include:

1. A recent cancer diagnosis that the patient is not aware of yet.
2. The gender of a baby.

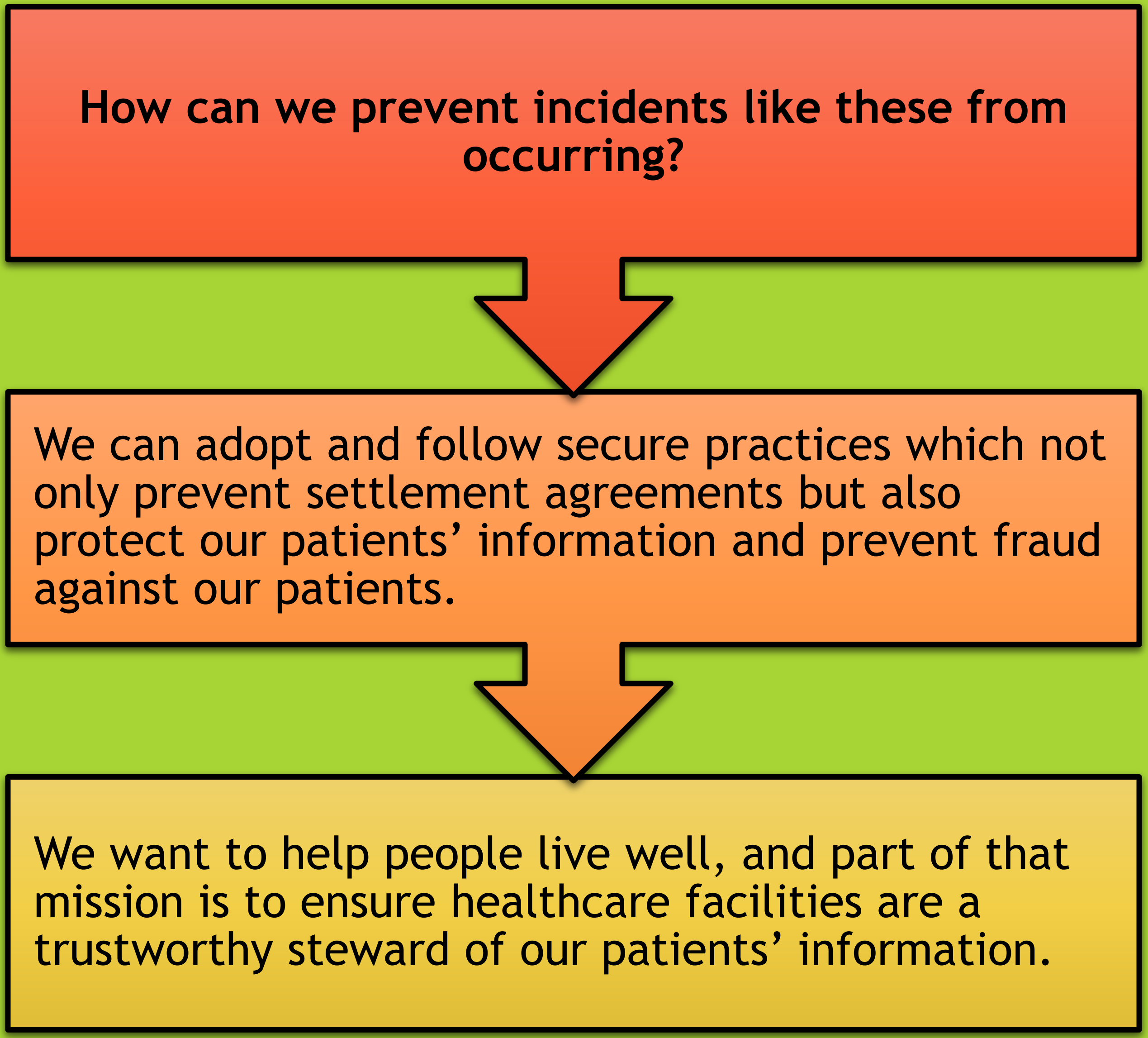
Why Protect PHI?

1. Electronic devices have been stolen, compromising millions of patients’ records and resulting in large financial settlements.

2. A stolen mobile device, with no encryption or password, and an unencrypted laptop compromised thousands of patients’ records and resulted in a $3.2 million settlement agreement.

3. A hospital agreed to pay $1 million after a caregiver left documents containing PHI on a subway train during their commute to work, resulting in 66 patient’s PHI being disclosed. The documents were never recovered.

Follow Secure Practices



How can we prevent incidents like these from occurring?

We can adopt and follow secure practices which not only prevent settlement agreements but also protect our patients' information and prevent fraud against our patients.

We want to help people live well, and part of that mission is to ensure healthcare facilities are a trustworthy steward of our patients' information.

Protecting PHI – Implement Safeguards

To protect PHI, it should:

1. **Not** be used or disclosed in excess of what is needed to fulfill a request or complete a job function.
2. **Not** be accessed for patients **not assigned to you**. Students **cannot** access records of any patient they were previously assigned to, or deceased patients.
3. **Not** be accessed by caregivers or others who do not have a right to know this information.
4. **Not** be disposed of without taking precautions to de-identify or render the information unrecognizable (i.e., shredding).
5. **Not** be transported offsite without proper authorization or precautions.
6. **Not** be handed off, faxed or mailed to an inappropriate recipient.
7. **Not** be stored in a manner that is unsecured.

PROTECTING PHI - IMPLEMENT SAFEGUARDS

You are subject to HIPAA rules and laws concerning patient medical records. Unnecessarily accessing any patient’s medical records for personal reasons can lead to termination.

- Do NOT access charts that are not assigned to you.
- Do NOT access your own, family members, friends / acquaintances patient care records. Proper release of information of record must be followed.
- By signing the required confidentiality agreement, you will be subject to, and agree to abide by, the same rules, regulations, policies, procedures, and standards of clinical agencies as are established for the organization’s employees in matters related to confidentiality.

Protecting ePHI

A medical assistant is caring for a patient, documenting the patient’s vitals in the **electronic medical record** when she receives a hospital page that she must attend to. What should she do? **Select your answer below.** *Decide your answer before proceeding to the next slide.*

A. She will be right back, and it is the patient’s own information, so she should leave right away to respond to the hospital page.

B. Before leaving the computer, she should sign off/lock/secure the workstation.

PROTECTING ePHI

Correct Answer:

B. If you need to walk away from your workstation, it is important to **always** safeguard PHI, so you should always log off or lock the workstation so others, including patients, do not see another’s information.

*At the end of your shift, you must also unassign your patients from the patient care team in EPIC.

Physical Safeguards

There are physical safeguards we can all use to protect PHI.

1. Paper documents should be disposed of in locked, confidential recycle receptacles.
2. Other media, including CDs, must be destroyed or defaced in a manner that effectively removes all PHI.
3. Challenge people who are walking in restricted areas without a nametag on. Insist they need a nametag/identification and assist them, if needed, in obtaining this. Caregivers **must always** wear their nametag while in facilities.
4. Store unused desktops and laptops in a locked cabinet, even if they are encrypted.
5. Ensure only the caregivers that need access to that equipment have access to the cabinet or closet.

Safeguarding PHI

1. Students should **NOT** be storing or transferring PHI.
2. Do **NOT** put patient PHI on clinical paperwork, in a text, email or on social media.
3. Understand and be compliant with HIPAA rules and regulations.
4. Always keep anything that contains patient information out of the public's eye.
5. Follow workplace security and privacy policies to protect PHI and network shared files.

PHI information should not be transferred to or from, or stored within, any form of personal technology (e.g., personal computers, laptops, USB drives, cell phones, etc.), nor should it be shared in any form of social media (e.g., Facebook, YouTube, etc.).

If you have questions about PHI safeguards, contact your clinical or rotation site.

Test Your Safeguard Knowledge

Does each of the following items demonstrate a safeguard or a lack of safeguards?		
	Safeguards	Lack of Safeguards
1. Login/passwords are posted for all to use.		
2. PHI is not visible to passersby on computer screen.		
3. PHI is disposed of in the nearest trash can.		
4. Fax machine/printer is unattended.		
5. Workforce training on HIPAA safeguards.		
6. Storing your device in a public area.		
7. Conversations are held in private areas.		
8. Locking the screen when your device is unattended.		

Answers: Test Your Safeguard Knowledge

ANSWERS: Does each of the following items demonstrate a safeguard or a lack of safeguards?		
	Safeguards	Lack of Safeguards
1. Login/passwords are posted for all to use.		X
2. PHI is not visible to passersby on computer screen.	X	
3. PHI is disposed of in the nearest trash can.		X
4. Fax machine/printer is unattended.		X
5. Workforce training on HIPAA safeguards.	X	
6. Storing your device in a public area.		X
7. Conversations are held in private areas.	X	
8. Locking the screen when your device is unattended.	X	

Your Responsibilities

- PHI comes in many forms. We must safeguard all of them, always.
- Make sure PHI is secured or locked away when not in use at the clinical or rotation site.
- Make sure devices are locked away appropriately when not in use.
- Do not save PHI locally on your device.
- If you have any questions or concerns about the privacy and security of PHI, talk to your leader!
- Failure to report a privacy violation is a violation.

Regulatory Fraud, Waste & Abuse

Every year, billions of health care dollars are improperly spent because of Fraud, Waste and Abuse.

- **FRAUD:** Intentionally submitting false information to the Government (to obtain money or a benefit).
- **WASTE:** Practices that directly or indirectly result in unnecessary costs to federally funded programs, such as overusing services or misusing resources.
- **ABUSE:** Actions that directly or indirectly result in unnecessary costs to federally funded programs, such as providing patients with medically unnecessary services.

Health care organizations maintain Compliance Programs to prevent, detect, and correct Fraud, Waste, and Abuse. You can help prevent Fraud, Waste, and Abuse:

- Act with honesty and treat others with respect, dignity, and fairness.
    - Review each organization's Standards of Conduct.
- Report concerns and suspected violations of the law, regulations, or the organization's Standards of Conduct.
    - Anonymous reporting is available. Reporting instructions will be provided by each organization.

HIPAA Privacy & Security - Conclusion

After completing all **five modules and you understand the information presented**, you will need to complete the ‘**Confidentiality Agreement and Acknowledgement of Orientation Modules**’ form. Please give the completed form to your school coordinator or faculty member, **not** the healthcare facility. The school will retain your signed/dated form.

The five learning modules need to be completed annually by students / advanced practice providers / residents / faculty.