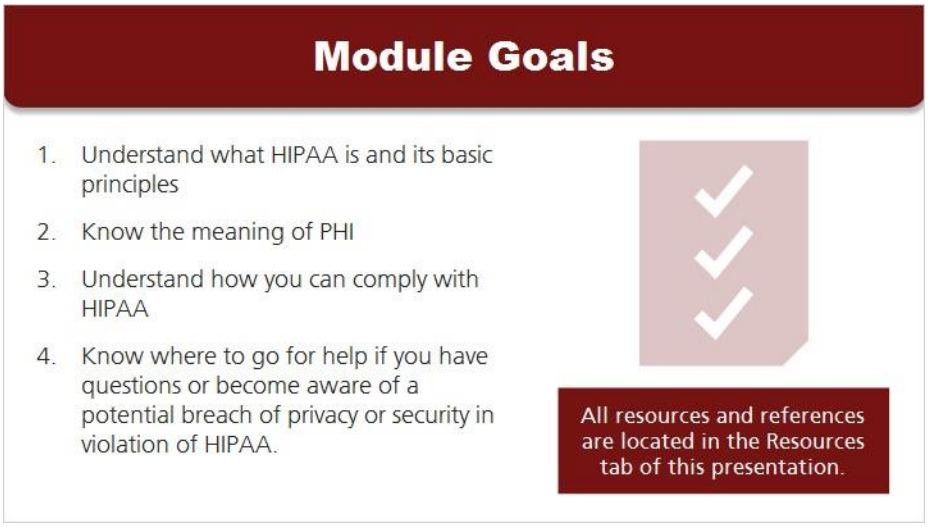
HIPAA Awareness Training

Welcome to the RecoveryU module on HIPAA awareness! Understanding HIPAA is an important component of Recovery Coaching in the Emergency Department Setting.



By the end of this module you will:

1. Understand what HIPAA is and its basic principles.
2. Know the meaning of PHI.
3. Understand how you can comply with HIPAA.
4. Know where to go for help if you have questions or become aware of a potential breach of privacy or security in violation of HIPAA.

First, we will discuss the basics of HIPAA, what it is and why it's important.

HIPAA is an acronym for the "Health Insurance Portability and Accountability Act" and is a federal law passed by congress in 1996.

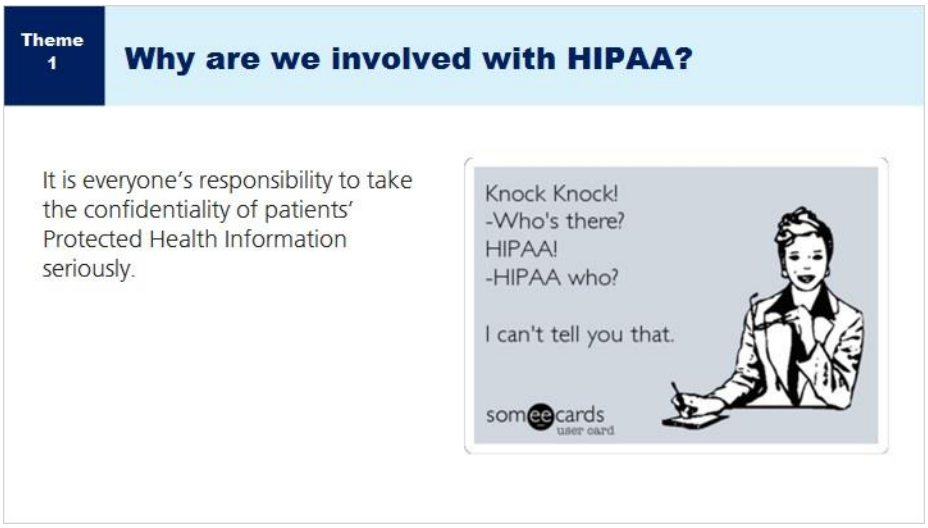
HIPAA sets national standards for the privacy and security of identifiable patient medical information. It applies to "covered entities" which include health care providers like hospitals, public health departments, medical professionals, insurance companies, home health care companies, surgery centers, and some research laboratories and covers ALL forms of "protected health information," including all oral, written, and electronic communication. HIPAA is enforced by the US Department of Health and Human Services Office of Civil Rights.

In general, HIPAA is based on two important ideas: privacy and confidentiality.

Privacy refers to a person's right to limit who knows what about their medical condition. It also refers to the right to have conversations about medical care in places where others can't overhear.

Confidentiality refers to a person's right to limit or place restrictions on who can access and share their medical information.

Doctors can share medical information with nurses, therapists, and other healthcare professionals on the patient's medical team. This is important for good care and is not affected by HIPAA.



Why are we involved with HIPAA training? Because it's everyone's responsibility to take the confidentiality of patients' Protected Health Information seriously.

Any time you come in contact with Protected Health Information that is in electronic format, written, spoken, or electronically transmitted, you become involved with some aspect of the HIPAA regulations. Because of this, HIPAA requires awareness training for all health care personnel, including volunteers, students, and trainees.

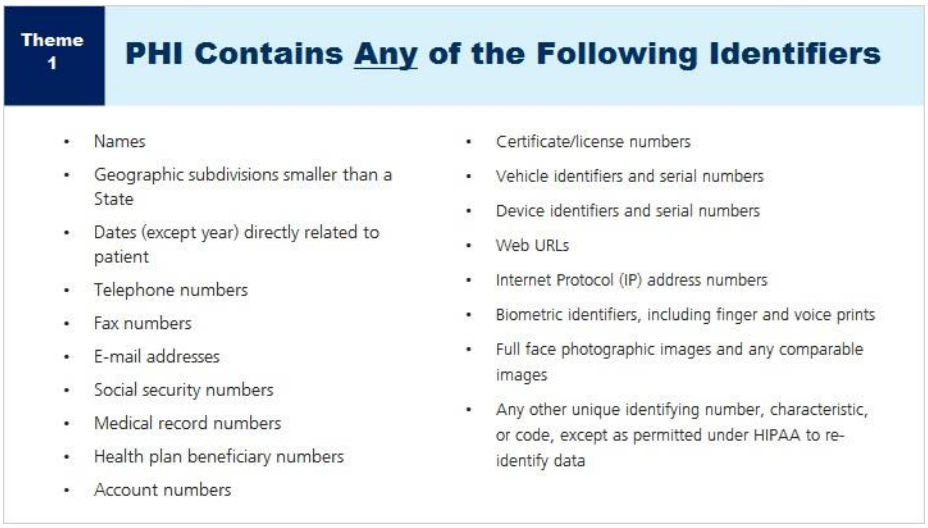
What are the consequences of not complying with HIPAA? Under HIPAA, there are now fines and penalties for failing to comply.

Accidental disclosures and unintentional violations of HIPAA often involve corrective action plans and fines. Wrongful and willful violations of HIPAA may lead to fines and can even involve jail time.

Not complying with HIPAA also erodes public confidence and decreases the likelihood that patients will be open and honest with their health care providers.

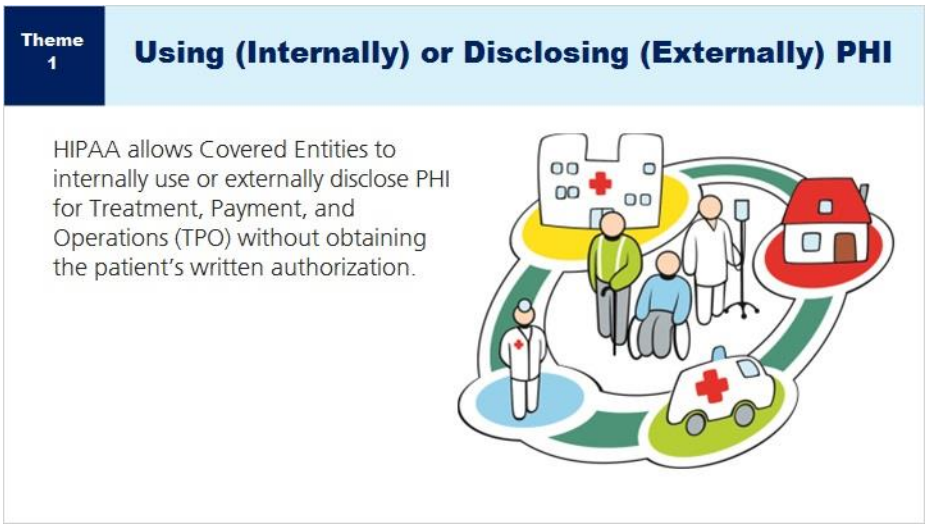
What is Protected Health Information, or PHI? PHI is a defined term under HIPAA meaning any individually identifiable health information created, received, transmitted, or maintained by a covered entity—in any form or medium (paper, electronic, or oral)—which relates to the past, present, or future physical or mental health of an individual.

Any health information that identifies someone or can be used to identify an individual must be protected by covered entities and can only be used or disclosed per HIPAA regulations.



Protected health information contains any of the following identifiers:

- Name
- Geographic subdivisions smaller than a State
- Dates (except year) directly related to patient
- Telephone numbers
- Fax numbers
- E-mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate or license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web URLs
- Internet Protocol or IP address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code, except as permitted under HIPAA to re-identify data

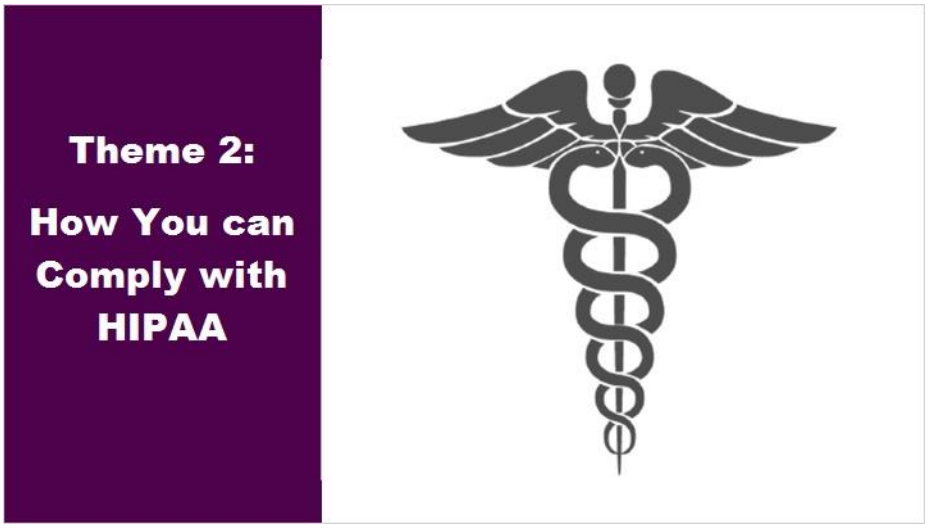


HIPAA allows covered entities to internally use or externally disclose PHI for Treatment, Payment, and Operations, or TPO, without obtaining the patient's written authorization. Patients need to give written authorization for most other uses of their PHI for non-TPO purposes, unless HIPAA specifically says otherwise.

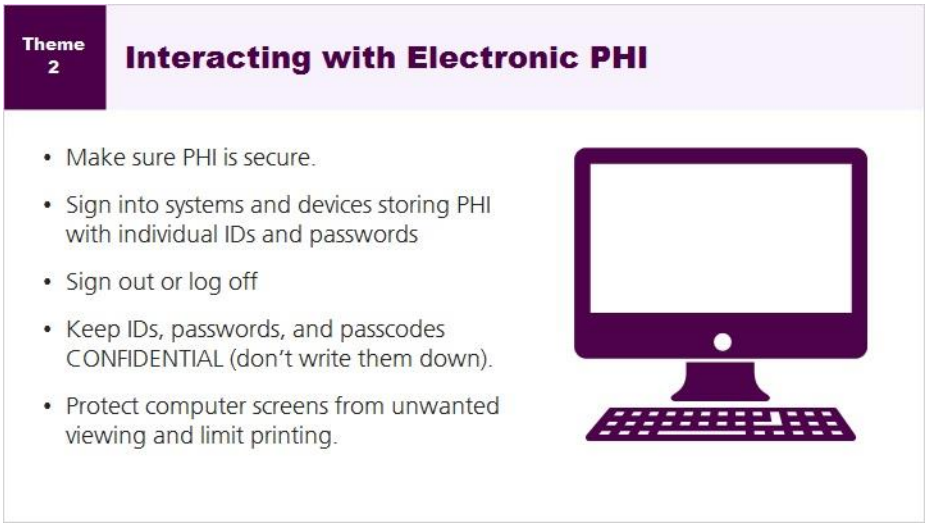
Treatment includes the provision, coordination, or management of health care and related services among covered entities, consultation between health care providers, or referral of a patient from one health care provider to another.

When working with PHI, you should access and use or disclose only the minimum amount of information needed to fulfil your assigned duties.

Access, use, and disclose only the minimum necessary amount of PHI, whether it's in electronic, paper, or oral or verbal format.



Next, we will learn how you can comply with HIPAA.



Make sure PHI is secure. This includes PHI on computers and mobile devices or shared electronically through email, texting, and any other method of information exchange.

Sign into systems and devices storing PHI with individual IDs and passwords, because covered entities are required to keep track of who can access PHI and log access to certain medical record systems.

Sign out of secure medical records systems or mobile devices when not using them. Keep IDs and passwords, and passcodes confidential and do not write them down. Protect computer screens from unwanted viewing and limit printing.

When interacting with PHI in paper formats:

- Access the PHI using the Minimum Necessary Standard.
- Double-check the names on printouts of PHI when handing them to others.
- Be careful not to lose or misplace printouts with PHI, and
- If you discover lost or misplaced printouts with PHI, know where to forward them for follow-up because a covered entity will need to analyze the situation to determine if a breach occurred that requires notification.

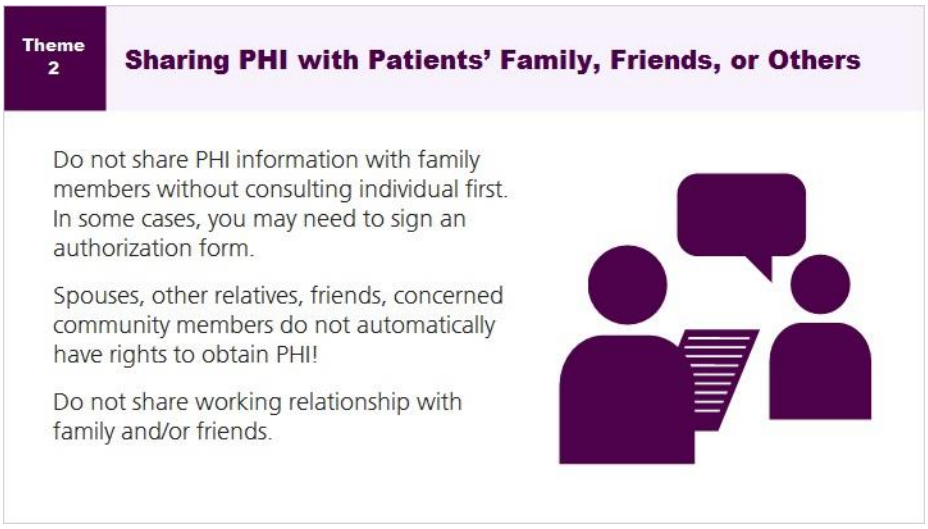
When interacting with PHI in oral and verbal formats:

- Use good judgment about what to discuss given your surroundings. Don't talk openly about PHI in cafeterias, elevators, lobbies, waiting rooms, or other public areas.
- Pay attention to your volume! This is especially important in public areas and when talking about PHI over the phone.
- Don't talk about PHI outside of work, volunteer, or training settings. Don't talk about PHI with others in public places like grocery stores, restaurants, or parks.
- Don't talk about PHI with friends, significant others, or acquaintances. If you're sharing stories about your day with people important to you, be general and avoid including any specific identifiers!

Verify to whom and to where you are phoning or faxing before disclosing PHI through phone calls or faxes.

Fax cover sheets should contain a confidentiality notice and contact information so the recipient knows who to call with any questions.

Be wary of placing calls while in public places, and be wary of accepting calls from someone who says they should have access to PHI. Verify the person's identity and double check with the individual whose PHI is requested before sharing any information.



Ask the person you're with if it's okay to share their PHI with anyone before you give it out. In some situations, you—the person—will need to sign an authorization form to document that they give permission for you to share PHI. Ask your supervisor or the Privacy Officer when authorizations are needed.

Spouses, other relatives, friends, and concerned community members do not automatically have rights to obtain PHI!

Be careful of mentioning you saw someone in the course of your work, even in casual conversation such as "Hey, I saw Ms. Jones earlier today. She seems to be doing really well lately." You should not even share the fact that you worked with her!

If you are asked to provide PHI to law enforcement, attorneys, employers, or anyone you are not directly working with, ask for assistance from your supervisor.

Disclosures to these individuals are likely to require authorization, and you should seek assistance from someone familiar with HIPAA and its authorization requirements and exceptions.

If you need to dispose of PHI, handle and dispose of it carefully. For paper records, use a shredder or confidential shredding bin instead of throwing them away in an open trash can.

If disposing of PHI in electronic format, ask for help from a supervisor to ensure that it's unreadable and destroyed properly. When in doubt, ask.

How to Report Violations:

It's everyone's responsibility to report potential breaches of the privacy or security of PHI. If you believe someone received PHI improperly, or shared PHI in the wrong way, or lost a laptop or cell phone with PHI, report the potential breach immediately. When in doubt...ASK!

If you come into contact with PHI that you believe was lost, inadvertently disclosed, or not properly secured, report it to your supervisor as soon as possible.

Ask for the name of the Privacy Officer at the facility where you work or volunteer, and then reach out to that person with any HIPAA-related questions.

It is important to report violations because any incidents involving PHI that meet HIPAA's definition of a "breach" will require patient notification and notification to the federal government, and might also require notification to the news media.

Details about breaches reported to the federal government are publicly available via the link on the screen.

If you are ever unsure how to report a suspected HIPAA violation, you can report it to UW-Madison's HIPAA Privacy Officer; it will then be forwarded to the Privacy Officer of the appropriate facility.

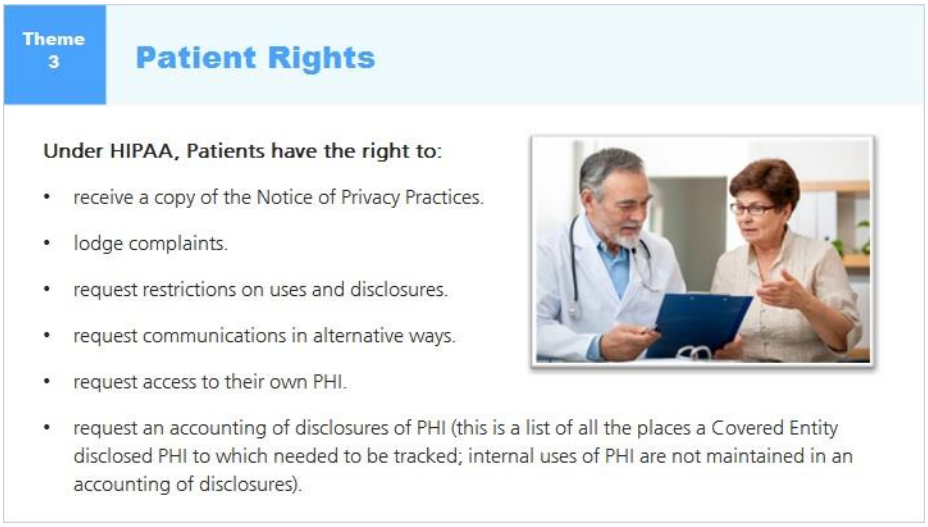
UW-Madison's "HIPAA Incident Report Form" is available via the link on this screen.

Remember to stop and ask yourself, "should I be sharing this PHI?" If you're unsure, ask for help.

PHI about fellow coworkers, volunteers, trainees, or neighbors should never be shared for any of your own personal reasons.

Be aware of how much information you share on social media, like on your own Facebook or Twitter pages, when sharing updates about your day. Don't report PHI about the people you work with to your own friends, acquaintances, or contacts. Make generic updates that don't include any of the PHI identifiers described earlier.

In this last section, we will discuss patient rights and provide additional resources for more information.



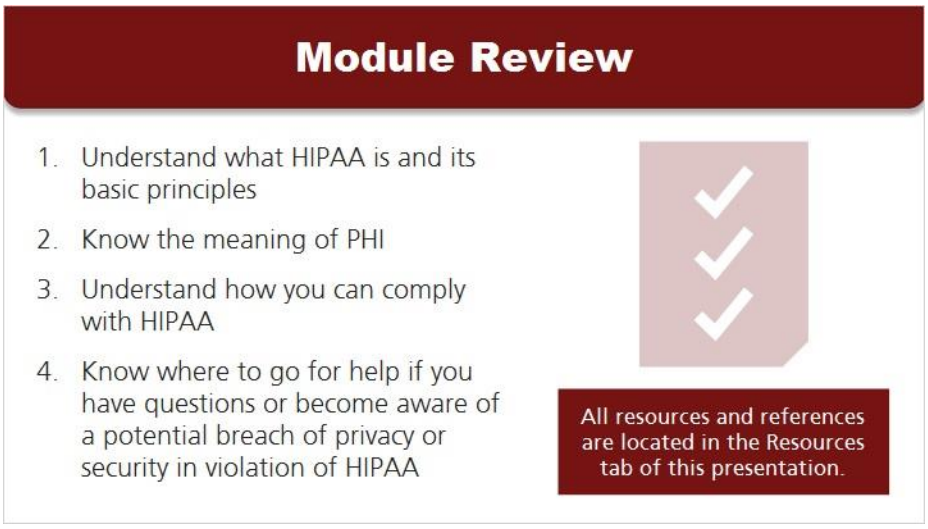
Under HIPAA, patients have the right to:

- receive a copy of the Notice of Privacy Practices.
- lodge complaints.

- request restrictions on uses and disclosures.
- request communications in alternative ways.
- request access to their own PHI.
- request an accounting of disclosures of PHI. This is a list of all the places a covered entity disclosed PHI to which needed to be tracked. Internal uses of PHI are not maintained in an accounting of disclosures.

To learn more about HIPAA where you're working, including how to honor patients' rights:

- Ask for contact information for the facility's HIPAA Privacy Officer.
- Ask where to find policies and procedures about HIPAA, working with PHI, and authorizations for the use or disclosure of PHI.
- Ask how to report suspected breaches involving PHI.



In this module, you learned about HIPAA and its basic principles, the meaning of patient health information or PHI, complying with HIPAA, and seeking help regarding HIPAA violations.

Thank you for completing this module on HIPAA Awareness!