Are you in the correct course?
This is a course on HIPAA Privacy and Security rules.

Did you access this course through Mlearning?

- **Yes?** Click the yellow arrow below to continue.

- **No?** If you have a Level 2 Password and are associated with Michigan Medicine, you must log in through Mlearning and enroll in the course to get credit. Log in at [https://trainingportal.med.umich.edu/Saba/Web/Main](https://trainingportal.med.umich.edu/Saba/Web/Main), then follow these instructions:
  1. Click on the Me Icon
  2. Click Search from the left-sided navigation list.
  3. Type “PRIV” in the search box.
  4. Launch Course Title “PRIV-10001 HIPAA Basics Learning Module – FAQ and Attestation”

*If you already accessed this course through Mlearning, or if you are not associated with Michigan Medicine, continue with this module:*

Click the yellow arrow to continue.
HIPAA Learning Module
Privacy and Security Rules Regarding HIPAA

10/04/2021
Our Commitment to Privacy

• The University of Michigan and Michigan Medicine are committed to protecting the privacy and integrity of our patients’ health information.

• The HIPAA Privacy and Security Rules recognize the importance and value of this commitment.

• Protecting Patient Health Information is the responsibility of all of us.
How to Report Concerns

1. Report through Supervisor/Manager
2. Compliance Office by phone (615-4400) or via http://www.med.umich.edu/compliance/index.htm
3. Anonymous through University of Michigan Compliance Hotline:
   Phone (866) 990-0111 or Online

Not sure? ....Report it.
Think it is too late? ....Report it.

You cannot be retaliated against for reporting a concern in good faith!
HIPAA Breaches

All violations are **PRESUMED** a “BREACH”

REPORT ALL HIPAA CONCERNS!
Let Us Do the Rest!

All HIPAA incidents are analyzed to overcome the Breach Presumption.

Factors Considered:
Nature & extent of information involved (e.g., types of identifiers, risk of re-identification)
Unauthorized person who used the PHI or to whom it was disclosed
Whether the PHI was actually acquired or viewed
Extent of mitigated

Written Notice Required Within Short Time:
• To Every Individual Affected
• To Federal Government - Department of Health & Human Services/Office for Civil Rights ("OCR")
• To Media – If >500 individuals

The “clock” starts when you become aware!
The privacy rule gives patients control over their Protected Health Information (PHI). You need to know…

- Patients’ rights regarding the use of their PHI
- Key terms and general rules you can apply
- When you can share patient information and when there are limits to what can be used or shared
Patient Rights

The Privacy Rule gives patients the right to:

- have their PHI protected;
- obtain/access to their records;
- request that PHI in their records be changed (amended);
- ask to limit/restrict how their PHI is used or shared;
- ask to be contacted in a specific way, such as at home, not at work;
- get a list of certain disclosures of their PHI.
Notice of Privacy Practices (NPP)

- Providers and Health Plans must have a Notice of Privacy Practices (NPP) - provides a detailed description of the various uses and disclosures of PHI that are permissible without obtaining a patient’s authorization.

- You can access our NPP here.

- In general, anytime you release patient information for a reason unrelated to treatment, payment (e.g., billing) or healthcare operations (e.g., quality review), an authorization is required.

- Patients are asked to acknowledge receipt of the Notice of Privacy Practices on their first encounter at Michigan Medicine, to note in writing that they were offered or received a copy of the Notice.
Covered Entities

- A Covered Entity is a health care provider or a health plan that submits bills/claims electronically (e.g., hospitals, physicians, health plans, etc.)
- Covered Entities and Business Associates (and any Subcontractors of business associates) that use or access PHI on a Covered Entity’s behalf are subject to HIPAA.
- The University of Michigan is a Hybrid Covered Entity. Click here for more information.
Protected Health Information (PHI)

- For Michigan Medicine, PHI is health information about a patient created or received by health care providers. PHI includes information:
  - Sent or stored in any form (written, verbal, electronic);
  - That identifies the patient or can be used to identify the patient;
  - That is about a patient’s past, present and/or future treatment and payment of services.

PHI is any health information that can lead to the identity of the individual or contents of the information can be used to make a reasonable assumption as to the individual’s identity.
Key Terms

**PHI includes one or more of these identifiers:**

- Names
- Address including Zip Codes
- All Dates
- Telephone & Fax Numbers
- Email Addresses
- Social Security Number
- Medical Record Number
- Health Plan Number
- License Number
- Vehicle Identification Number
- Account Number
- Biometric Identifier
- Full Face Photo
- Any Other Unique Identifying Number, Characteristic, or Code
Question:

If you have a document or an electronic device such as a thumb/flash drive that contains patient initials and medical record number(s), does your document or device contain PHI?
Test Yourself

Answer: Yes.

Your document or device contains data elements – patient initials with medical record numbers – which can be used to identify the patient(s). It does not matter that the full patient name is not included.

PHI is *anything* that is received, sent or stored in any form by a health care provider that identifies the patient or can be used to identify the patient and is about a patient’s past, present and/or future treatment and payment of services.

In other words: PHI is any health information that can lead to the identity of the individual or the contents of the information can be used to make a reasonable assumption as to the individual’s identity.
Test Yourself

Take Away:

Do not use patient identifiers if you do not need to do so.

If using patient identifiers cannot be avoided, only use what is minimum necessary and nothing more.
Treatment, Payment and Operations (TPO)

- **Treatment [T]:** Various activities related to patient care.

- **Payment [P]:** Various activities related to paying for or getting paid for health care services.

- **Health Care Operations [O]:** Day-to-day business activities of the covered entity, such as planning, management, training, improving quality, and education of workforce.

- **NOTE:** Research is not considered TPO. Written patient authorization is required to access PHI for research unless an authorization waiver is approved by the IRB. See the HIPAA course on research for more information.
Minimum Necessary Rule

Generally, the amount of PHI used, shared, accessed or requested must be limited to only what is needed. Workers should access or use only the PHI necessary to carry out their job responsibilities.

For Example:

When we bill for a blood test, the billing company is not provided with the entire medical record. Rather, only the applicable procedure code(s), etc. are included for the bill to be processed and paid.
Workers should have access to and only use PHI required to fulfill their job responsibilities.

For example, someone who delivers food trays to patients may need PHI about the patient’s diet (e.g., low salt), but does not need to know why the patient is in the hospital.
In some cases, the “Minimum Necessary” Rule does not apply, such as:

- When PHI is shared or requested among health care providers for treatment;
- Disclosures to the patient;
- Authorized uses or disclosures approved by the patient.
**Key Terms**

- **“Use” of PHI?**
  - Use of PHI refers to how PHI is *internally* accessed, shared and utilized by the covered entity.

- **“Disclosure” of PHI:**
  - Disclosure of PHI refers to how PHI is shared with individuals or entities externally (external to the covered entity.)

- **Different rules apply to Use vs Disclosure of PHI**
Types of Disclosures

There are 3 types of disclosures, depending on whether there is an authorization requirement:

1. No Authorization Required
2. No Authorization Required, but Must Give Opportunity to Object
3. Authorization Required

Each one of these is covered separately in the next three slides
Types of Disclosures

**Type 1: No authorization is required to make the following disclosures:**

- To disclose PHI to the patient

- To use or disclose PHI for treatment, payment or healthcare operations (Examples: A physician discusses the patient’s condition with another consulting physician; a health provider submits a bill to a health insurance plan; and patient record reviews for quality improvement purposes)

- Certain disclosures required by law (for example, public health reporting of diseases, child abuse/neglect cases, etc.)
Types of Disclosures

Type 2: No Authorization is required, but opportunity to object must be given

- The Patient must be offered an “opportunity to object” to disclosure before discussing PHI with a patient’s family or friends

Before discussing patient information in an exam room, ask the patient if it is okay to discuss information in front of the family member/friend. Best practice is to just ask the family member or friend to leave the room for private discussions, especially if the information is highly confidential.

- Limited PHI (e.g., patient’s hospital room/location number) is included in the “Hospital Directory” and provided to clergy members, but patients are offered option to “Opt Out” of the directory
Types of Disclosures

Type 3: Written authorization is required from the patient

- To access, use or disclose PHI for research (unless an Institutional Review Board such as the U-M IRBMED approves a waiver of authorization)

- To conduct certain fundraising activities

- For certain marketing activities and any sale of PHI

There are additional HIPAA Training Modules for individuals involved in Research, Fundraising and/or Marketing Activities. Contact the Compliance Office at 734-615-4400
Incidental Disclosures

Some disclosures are not avoidable and are permitted under HIPAA. These are “Incidental Disclosures”

- Examples: Calling a patient name in a waiting room; a hospital patient in a 2-bed room hears a physician speaking to the other patient.

- HIPAA requires reasonable steps to be taken to minimize incidental disclosures such as:
  - Speak quietly when discussing PHI in open areas such as the recovery room, emergency department, etc.;
  - Do not discuss PHI in public hallways, elevators or other public locations such as the cafeteria;

Follow the minimum necessary rule to minimize incidental disclosures
State and Federal laws provide greater protection than HIPAA in some cases. These “Highly Confidential” areas include:

- Mental Health and Substance Abuse
- HIV/AIDS Testing or Treatment
- Genetic Tests/Information
- Certain communicable diseases (e.g., sexually transmitted disease, hepatitis, etc.)
- Certain diagnostic and treatment services rendered to minors like pregnancy and prenatal care
- If you have questions about handling highly confidential information, ask your supervisor or contact hipaaquestions@umich.edu.

Discuss with your supervisor about special precautions to protect highly confidential information and any authorization requirements for disclosures.
Test Yourself

Question:
You are a nurse asking a newly admitted patient a number of questions as part of the admission process. You see that the patient is HIV positive. Would it be appropriate for you to discuss the patient’s HIV status in front of the patient’s accompanying family member?
Because HIV status is highly confidential information, it is subject to greater protections beyond HIPAA. If you need to discuss the patient’s HIV status, take precautions to prevent others from overhearing. In this scenario, you should not discuss any highly confidential information in front of the patient’s family member without the patient’s permission. Instead, have the family member leave the room before proceeding to complete the admission paperwork.
Accessing Electronic PHI

- Use your electronic access to information systems only to perform your job-related duties and only access PHI on a need-to-know basis
- All electronic systems are audited – an audit log of all accesses is maintained and monitored to protect patient privacy
- Inappropriate access to a patient’s electronic medical record leads to disciplinary action, up to and including termination and even possible criminal liability/penalties such as jail time and criminal fines
Test Yourself

Question:
Is it okay to look up a coworker’s address in the electronic medical record to send a get well card?
Test Yourself

Answer: No.

Do not look up a coworker or any other person in the electronic medical record to obtain an address or see if they are a patient. Use public options (e.g., internet search, ask the person, etc.) to obtain the address/other information. Accessing the electronic medical record system for purposes other than to do your job is not permitted. Inappropriate access to a patient’s electronic medical record results in disciplinary action, up to and including discharge.

NOTE: It is inappropriate to search for a patient and view the demographics screen, even if you don’t view other aspects of the record.
Right of Access to Medical Information

- Patients have the right to obtain a copy of their medical records – generally within 30 days of their request. Some exceptions exist.
- Patients have a right to request an electronic copy of their health information held in an electronic medical record system.
- If a patient requests copies – paper or electronic – direct them to the Medical Records/Health Information Management Department which will manage the request within the appropriate time frames.
Information Security

- Use strong break passwords
- Never share your password with another person
- Log off from all electronic record applications (e.g., the electronic medical record system)
- Secure all electronic records (e.g., encryption) – Call IT support to securely set up electronic devices, etc.
- Do not save any PHI on unencrypted portable electronic devices such as laptop computers, flash/thumb drives, whether you personally own the device or if it was purchased by Michigan Medicine
- Immediately report to IT Support if any of these devices are lost or stolen
Protecting Electronic Data

Sensitive information stored on computers and other electronic devices is subject to threat of invasion (e.g., viruses, malware, etc.). To do avoid these threats:

- Be attentive - don’t click on attachments or links in suspicious email (phishing emails)

Refer to:

http://www.safecomputing.umich.edu/main/phishing_alerts/
http://www.itcs.umich.edu/help/faq/viruses.php
Internet Threats

- Phishing
- Malware
- Personal E-mail
- Cloud Computing
Phishing is unwanted e-mail ("spam") that tries to trick you into revealing confidential information, like your user name and passwords, credit card information, etc.

Do NOT reply to any e-mail message that might be a phishing attempt.

Do NOT click on links or download files if you are not sure they are safe.

See [http://www.med.umich.edu/u/compliance/area/phishing.htm](http://www.med.umich.edu/u/compliance/area/phishing.htm) for more information.
Cloud computing gives access to computer files and programs over the internet, and may include backing up or synchronizing those files with a cloud service provider. Gmail, Google Calendar, Google Docs, etc. are examples of “Cloud Services”.

NEVER store PHI or other sensitive information on public cloud services*

*NOTE: Use of Cloud Service Provider(s) requires special contracts and information security specifications. See the University of Michigan Sensitive Data Guide - at https://www.safecomputing.umich.edu/dataguide/ - for the latest information on what services can be used to store PHI.
Internet Threats: Personal Email

Michigan Medicine Users: Email within the Michigan Medicine E-mail System is secure (using your “@med.umich.edu” e-mail to others within the same system.)

Michigan Medicine Users: E-mail sent outside of the Michigan Medicine E-mail System is NOT secure. Examples: “@umich.edu” or “@gmail.com” email account

Internet Threats

Personal E-mail

Do NOT transmit PHI or other sensitive information to or from your personal email
Malware is software designed to harm your computer. Malware gets into your computer through e-mail attachments, compromised websites, etc.

Examples: Computer virus, worms and spyware. It can destroy your data and cause inappropriate access to or disclosure of sensitive information such as PHI.

Malware is blocked through up-to-date antivirus software programs and antispyware scanning program. Do not click on links or attachments in suspicious emails.
Emailing PHI

- For Michigan Medicine E-mail Users: E-mail to e-mail transmission within the Michigan Medicine E-mail System (“med.umich.edu”) is considered secure, but use/send only the minimum necessary PHI.
  - E-mail from the Michigan Medicine e-mail system to any other system is not secure (This includes email to a “umich.edu” address or to a hotmail®, yahoo®, comcast®, or other type of personal e-mail address).

- For non-Michigan Medicine users: Check with your supervisor for department-specific procedures for emailing PHI.

- Do not send documents or files that contain PHI from the Michigan Medicine E-mail System to an external system or vice versa. Use a secure file transfer system such as MiShare or check with your supervisor. Click here for more information.
When there is a Breach, the Covered Entity must provide written “Breach” notice:

- To Every Individual Affected
- To Federal Government - Department of Health & Human Services/Office for Civil Rights (“OCR”)
- To Media – If >500 individuals residents

For sending these notices, Michigan Medicine is subject to a tight time frame (The “clock” starts ticking the moment you become aware of a privacy or information security violation.

Immediately Report any HIPAA concern!
Disciplinary action must be applied to workforce members for violating HIPAA, up to and including discharge.

Most common HIPAA violation resulting in termination of employment: Inappropriate access to electronic medical record(s)
Practical Applications

• You can talk with other providers or with patients, even if you may be overheard, but use reasonable precautions to avoid being overheard (move to private location, speak with lower volume, etc.)

• You can discuss a patient’s condition with the patient, other providers, or with family members (unless the patient objects) over the phone or even in a patient’s semi-private room

• You can talk about patient conditions for education of our employees and students (de-identify if possible, or use minimum necessary)
• Voice messages can be left or with those who answer the phone, limited to minimum necessary (but do not include highly sensitive information)
• Try to honor patient requests about how and where to reach them (e.g., cell phone only, not via home phone number)
• Patients’ names can be called in waiting rooms
• Patient care signs are allowed outside inpatient rooms (e.g., dietary restriction sign)
• Whiteboards/Locator boards are allowed in clinical spaces
• PHI can be shared in group therapy settings for treatment
Authorization is usually needed to access/use PHI for research purposes

• Example: A researcher cannot enroll a patient in a study without an authorization that includes what the PHI will be used for, who can use it and for how long.

Note: If you are involved in research, see the “HIPAA and Research” content for more information

Contact IRBMed for assistance.

Contact the Michigan Medicine Corporate Compliance Office if you have questions at 734-615-4400 or by email compliance-group@med.umich.edu
FAQs

• You must complete the next section on Frequently Asked Questions (FAQs).

• External Individuals who are taking this module prior to interacting with Michigan Medicine: After reviewing the FAQ section, be sure to click on and complete the form on the last slide of the FAQ section. **This is the only way for you to get a certificate and credit for this education module.**
Q: What if I overhear information about a patient while I am at work?

A: This is an incidental disclosure under HIPAA. Reasonable precautions must be taken to minimize incidental disclosure, and you are obligated to keep the information confidential.

HIPAA is not meant to prevent health care team members from communicating with each other and their patients during the course of treatment. These "incidental disclosures" are allowed under HIPAA with reasonable precautions.
Q: What should I do if a government agency or law enforcement person requests information about a patient?

A: Inform the law enforcement official that you need to contact one of our attorneys to work with the officer. Contact your supervisor or the Michigan Medicine’ attorneys at 764-2178 (the attorney on call can be contacted through the hospital operator.) Those who do work directly with law enforcement receive special training on the special rules about disclosing patient information to law enforcement authorities.
Q: When speaking to a patient, and friends or family members are in the room, do I assume the patient has given permission to discuss their PHI in front of these persons?

A: Do not assume it is okay to speak in front of the other people. Ask the patient if it okay to discuss their PHI in front of the person(s). If highly sensitive information needs to be discussed (HIV status for example), then ask the person(s) to leave the room before beginning any discussion about the highly sensitive information.
Q: Can someone else pick up a patient's prescription, x-rays, or medical supplies?

A: Yes, it is okay to give the prescription, x-rays or medical supplies to that individual, using your professional judgment and what is in the patient’s best interests.
Q: I have students and temporary staff who will only be here a short time. They need computer access. Can I have them log them in using my user name and password?

A: No. It is against policy to allow any staff, including temporary staff, to use another employee's log in and/or password for computer access. Sharing your password with another person can result in disciplinary action, up to and including termination.
Q: How do I get rid of papers or electronic devices that include PHI?

A: Papers containing PHI need to be shredded or placed in a designated confidential recycling bin (one of the locked confidential blue bins).

Electronic devices (e.g., thumb/flash drives, hard drives, etc.) must be physically destroyed or “electronically shredded”. Contact your IT Support for assistance.
Certificate and Credit for Course Completion

If you are **associated with Michigan Medicine:**

Close this window and make sure you complete the remainder of the learning activity in the Mlearning system to obtain credit for taking this course.

If you are not **associated with Michigan Medicine:**

Download and fill out a printable PDF certificate. Give it to your sponsoring department to show you’ve taken this course. Click here to download and complete a printable PDF certificate.