University of Michigan Health System

Are you in the correct place?

This is a training module on the HIPAA Privacy and Security rules.

- Did you access this module through Mlearning?
  - If yes: Continue with this module
  - If not: If you are associated with UMHS (University of Michigan Health System), and did NOT access this course through MLearning, you will not get credit unless you log into MLearning, and enroll in the course - Log into Mlearning, search for "HIPAA" and enroll in course *PRIV-10000, HIPAA for Non-clinicians with no research responsibilities*.
- If you DID access this through MLearning OR you are NOT associated with UMHS, continue with this module.

University of Michigan Health System

HIPAA Learning Module: Basic

HIPAA Privacy and Security Rules… The Basics

University of Michigan

Updated 09/23/2013

HIPAA Learning Module: Basic
Our Commitment to Privacy

- **The University of Michigan and the University of Michigan Health System 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 <u>all of us.</u>**

HIPAA Learning Module: Basic Learning Objectives

- **Key things for you to know:**
  - ✓ **Just Ask! Check with your supervisor or the UMHS Compliance Office *whenever* you have a question or concern**
  - ✓ **HIPAA 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**
  - ✓ **UMHS' Notice of Privacy Practices (NPP) explains patients' rights regarding the use of their health information**
  - ✓ **Your role in protecting patient information stored electronically**

University of Michigan Health System

Reporting Concerns

- Report through **Supervisor/Manager**
- Otherwise, **Compliance Office**:
  - ✓By Phone: 615-4400
  - ✓By Email: Compliance-Group@med.umich.edu
  - ✓Website: http://www.med.umich.edu/compliance/index.htm
- Anonymous **Compliance Hotline or Online Reporting:**
  - ✓Phone: (866) 990-0111
  - ✓Online Reporting: http://www.tnwinc.com/WebReport/

Not sure? ….Report it anyway.
Too late? ….Report it anyway.
Already told us? ….Report it again!

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

University of Michigan Health System

OVERVIEW

What this means to you and our patients

The privacy rule gives patients more control over their Protected Health Information (PHI). So you need to know…

- **Patients' rights regarding the use of their PHI;**
- **Key terms and general rules that you can apply; and,**
- **When you can share patient information and when there are limits to what can be used or shared.**

University of Michigan Health System

OVERVIEW
Patient Rights

The Privacy Rule gives patients the right to:

- **have their PHI protected;**
- **inspect and copy their records;**
- **request that PHI in their records be corrected or changed;**
- **ask for limits on how their PHI is used or shared;**
- **ask that they be contacted in a specific way, such as at work and not at home;**
- **get a list of disclosures made of their PHI.**

HIPAA Learning Module: Basic Key Terms

University of Michigan Health System

Notice of Privacy Practices (NPP)

- **Providers and Health Plans must have a Notice of Privacy Practices (NPP) - it provides a detailed description of the various uses and disclosures of PHI that are permissible without obtaining a patient's authorization.**
- **You can access the UMHS' NPP here.**
- **In general, anytime you release patient information for a reason unrelated to treatment, payment (e.g., billing) or healthcare operations (TPO), an authorization is required.**

University of Michigan Health System

GENERAL RULES

Notice of Privacy Practices

- **Patients are asked to acknowledge receipt of the Privacy Notice on their first encounter at UMHS, to note in writing that they received a copy of the Notice.**

HIPAA Learning Module: Basic Key Terms

University of Michigan Health System

Covered Entities

- **A Covered Entity is a health care provider or a health plan that submits bills electronically.**
  - **Examples include: Health Systems such as the University of Michigan Health System; Hospitals; Physicians; Health Plans such as Blue Cross Blue Shield of Michigan; etc.**
- **All Covered Entities, along with their Business Associates and any subcontractors of their business associates, that use or access patient information on the Covered Entity's behalf are subject to HIPAA.**
- **The University of Michigan is a *Hybrid Covered Entity*. Click here for more information.**

HIPAA Learning Module: Basic Key Terms

University of Michigan Health System

Protected Health Information (PHI)

- **PHI is health information about a patient created or received by health care providers and health plans. 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 the contents of the information can be used to make a reasonable assumption as to the individual's identity.

University of Michigan Health System

HIPAA Learning Module: Basic *Key Terms*

PHI includes one or more of these identifiers:

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

Test Yourself

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?

University of Michigan Health System

Test Yourself

Answer: Yes.

Your document or device contains patient identifiers – patient initials and medical record number – that 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 or health plan:

- 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.

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 the use of patient identifiers cannot be avoided, then only use those identifiers that you minimally need and nothing more.

HIPAA Learning Module: Basic Key Terms

University of Michigan Health System

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]: Generally refers to day-to-day activities of a covered entity, such as planning, management, training, improving quality, providing services, and education.**
- NOTE: Research is not considered TPO. Written patient authorization is required to access PHI for research unless authorization waiver is approved by the IRB. See the education program on research for more information.

HIPAA Learning Module: Basic Key Terms

University of Michigan Health System

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, we only provide the applicable diagnosis and procedure codes, etc. for the bill to be processed and paid.

University of Michigan Health System

Key Term
Minimum Necessary

- Workers should have only such PHI as their job responsibilities require.

For example, someone who delivers food trays to patients may need PHI about the patient's diet, but does not need to know why the patient is in the hospital.

University of Michigan Health System

KEY TERM

Minimum Necessary – Cont'd.

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 a patient about his or her own PHI;
- Authorized uses or disclosures approved by the patient; and,

HIPAA Learning Module: Basic Key Terms

University of Michigan Health System

- **What is "Use" of PHI?**
  - Use of PHI refers to how PHI is *internally* accessed, shared and utilized by the covered entity. For UMHS, "use" refers to accessing, sharing, and utilizing PHI *within* the health system. For other university providers such as University Health Service (UHS), "use" refers to accessing, sharing, and utilizing PHI within UHS
- **What is "Disclosure" of PHI:**
  - Disclosure of PHI refers to how PHI is shared with individuals or entities externally. For UMHS, "disclosure" refers to sharing PHI with others *outside of (external to)* the health system.
- **Different rules apply to Use vs Disclosure of PHI**

University of Michigan Health System

HIPAA Learning Module: Basic Key Terms

What is an Authorization?

- **A written permission signed by the patient or the patient's personal representative (e.g., a parent) to allow a Covered Entity to Use or Disclose a patient's PHI for reasons generally not related to Treatment, Payment or Healthcare Operations (TPO purposes).**
- **The Authorization must include: A detailed description of the PHI to be disclosed, who will make the disclosure, to whom the disclosure will be made, expiration date, and the purpose of the disclosure.**

University of Michigan Health System

HIPAA Learning Module: Basic Types of Disclosures

There are 3 Types of Disclosures:

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

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

University of Michigan Health System

HIPAA Learning Module: Basic Types of Disclosures

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 submit a bill to a health insurance plan; and patient records are reviewed for quality improvement purposes)

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

HIPAA Learning Module: Basic Types of Disclosures

University of Michigan Health System

2. **No Authorization is Required, but Must Offer Opportunity to Object:**

- The Patient must be offered an opportunity to object 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 patient's family member or friend. Alternatively, you can ask the family member or friend to leave, especially if the information is highly confidential.

- Limited PHI (e.g., patient's hospital room/location number) is included in the "Hospital Directory" but patients are offered an "Opt Out" opportunity and certain disclosures to clergy members

HIPAA Learning Module: Basic Types of Disclosures

University of Michigan Health System

3. **Authorization Is Required:**

Written authorization is required from the patient for the following:

– 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 marketing activities and sale of PHI

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

HIPAA Learning Module: Basic Incidental Disclosures

University of Michigan Health System

Incidental Disclosures

Some disclosures are not completely avoidable. These are permitted under HIPAA and are called "Incidental Disclosures"

- Examples of "Incidental Disclosures": Visitors hear a patient's name called out 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:
  - Speaking in soft tones 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;

Only use the minimum necessary to minimize incidental disclosures

University of Michigan Health System

HIPAA Learning Module: Basic "Highly Confidential" Information

Highly Confidential Information

- Michigan and other Federal law provide even more 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

University of Michigan Health System

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?

University of Michigan Health System

Test Yourself

Answer: No.

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, you must take extra precautions to prevent others (including other patients) from overhearing the information. In this scenario, you should not discuss any highly confidential information in front of the patient's family member without patient's permission. Instead, require that the family member to leave the room before proceeding with gathering your information to complete your admission paperwork.

HIPAA Learning Module: Basic 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 – a log of all accesses is maintained and designed to protect patient privacy
- Inappropriate access to a patient's electronic medical record can lead to disciplinary action, up to and including termination from employment

University of Michigan Health System

Test Yourself

Question:

Would it be permissible for you to look up a coworker's address in the electronic medical record so you can send the coworker a get well card?

University of Michigan Health System

Test Yourself

Answer: No.

You cannot access a coworker's electronic medical record. If you need information about a coworker, check with your supervisor. Accessing the electronic medical record system for purposes other than to complete your job responsibilities is not permitted. Inappropriate access to a patient's electronic medical record can lead to disciplinary action, up to and including discharge.

University of Michigan Health System

HIPAA Learning Module: Basic

Right of Access to Medical Record Information

- Patients have the right to obtain a copy of their medical record – 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 request copies – paper or electronic – direct them to the Medical Records/Health Information Management Department which will manage the request within the appropriate time frames

University of Michigan Health System

HIPAA Learning Module: Basic

Sharing Immunization Records

- HIPAA allows Health Care Providers to share immunization records directly with schools with either written or verbal consent from the parent or guardian (for minor child) or from the individual (for adults)
- If verbal consent is obtained, document the consent in the patient's medical record
- Best Practice at UMHS: Immunization records can be obtained directly by the patient or, the parent in the case of a minor, through the patient portal (MyChart). Encourage the person to sign up for the patient portal and they can then access immunization records directly and provide the record to the school themselves

HIPAA Learning Module: Basic

Information Security

- Use difficult to break passwords
- Never share your password with another person
- Log off from all electronic record applications (e.g., the electronic medical record system) before walking away from the computer
- Secure all electronic records using encryption – Call IT support to set up secure electronic systems
- Do not save any PHI on unencrypted portable electronic devices such as laptop computers, flash/thumb drives, electronic tablets, etc., whether you personally own the device or if it was purchased by UMHS
- Immediately report to your Supervisor or the UMHS Compliance Office if any of these devices are lost or stolen

HIPAA Learning Module: Basic Protecting Electronic Data

University of Michigan Health System

Sensitive information stored on computers and other electronic devices must be appropriately secured. To do this, you should:

- **Avoid internet threats**
- **Encrypt the data**
- **Create and use strong passwords**
- **Secure computers and other mobile devices**
- **Report immediately if the device is lost or stolen**

Refer to:

http://www.safecomputing.umich.edu/main/phishing_alerts/

http://www.itcs.umich.edu/help/faq/viruses.php

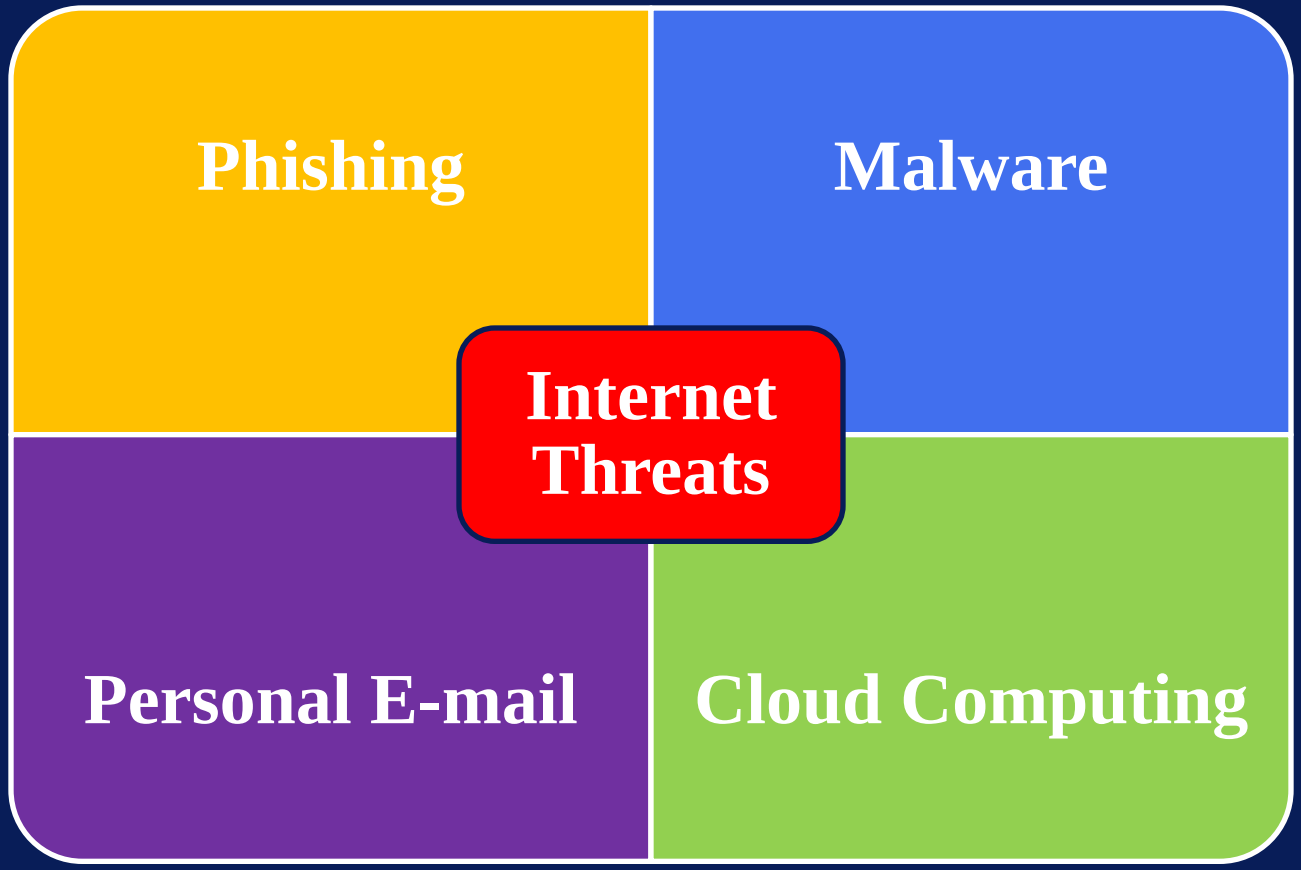
HIPAA Learning Module: Basic Strong Passwords

University of Michigan Health System

In addition to encryption, a "strong" password is an important way to protect confidential information stored electronically

- Use at least 8 characters (9 or more is ideal), unless limited by system capabilities
- Use at least 3 of the following character types:
  - lowercase letters
  - uppercase letters
  - numbers
  - symbols (@, %, $, &, etc.)
  - punctuation marks (?, !, etc.)
- Do not use names, identifiers, simple phrases or words in any language ("password", "michigan", your user ID, "hello2u", etc.)
- Do not use sequences of characters or keys ("123456", "abcdef", "qwerty", etc.)
- Use different passwords on different systems so if one password is lost or stolen, there is no risk to the other systems
- To help you remember your password, create an acronym from a phrase and substitute letters with numbers and symbols. For example, pick a phrase that is meaningful to you, such as "Moose Tracks ice cream is better with sprinkles". Using that phrase as your guide, you might use "MT1c1bw$" (where the "i"s have been replaced with "1"s and the "s" with "$") for your password
- For more information, see http://www.itcs.umich.edu/itcsdocs/r1162/

HIPAA Learning Module: Basic Internet Threats



HIPAA Learning Module: Basic Internet Threats - Phishing

University of Michigan Health System

Phishing

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.

Internet Threats

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 for more information.

HIPAA Learning Module: Basic Internet Threats: Malware

University of Michigan Health System

Malware

Malware is software designed to harm your computer. Malware gets into your computer through e-mail attachments, compromised websites, etc.

Internet Threats

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 an up-to-date antivirus software program and antispyware scanning program. Contact your IT Support for help.

HIPAA Learning Module: Basic Internet Threats: Cloud Computing

University of Michigan Health System

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"

Internet Threats

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

Cloud Computing

*A Business Associate Agreement is required before doing so. As of 09/2013, no cloud service Provider has entered into a BAA with either U of M or with the UMHS.

HIPAA Learning Module: Basic Internet Threats: Personal Email

University of Michigan Health System

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

UMHS Users: E-mail sent outside of the UMHS 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

HIPAA Learning Module: Basic Emailing PHI

- For UMHS E-mail Users: E-mail to e-mail transmission within the UMHS E-mail System ("med.umich.edu") is considered secure, but use/send only the minimum necessary PHI.
  - E-mail from the UMHS 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-UMHS users: Check with your supervisor for department-specific procedures for emailing PHI
- Do not send documents or files that contain PHI from the UMHS 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.

HIPAA Learning Module: Basic Encryption

Proper Encryption makes data on computers and other electronic devices unreadable. Users must have an "encryption key" to "unlock" the encryption to access the data.

All sensitive information, including PHI, must be encrypted prior to being sent electronically *outside* of the University of Michigan Health System. These outside/external communications include electronic communications sent from persons within UMHS to persons within U of M.

HIPAA Learning Module: Basic Encryption

Encryption Resources

At UMHS, Contact Medical Center Information Technology (MCIT) for assistance with encryption.

For Non-UMHS: Check with your supervisor and work with your IT Support for determining appropriate encryption methods available to you. See http://safecomputing.umich.edu/protect-personal/what-is-encryption.php for more information.

University of Michigan Health System

Test Yourself

Question:

Which of the following is a strong password?

A. Michigan1

B. 1234abcd

C. MT1c1bw$

University of Michigan Health System

Test Yourself

Answer: C.

A. Michigan1	This is a weak password. Do not use names, identifiers, simple phrases or words in any language ("password", "michigan", your user ID, "hello2u", etc.)
B. 1234abcd	This is a weak password. Do not use sequences of characters or keys ("123456", "abcdef", "qwerty", etc.)
C. MT1c1bw$	This is a strong password. Mix numbers, letters and special characters to create a strong password

HIPAA Learning Module: Basic
Securing computers & mobile devices

Computers, Etc.

- Log out or Lock your computer when you leave
- Position your screen away from public areas
- Place Printers and fax machines where PHI can be printed should not be positioned in public areas (like waiting rooms)

Laptops & Tablets

Smart Phones & Cell Phones

Cameras & Recorders

Thumb Drives, Memory Cards, CDs/DVDs & External Hard Drives

Mobile Devices

- Mobile devices with PHI or other sensitive information should be encrypted and password protected. If not able to encrypt, they should physically secured in a locked drawer or safe

HIPAA Learning Module: Basic
Report Lost or Stolen Devices

University of Michigan Health System

Report immediately if the device is lost or stolen

Even if you just suspect a security incident (e.g., your laptop might have been stolen, but you don't know for sure), immediately notify your IT Service Provider.

Within UMHS - Contact the MCIT Help Desk at (734) 936-8000.

HIPAA Learning Module: Basic HIPAA 2013 Modifications

HIPAA was modified between 2009 and 2013.

Under these modifications…

HIPAA Learning Module: Basic

HIPAA 2013 Modifications

All violations are PRESUMED a "BREACH"

As a result: All HIPAA incidents must be analyzed under a 4-prong test to overcome this Breach presumption. T*his analysis is conducted by the UMHS Compliance Office. This analysis must be documented and retained for 6 years. (Thus, do NOT do this analysis yourself!)*

You don't need to know the 4-prong test, **BUT YOU MUST REPORT ALL PRIVACY CONCERNS!**

4-prong test:

1. Nature and extent of information involved, including the types of identifiers and risk of re-identification
2. Unauthorized person who used the PHI or to whom it was disclosed
3. Whether the PHI was actually acquired or viewed
4. Extent to which risk to the PHI has been mitigated

HIPAA Learning Module: Basic HIPAA 2013 Modifications

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 residing in single state or "jurisdiction" (e.g., SE Michigan)

The Covered Entity is subject to tight time frames for sending these breach notices

So it is important that you <u>Immediately</u> report all HIPAA concerns!

HIPAA Learning Module: Basic HIPAA 2013 Modifications

University of Michigan Health System

When is a "Breach" discovered?

Breach is "discovered" as soon as an employee or another agent knows or should reasonably have known of the incident causing the breach

The "clock" will start ticking the moment *you* become aware of a privacy or information security violation

Your duty: Report the violation immediately – even just a suspected violation

HIPAA Learning Module: Basic HIPAA 2013 Modifications

Under the 2013 modifications:

- **Civil Fines Increased Up to $1.5 million** per HIPAA violation per year (prior max was $25,000/violation/year)
- Criminal fines: $250,000/up to 10 years imprisonment, **criminal penalties expanded to individuals.** NOTE: Individuals (This means You!) can be subject to criminal prosecution, fines and imprisonment

HIPAA Learning Module: Basic Disciplinary Action

The Covered Entity's policies require disciplinary action be taken against individuals for violating HIPAA, up to and including discharge.

University of Michigan Health System

HIPAA Learning Module: Basic

ADDITIONAL INFORMATION FOR YOUR AWARENESS…

HIPAA Learning Module: Basic Key Terms

University of Michigan Health System

Business Associate:

- Vendors who have access to or use PHI on our behalf must have a Business Associate Agreement - a signed agreement promising to keep PHI confidential in accordance with HIPAA.
- Example: A company developing order entry software must see actual PHI so they would need a written agreement.

NOTE: Contact the UM Procurement Office for help to determine if a Business Associate Agreement is needed with a vendor.

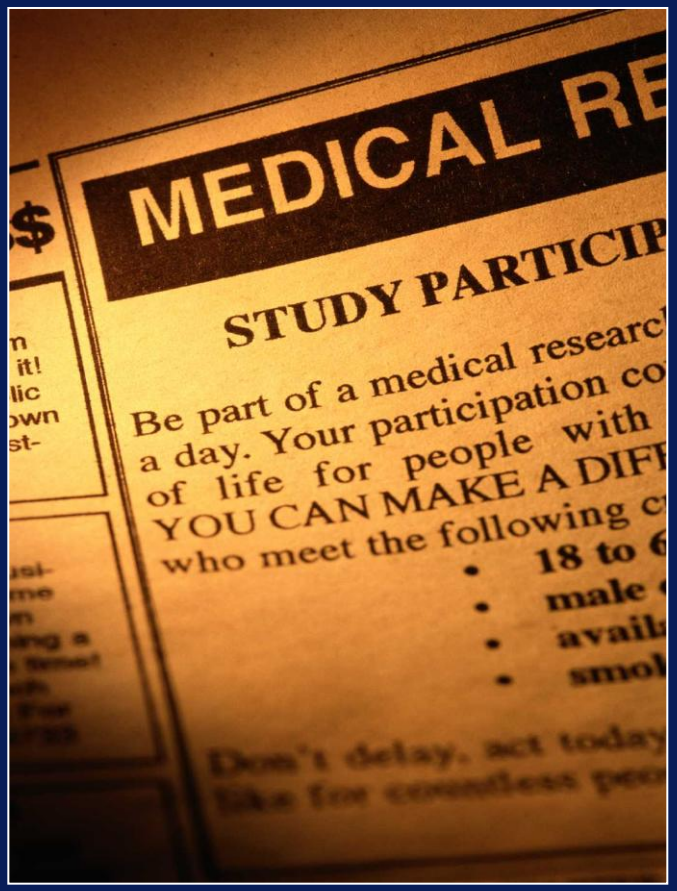
You may need to take the additional HIPAA training module on business associates, depending on your job responsibilities. Talk to your Supervisor or call the UMHS Compliance Office (615-4400)

RESEARCH

Written Permission IS Needed

- **Patient permission or "*authorization*" is usually needed to use or share PHI for research.**

For 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.



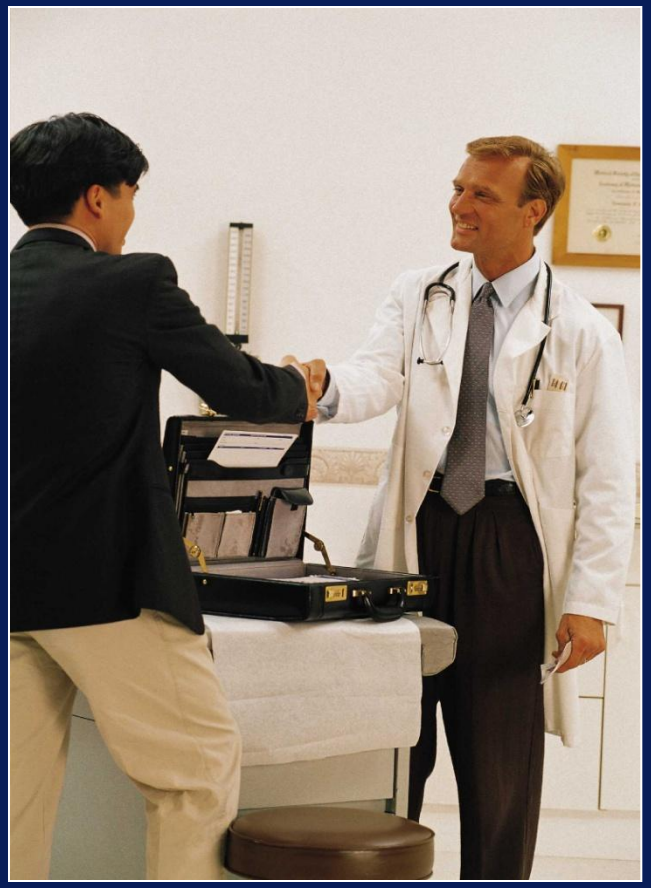
MARKETING AND FUNDRAISING

Written Permission IS Needed

- **Patient permission or "*authorization*" is needed to use or share PHI for certain marketing and fund-raising activities.**

  For example, a doctor cannot give a diaper company the names of pregnant patients without an authorization that includes what the PHI will be used for, who can use it and for how long.

  NOTE: Contact t*he UMHS Compliance Office for more information about fundraising and marketing of 3rd party products or services.*



University of Michigan Health System

Questions?

- **For questions about HIPAA:**
  http://www.med.umich.edu/u/compliance/area/privacy/index.htm

- **For more information:**

  http://www.hhs.gov/ocr/privacy/

  http://www.cms.hhs.gov/HIPAAGenInfo/

University of Michigan Health System

FAQs

- **You must complete the next section on Frequently Asked Questions (FAQs).**
- **Click HERE to Continue to the FAQ Section.**
- **External Individuals who are taking this module prior to interacting with UMHS: 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.**