Module 3

Patient Information Safety
# Learning Guide

<table>
<thead>
<tr>
<th>Directions</th>
<th>Reference Material</th>
<th>Learning Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go through <strong>each</strong> slide and read/listen to the information (this module will be marked as ‘Completed Unsuccessfully’ until you have viewed all of the slides)</td>
<td>Throughout the Module there will be notes like this that will list additional materials to access. Refer to your <strong>‘2016 AME Guide’</strong> (provided at the beginning of this training and as a downloadable attachment)</td>
<td>Learning Goals are outlined so you are able to identify what is expected of you upon completion of the training.</td>
</tr>
</tbody>
</table>

**Access and review** documents as indicated by searching online or using the links provided in the ‘2016 AME Guide’
Module 3: Information Safety

- **Lesson 3.1: HIPAA And Protected Health Information**
  - *Topic 3.1.1: HIPAA And Releasing Information To Law Enforcement*

- **Lesson 3.2: Privacy Incidents**
  - *Topic 3.2.1: How To Prevent: Misdirected Or Lost Documents*
  - *Topic 3.2.2: How To Prevent: Paperwork Handoff Errors*
  - *Topic 3.2.3: How To Prevent: Inappropriate Access*
  - *Topic 3.2.4: How To Prevent: Oral Disclosures Of PHI*
  - *Topic 3.2.5: How To Prevent: Social Media Violations*
  - *Topic 3.2.6: How To Protect: Information Security*
Learning Goals

- Define HIPAA and PHI
- Identify your responsibilities for protecting patient, associate, and organizational information
- Select what equals de-identified information
- Name ways to prevent privacy incidents
• You have the responsibility to protect patient, associate, and organizational information.

• This means following:
  – HIPAA law
  – Standards on protected health information
  – MHS Information Security and Privacy Policy
  – MHS HIPAA Privacy and Security Policies
  – MHS Network Access Agreement

• For additional information on keeping protected health information (PHI) safe, contact
  – Information Security at ext. 14811
  – Corporate Compliance at ext. 11983
Module 3:
Information Safety

Lesson 3.1

HIPAA and Protected Health Information
HIPAA includes both the HIPAA Privacy Rule and HIPAA Security Rule. These rules outline National standards for protecting PHI and security standards to protect PHI that is held or transferred electronically. This includes how to keep PHI safe and confidential by taking certain administrative, physical, and technical safeguards.

<table>
<thead>
<tr>
<th>HIPAA</th>
<th>Health Insurance Portability and Accountability Act 1996</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHI</td>
<td>Protected Health Information</td>
</tr>
</tbody>
</table>

What is HIPAA and PHI?
• It is your responsibility to protect the privacy and security of patient’s Protected Health Information (PHI).

• PHI includes:
  – Patient identification
  – Demographic information
  – Medical record information
  – The fact that a patient is in the facility
It’s not worth losing your job!

• Do not access a record if you do not need to for patient care!
• Consequences of inappropriate access include:
  • Termination
  • Legal action
  • Written warning
  • Counseling / Education
• Any impermissible use or disclosure is presumed to be a breach, unless we can prove there is a low probability of compromise to the PHI.
MHS conduct audits of records to look for inappropriate access to files

- **Audits** of medical record access
  - Can **confirm inappropriate access**
  - Are done randomly and regularly.

- “High-profile patient” records are routinely **audited** for inappropriate access
High Profile Patients

• High profile patients include:
  – Famous people
    ▪ Patients who may attract (or whose families or significant others may attract) media and/or community interest
    ▪ Local, national, or international
  – Traumas
    ▪ Patients with extreme or unusual injury or illness, or patients whose injury or illness resulted from an extreme or unusual event
  – Criminals or protected witnesses
High Profile Patients

• If you become aware of a high profile patient
  – **Call the Command Center at ext. 15741** so that a Lead Security Officer can be dispatched immediately to that location
Module 3: Information Safety

Lesson 3.1 HIPAA and Protected Health Information

Topic 3.1.1 HIPAA and Releasing Information to Law Enforcement
Releasing Information to Law Enforcement

• We want to do what is right and helping law enforcement seems right. However, when it comes to PHI, we cannot just ‘answer’ or ‘release’ information. HIPAA and Florida Law have special requirements that must be respected.

• It is your responsibility to follow policy when Law Enforcement asks for patient information.

If Law Enforcement makes a request: be respectful, but do not be intimidated into disclosure!
### Example Situations

If a patient is **not** “in custody” of Law Enforcement, information can only be released in certain situations.

<table>
<thead>
<tr>
<th>Situation</th>
<th>What to do</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the patient or personal representative has signed a valid authorization.</td>
<td>You CAN release information</td>
</tr>
<tr>
<td>If the patient has consented to being listed in Martin Health System (MHS) directory and Law Enforcement requests information on the patient by name, then</td>
<td>Law Enforcement can be told “directory” information (i.e., only patient location and condition in <em>general</em> terms—critical, good, etc.) Law Enforcement cannot be told a time or plan for discharge.</td>
</tr>
<tr>
<td>If the patient poses imminent threat to himself or others and the information is needed to avoid harm to the public.</td>
<td>You CAN release information</td>
</tr>
<tr>
<td>If Law Enforcement requests information on a patient that is a suspected victim of a reportable offense under Florida Law, including child or vulnerable adult abuse.</td>
<td>Check with Risk Management, Legal, or Compliance on situations</td>
</tr>
<tr>
<td>If a Law Enforcement request involves possible criminal conduct occurring at MHS.</td>
<td>Check with Risk Management, Legal, or Compliance on situations</td>
</tr>
<tr>
<td>If a patient is a suspected victim in a crime</td>
<td>Information can be released if the patient signs a valid authorization</td>
</tr>
</tbody>
</table>
Module 3:
Information Safety

Lesson 3.2

Privacy Incidents
Privacy Incidents and PHI

• Privacy incidents include patient information
• Do not access or send a record if you do not need to for your job!
• Consequences of inappropriate access or use of PHI:
  • Termination
  • Legal action
  • Written warning
  • Counseling / education
Your Responsibilities

• You are accountable for the privacy and security of patient information
• Associates are required to follow HIPAA
• Associates are required to understand and follow MHS’s:
  – HIPAA Privacy and Security Policies
  – Network Access Agreement

For additional information:
On Hospital Portal
→ MHS HIPAA Privacy and Security Policies
On MartinLink
→ MHS Computer Network Access Agreement
### PHI and Personal Identifiers

**You must keep this information private because it can identify patients!**

- **Contact Information**
  - Names
  - Street address, city, county, precinct, zip code
  - E-mail addresses
  - Telephone numbers
  - Fax numbers

- **Other personal information**
  - Social Security number
  - Medical record numbers
  - Account numbers
  - Certificate/license numbers
  - Biometric identifiers, including finger and voice prints
  - Health plan beneficiary numbers
  - Full-face photographic images and any comparable images

- **All elements of dates (except year)**
  - Birth date
  - Admission date
  - Discharge date
  - Date of death
  - Ages over 89

- **Electronic Device and Internet Information**
  - Device identifiers and serial numbers
  - Website addresses (URLs)
  - Internet Protocol (IP) addresses

- **Vehicle information**
  - Serial numbers
  - License plate number
  - Other vehicle identifier

- **Any other unique identifying number, characteristic or code**
Be aware of your surroundings when discussing patients and sharing PHI. Think about:

– Who is around you?
– What you are sharing?
– Where are you?
– When are you sharing?

If you obtain a patient’s verbal authorization to disclose PHI, be sure to document the authorization in the patient’s electronic medical record (EPIC).

Review information prior to release to be sure you are giving it to the correct patient or authorized person.
De-identified Information

• Information is de-identified if:
  – All of the identifiers (listed on the PHI and Personal Identifiers slide) of the individual or of relatives, employers, or household members of the individual are removed.

  **AND**

  – The covered entity* does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

*Covered entities are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.
Module 3: Information Safety

Lesson 3.2 Privacy Incidents

Topic 3.2.1 How to Prevent: Misdirected or Lost Documents
• Slow down and verify recipients and content.

• Before you share information, verify:
  – Identities
  – Phone number(s)
  – Fax number(s)
  – E-mail recipient(s)
  – Correct attachment(s)
Proper Management of Documents

• Don’t leave printers or faxes unattended when confidential corporate or patient data is printing.
• Secure interoffice mail
• Dispose / shred in accordance with policies
How to Prevent: Paperwork Handoff Errors

Lesson 3.2 Privacy Incidents

Module 3: Information Safety
How to Prevent: Paperwork Handoff Errors

• Check ALL papers before handing to a patient

• Use TWO patient identifiers to confirm you are handing to the correct patient
  – Name
  – Date of Birth
  – Use the 2 step method
    1. Ask patient to confirm the 2 identifiers
    2. Check their arm band
Module 3: Information Safety

Lesson 3.2 Privacy Incidents

Topic 3.2.3

How to Prevent: Inappropriate Access
No! Do Not Access

Do **NOT** access records (electronic or paper) not needed to do your job.

Records that you should NOT access include:

– Records of patient not in your care
– Records of a friend, family, or fellow associate (even if they ask)
– Your own medical record
  - Instead use: My Chart or request your records through Health Information Management Team (HIM)

I’d like to help. But you really need to call HIM. They’ll get your information.
It is **OKAY** to access information that you need to do your job, such as for

– Patient treatment

– Patient scheduling

– Coding a patient chart

– Admitting a patient

– Obtaining authorization for treatment
A patient’s medical record includes:
• Treatment information
• Demographic information
• Scheduling and appointments

Accessing any portion of a patient’s information, unless needed for work, is inappropriate.
“Break the Glass”

• This is a Special Privacy Setting in EPIC that Triggers an Audit Trail. (EPIC is our Clinical Information System, certain job roles have access)

• If you have a **“need to know” to do your job**, follow the instructions to “break the glass” and **proceed**. You are asked to give your reason for needing to be in the record and identify your entry once in a 24-hour period.

• If you **do not need** to be in the record, **do not enter** it. The automatic audit helps keep our patients’ information private, and also protects us from momentary lapses in judgment and accidental intrusion into sensitive matters.
Unauthorized Access

- If you do not need the information to do your job...then do NOT access it!
- Notify your leader if you have access to more information than you need on your computer.
Remember:

– You are held accountable for unauthorized access of information. This is outlined through procedures within:
  - HIPAA (Law)
  - MHS Policy
  - MHS Access Agreement

– We run audits routinely to identify unauthorized access, taking our corporate responsibility to protect patient information.
Topic 3.2.4

How To Prevent: Oral Disclosures of PHI
• **Be aware of surroundings** when discussing patients and sharing PHI. Think about
  – Who is around you?
  – What you are sharing?
  – Where are you?
  – When are you sharing?

• Verify identities and phone numbers prior to disclosures
Module 3: Information Safety

Lesson 3.2 Privacy Incidents

Topic 3.2.5

How To Prevent: Social Media Violations
• Remember...the world sees what you post
  – Represent MHS as a professional
  – Protect patient and MHS information and privacy
• PHI and personal identifiers can come out easily in an innocent post.
• Think before you tweet or post!
<table>
<thead>
<tr>
<th>Jamie Jones</th>
<th>June 15, 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Works at: Martin Health System</td>
<td>“We were outstanding today!”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sam Miller</th>
<th>June 15, 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Works at: Martin Health System</td>
<td>“I don’t know how you all did it!”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Jamie Jones</th>
<th>June 15, 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Works at: Martin Health System</td>
<td>“It was like an episode of Grey’s Anatomy.”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sam Miller</th>
<th>June 15, 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Works at: Martin Health System</td>
<td>“Without the Dr. McDreamy...”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Jamie Jones</th>
<th>June 15, 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Works at: Martin Health System</td>
<td>“But we had Dr. Yang to crack the guy’s chest!”</td>
</tr>
</tbody>
</table>
• From this chat, you can tell that
  – This happened at Martin Health System
  – On June 15, 2016
• If there was a patient who got his chest “cracked,” this conversation went too far! This conversation has identifiable health information!
And it could easily be worse. Suppose someone else commented and
  – Added a piece of PHI?
  – Referred to a news story with information?
If this happened, you would be faced with consequences for being a part of a privacy breach.

Play it safe. Do not risk it.
Do you want to be the associate who needs to worry and explain? Compliance does not want that either.
Consequences of Posting

• You could:
  – Be terminated
  – Be fined
  – Face legal consequences

For additional information:
On Hospital Portal
→ Administrative Policy: Social Media Guidelines
### Consequences of Posting: Examples

<table>
<thead>
<tr>
<th>Situation</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Several Employees here at MHS took pictures of a shark attack victim.</td>
<td>Employees involved received written warnings, demotions, and/or suspensions.</td>
</tr>
<tr>
<td>A Rhode Island ER doctor posted information online about a trauma patient. The doctor did not include the patient’s name, but she wrote enough that others in the community could identify the patient. (<em>Boston Globe</em>, April 2011)</td>
<td>The doctor was fired, fined $500, and reprimanded by the Rhode Island Medical Board.</td>
</tr>
<tr>
<td>At a medical center in Oceanside, hospital managers discovered that five nurses had been discussing patients on Facebook.</td>
<td>The five nurses were fired.</td>
</tr>
<tr>
<td>The Phoenix Cardiac Surgery of Arizona was posting clinical and surgical appointments for its patients on an internet-based calendar that was publicly accessible. (<em>HHS</em>, April 2012)</td>
<td>The practice agreed to pay the U.S. Department of Health and Human Services a $100,000 settlement and take corrective action to implement policies and procedures to safeguard PHI of its patients.</td>
</tr>
</tbody>
</table>
Module 3: Information Safety

Lesson 3.2 Privacy Incidents

Topic 3.2.6

How to Protect: Information Security
Follow the MHS Computer Network Access Agreement and MHS HIPAA Privacy and Security Policies.

For additional guidance, contact Information Security (ext. 14811) or Corporate Compliance (ext. 11983). If unavailable, you can also contact Command Center (ext. 15741).
Ways to Protect Information Security

• Make an effort to obscure PHI from public view on monitors and papers at your station.
• Lock your computer or log off if you need to walk away
• Do not add, delete or change software without IT approval
• Do not send PHI via email. It is like a postcard...anyone could turn it over and read it along the way.
• If you need to send PHI via email, enter [secure] anywhere in the subject line. This encrypts the message through a process set up by our IT department.
• Verify identities, fax, and phone numbers prior to disclosures
Phishing Messages

How To Spot A PHISH

What is Phishing? A technique used to fraudulently obtain usernames, passwords, credit card numbers, and other sensitive information.

Fraudulent emails typically ask you to:
- Open an attachment or,
- Click on a link, redirecting you to a malicious website.
- You may be prompted to enter personal information.

Types of Phishing Attacks

- Spear Phishing: A highly targeted form of phishing that hones in on a specific group of individuals or organization.
- Whaling: A form of phishing, targeted at executive level individuals.
- Cloning: Whereby a legitimate email is duplicated but, the content is replaced with malicious links or attachments.

Anatomy of a Phishing Email

- Contains links or attachments
- Poor grammar and spelling
- Requests personal or sensitive information
- High sense of urgency and/or privacy
- Discusses confidential subjects like salaries
- Incentivizes through threat or reward

Keep it Safe and Secure
Martin Health System has partnered with KnowBe4 to assist our organization in building “Human Firewalls”.

A human firewall is created when individuals within an organization are educated about how to interrogate their emails: when to click on a link or open an attachment, and when to delete it.

Please click on the link below to learn about Social Engineering. Be sure to click “Next” on the landing page.

Social Engineering Education
Password Tips

• Make it difficult to guess
• Include
  – Letters
  – Numbers
  – Special characters
• Never include personal info. (ex: birthday)
• Never give your password to anyone
• Never use anyone else’s password
• Never store passwords where they can be found

• If you suspect your password has been breached, contact the Help Desk (ext. 14357) to change it

• If your password was used maliciously, report the breach to your leader
• Patient Information
  – Never take reports or computer media that contain patient information outside of your workplace.

• Other Confidential Information
  – Taking or accessing associate and organizational information outside of the workplace increases the risk of a security breach.
  – Protect paper documents, USB drives, and laptops.
    ▪ If information is taken outside of the workplace, make sure to secure the information in a locked area.
    ▪ Leaving items in a car increases risk because it can easily be broken into.
  – Protect information accessed electronically.
    ▪ If you access information electronically, make sure to use a proper device with security protection.
You have now reached the end of this module!

- You can now review any content in this module by using the back button or the Table of Contents on the left side of the screen.
- This module will be marked as ‘Completed Unsuccessfully’ until you have viewed each slide. You will not be able to proceed to the quiz until it is marked ‘Completed Successfully’.

Once you finish reviewing this module, you can return to iLearn to take the Module 3 Quiz.

- Click the ‘X’ at the top right corner of the screen to exit the module and confirm that you have reviewed all content and reference material. Then click ‘Exit and Finish’.
- The next activity that you will complete in iLearn will be the Module 3 Quiz. You can then start the quiz by clicking ‘launch’ in the list of activities.