OBJECTIVES

At the completion of this course, the learner will be able to:

- Define the Purpose of HIPAA
- Define Business Associate
- Identify Patients’ Rights
- Understand the Consequences of HIPAA violations
ABBREVIATIONS

HIPAA – Health Insurance Portability and Accountability Act
PHI – Protected Health Information
TPO – Treatment, Payment and Operations
CE – Covered Entities
BA – Business Associate
BAA – Business Associate Agreement
EHR – Electronic Health Record
HITECH - Health Information Technology for Economic and Clinical Health Act
ARRA - American Recovery and Reinvestment Act
THE PURPOSE OF HIPAA IS TO...

- Protect and enhance rights of consumers by providing access and controlling inappropriate use of their health information.
- Improve the quality of health care in the U.S. and restore trust in the health care system.
- Improve healthcare delivery through national health privacy protection initiatives.
PROTECTED HEALTH INFORMATION (PHI)

- PHI is any Health Information whether written, verbal, or electronic which is created or received by the covered entity and relates to a person’s past, present or future physical or mental health condition, to the provision of health care to the person, or to the past, present or future payment for that person’s health care.
DEFINE BUSINESS ASSOCIATES “BA”

- A person or entity that provides certain functions, activities, or services for or to the Hospital involving the use and/or disclosure of PHI is a Business Associate.

- All identified BA are bound by the same regulations as the CE and should have a written BAA with the CE.
  - Ex: Transcription company, Software vendor providing remote support to system with PHI
PATIENT’S RIGHTS ESTABLISHED BY HIPAA

- Notice of Privacy Practices
- Minimum Necessary
- Opting of our Facility Directory
- Restriction Requests
- Confidential Communications
- Right to Access and Amend PHI
- Accounting of Disclosures
Patients have a right to receive notice of how covered entities plan to use and disclose PHI.

Notice must be written in plain language and contain the following:

- Description of uses and disclosures expected to be made without individual authorization
- Statement that other uses and disclosures would be made only with authorization and authorization may be revoked
MINIMUM NECESSARY

- Access to and use or disclosure of “PHI” must be restricted based on specific job responsibilities and roles.
- If you access or use PHI for anything other than job duties you have violated HIPAA. (Even if the PHI is not disclosed to anyone)
MINIMUM NECESSARY

- Computer passwords are assigned according to the scope and responsibilities of an employee’s position.
- Access to “PHI” whether electronic, verbal or paper should be limited to the amount necessary to perform your job.
OPTING OUT

- Patients have a right to be informed of information contained in the facility directory and its use.
- Patient must be given opportunity to opt-out or limit information that can be released from the directory.
- If a patient is identified by name, the following information can be released if they do not opt-out.
  - general condition (fair, critical, stable) and location in the facility.
OPTING OUT

- Clergy may receive information without asking for individuals by name including:
  - Name
  - General Condition
  - Location
  - Religious Affiliation

- Information regarding patient’s who opt out of the directory may not be released to anyone, including clergy.
RESTRICTION REQUEST

- Patients have the right to request restrictions regarding their PHI.
- We are not required to agree to all restrictions.
- You must adhere to restrictions to which you have agreed except in emergency treatment situations.
A CE must comply with the requested restriction if:

- the disclosure is to a health plan for purpose of carrying out payment or health care operations (and is not for purposes of carrying out treatment); and
- The PHI pertains solely to a health care item or service for which the health care provided has been paid out of pocket in full.
CONFIDENTIAL COMMUNICATIONS

- Covered entities are required to permit individuals to request confidential communications of PHI.
- Covered health care providers must comply with all reasonable requests.
- Individual may request communications by alternate means or at alternate locations.
- Any request for confidential communications must be submitted in writing to the Privacy Officer.
RIGHT TO ACCESS AND AMEND PHI

- Individuals have a right to have covered entities amend PHI about themselves for as long as the covered entity maintains the information.
- Requests should be in writing and directed to the Privacy Officer, Kathy Alberson.
HOW DO I HANDLE... 

...An individual asking for access to their record?

- Individuals have a right to access their PHI and can do so electronically if the facility has an electronic health record.
- Route requests to Health Information Management.
ACCOUNTING OF DISCLOSURES

- Patients have a right to request from a covered entity an accounting of disclosures of PHI other than for TPO. The accounting can include up to 6 years of disclosures.
OTHER POLICIES BROUGHT ABOUT BY HIPAA

PRIVACY

- Faxing of PHI should be restricted to limited situations.
  - Fax machines receiving PHI must be in secure locations
  - All faxes containing PHI should be accompanied by a cover sheet.
- Be aware that misdirected faxes can result in a Breach that must be reported.
REPORTING INAPPROPRIATE USES AND DISCLOSURES OF PHI

- Mitigating Harmful Effects
  - CE are required to address improper uses or disclosures whether intentional or unintentional.
  - All members of the workforce are expected to report any inappropriate use or disclosure of PHI to your supervisor, any manager, the Privacy Officer or by utilizing the compliance hotline.
WHAT HAPPENS IF A PRIVACY POLICY IS VIOLATED?

- Employee sanctions
- Patients have a right to file a complaint with CE and/or the DHHS.
- Civil and criminal penalties
PENALTIES

- The person did not know
  - At least $100 for each violation not to exceed $25,000
- Due to reasonable cause and not willful neglect
  - At least $1000 for each violation not to exceed $100,000 each
- Willful neglect
  - Violation is corrected - $10,000 required for each violation not to exceed $250,000
  - Violation not corrected - $50,000 required not to exceed $1,500,000
HIPAA Security

What Does This Mean For You?
OBJECTIVES

After completing this course, the learner will be able to:

- Identify Security Measures that we take to ensure privacy for our patients.
- Identify Sanctions for HIPAA violations.
- Understand how to identify a security breech.
- Identify PHI Access
- Summarize Policy and Procedures at TRMC
SCREEN SAVERS, LOG-OFFS & ENCRYPTION

- **Screen Savers**: MIS sets desktop screen savers to activate after 5 minutes of inactivity. This protects PHI from being exposed on screens.

- **Auto-Log Off**: Critical information systems log users out after a period of inactivity.

- **Encryption**: All outgoing email is automatically scanned for PHI and encrypted if necessary. When a user is attaching files such as a Word or PDF document, it is important that they add “zyxencrypt” (one word) in the subject line of the email. This insures the email is encrypted.
SCREEN SAVERS, LOG-OFFS & ENCRYPTION

- **Unique User Accounts:** All users of information systems at TRMC have a unique username and password assigned to them. These are not to be shared with any other employee at any time.

- **Audits:** All critical information systems at TRMC maintain audit trails of the activities of each user in the system.
HIPAA SAFEGUARDS AND CONTROLS

- Technical Safeguards include integrity controls such as virus protection systems.
- Physical Safeguards are all about the protection of the computer systems. Access to our data center falls under this safeguard.
- Facility Access Controls include passwords and automatic log offs that identify and protect individual system users.
HIPAA SANCTIONS

- Sanctions For HIPAA Violations: TRMC will apply appropriate sanctions against members of its workforce who fail to comply with the Hospital’s HIPAA policies.
- There have been terminations at TRMC for HIPAA violations. It is serious business!
HIPAA INCIDENT REPORTING

- Workforce members shall report all suspected security incidents, including all threats, or violations that affect or may affect the confidentiality, integrity, or availability of electronic systems containing PHI.

- System owners must work with the HIPAA Security Officer and IT to develop recommendations and implement countermeasures to prevent the breach from occurring again.
HIPAA INCIDENT REPORTING

- Guy McAllister, as HIPAA Security Officer and Kathy Alberson, as HIPAA Privacy Officer must notify each other of security or privacy issues if they determine that an incident or issue could affect the other office.
HIPAA SECURITY POLICIES & PROCEDURES

- The HIPAA Security Policies may be found in the Administrative Policy Manual and online at MedNet.
HIPAA SECURITY BREACH

- Breach - A use or disclosure of PHI that compromises the security or privacy of information in a way that poses a significant risk of financial, reputational, or other harm to the individual.

  - Example

    - The loss of a lap top that contains information including SSN that could be used to steal someone’s identity.

    - Patient’s HIV results faxed to a residential fax machine rather than to the ordering provider.
HIPAA SECURITY BREACH

When a breach occurs there are multiple steps that must be taken to mitigate damage including:

- Notifying the individual(s) whose information was compromised
- Notifying the media when more than 500 individuals are involved
- Notifying the federal government through the Secretary of the Department of Health and Human Services (DHHS)

Breach notifications are posted on the DHHS web site.
**PHI ACCESS**

- PHI refers to a patient’s protected health information.
  - Federal regulations are specific as to what can and cannot be done with PHI. HIPAA Privacy and Security regulations are dedicated to protecting one’s personal health records.
PHI ACCESS

- You may not transmit any PHI outside of the hospital, unless authorized to do so.

- This includes email, FTP services and disk transfer. Any email within “tiftregional.com” is appropriate since each of those email remain inside TRMC’s firewall; however, sending PHI to another email domain is not appropriate.

- If you are ever unsure as to where PHI may be sent, please contact the HIPAA Security Officer at ext. 3320 or HIPAA Privacy Officer at ext. 7553.
WHO TO CONTACT WITH CONCERNS

Compliance Information Management Subcommittee
Kathy Alberson, HIM Director/Privacy Officer
Guy McAllister, Asst. VP & CIO/Security Officer
Josh Sumner, Information Technology Director
Karen Summerlin, Legal Counsel
Dennis Crum, VP & CFO
Laverne Cook, Asst. VP Patient Care
Mindy McStott, Director Quality Management
Karen Kimsey, Director Education
WHO TO CONTACT WITH CONCERNS

- Any Manager
- hipaahotline@tiftregional.com
- Compliance helpline - 353-6250
INTRANET SERVICES

- Along with Portal, Tift Regional also offers an employee site; MedNet (http://mednet), which is the home page on all hospital PCs.
- MedNet provides web-based hospital-wide information to all employees through any PC in the hospital using Internet Explorer.
- News and events will be published and updated on MedNet.
- Many departments have active, updated pages on MedNet.
INTRANET SERVICES

- MedNet will maintain electronic versions of all policy and procedure manuals as well as the employee handbook and all other compliance information.
- MedNet is provided to improve hospital-wide communication.
POLICY SUMMARY

- Tift Regional provides electronic mail, voice mail and Internet access to promote and support its mission; such communications systems are the property of TRMC and are to be primarily used for business purposes.

- Highly limited reasonable personal use of the systems is permitted; however, you should assume that these communications are not private.

- All TRMC employees having e-mail are responsible for any communication sent to them via e-mail.
POLICY SUMMARY

- Employees and others with access to these services must use them responsibly and consistent with their job duties and Tift Regional’s mission.
- Employees may not use internal communication channels or access to the Internet at work to post, store, transmit, download, or distribute any propriety data, trade secrets, or other confidential information.
- TRMC’s communication systems cannot be utilized to engage in any type of unethical, illegal, or in any conduct which violates TRMC’s Code of Ethics or Corporate Compliance Program.
POLICY SUMMARY

- TRMC reserves the right to review, audit, intercept, access and disclose all messages. The contents of electronic mail, properly obtained for legitimate business purposes, may be disclosed within TRMC without the permission of the employee.

- TRMC reserves the right to discipline any user for inappropriate use of the e-mail system.

- Phone/Voice Mail, Email, MedNet and paper memos are recognized means of communication within TRMC.
POLICY SUMMARY

- Adhere to Tift Regional’s policies.
  - Use only services you have authorization to access.
  - Always represent yourself as yourself, never as someone else.
  - Ensure that any software placed on your PC or LAN (Local Area Network) complies with applicable licensing agreements and copyrights.
  - Always comply with applicable licensing agreements and copyrights when downloading software from the Internet and/or placing it on the LAN.