HIPAA Compliance for Students
The Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996 by the United States Congress.

It’s intent was to help people obtain health insurance benefits when they changed jobs.
It includes guidelines for healthcare agencies to manage information easier; protect a patient’s privacy and protect the security of a patient’s health information.

The first phase of HIPAA addressed privacy. Hospitals were required to be in compliance by April 2003.

The second phase of HIPAA addressed Security. Compliance was required by April 2005.
HIPAA regulations refer to healthcare agencies as “Covered Entities”.

Covered Entities include health plans, healthcare clearinghouses and healthcare providers who transmit any health information in electronic form when conducting business.

HIPAA also defines Third Party payers as an insurance company (including Medicare and Medicaid) that is primarily responsible for payment of services a patient receives from a “Covered Entity”.

In order for Tift Regional Health System (TRHS) to conduct business and receive payment for the services we render, the organization (meaning all employees, students and faculty) must adhere to the guidelines. If we don’t, both our organization and individuals can pay the penalty for non-compliance.

What are the possible Penalties?
According to modifications in the Social Security Act Penalties, there is a tiered set of penalties as established:

1. Where there is a violation and it is established that the person did not know (and by exercising reasonable diligence would not have known) that such a person violated a provision, a penalty for each violation will be at least $100 for each violation, not to exceed $25,000.

2. Where there is a violation and it is established that the violation was due to reasonable cause and not to willful neglect, a penalty for each such violation will be at least $1,000 for each violation, not to exceed $100,000 for each violation.
3. Where there is a violation where it is established that the violation was due to willful neglect:
   • If the violation is corrected, a penalty in the amount of $10,000 will be required for each violation not to exceed $250,000.
   • If the violation is not corrected as described, a penalty in the amount of $50,000 will be required not to exceed $1,500,000.
This CBL will review the basic guidelines associated with HIPAA regulations and assist all parties to continue to meet compliance requirements. At the conclusion of this program, the participant will be able to:

1. Recognize terminology used in HIPAA legislation.
2. Define “Protected Health Information”.
3. Understand the principle of Minimum Necessary”
Objectives

4. Discuss ways of handling situations that could result in a HIPAA breach.
5. Identify HIPAA Security requirements.
6. Recognize potential breaches in security.
7. List who to report HIPAA violations to.
8. Locate additional information and TRHS organizational HIPAA policies.
Like many other laws and regulations, there is a lot more beneath the surface than what we initially see and think.

Let’s review some very basic guidelines:
What is PHI?

- PHI is the abbreviation for the term “Protected Health Information”.
- PHI is any health information that would let someone know about an individual’s health status.
Protected Health Information (PHI)

• Anything that can connect personal information to a person
• It can be in oral, written or electronic form
• May include
  • Name
  • Social Security number or medical record numbers
  • Date of birth
  • Room number
• All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census.
PHI

• Also includes:
  • Billing information
  • Telephone numbers;
  • Fax numbers;
  • Electronic mail addresses;
  • Social security numbers;
  • Medical record numbers;
  • Health plan beneficiary numbers;
• Account numbers;
• Certificate/license numbers;
• Vehicle identifiers and serial numbers, including license plate numbers;
• Device identifiers and serial numbers;
• Web Universal Resource Locators (URLs);
PHI

- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code
Release of one piece of a patient’s information, can be a breach in compliance and open the hospital and you to legal and monetary fines and penalties.

One of the most common ways a breach occurs is for an employee or student to inadvertently say or ask something about a patient in the presence of someone else who should not have access to the information.
Students must be careful about who, what and where they are talking. Just asking a visitor you know why they are in our facility can result in the release of information about a patient.

BE CAREFUL
How Do I Know...

...When information is considered private?
Ask yourself the question:

- Did you learn it through your clinical experience at one of Tift Regional’s campuses?

If yes, then it is considered private
How much am I allowed to tell someone about a patient?

- Follow the Rule/TRHS Policy of Minimum Necessary
  - Access to and use or disclosure of “PHI” must be restricted based on specific job responsibilities and roles. Ask yourself the question: Does this person NEED to know the information to protect the safety and health of the patient?
TRHS’s Minimum Necessary policy also includes Security safeguards such as:

- Computer passwords are assigned according to the scope and responsibilities of a student’s clinical assignment.
- **NEVER** share your computer password or your student number with anyone.
How Do I Handle...

...Another member of the workforce inquiring into a patient’s condition or treatment? ASK YOURSELF:

- Is it necessary to their job function?
- Is it related to treatment?
- If neither are true, the information should not be shared.
Patients have a right to be informed of information contained in the facility directory and its use.

Patients must be given opportunity to opt-out or limit information that can be released from the directory. TRHS’s main campus opt out symbol for the STAR system is the @ sign. TRHS’s main campus opt out symbol in Horizon Expert Documentation is the privacy button on the title bar.

If a person identifies a patient by name, the following information may be provided if the patient has not chosen to opt out.

- general condition (fair, critical, stable)
- location in the facility
Clergy may receive information without asking for an individual by name including:

- Individuals Name
- General Condition
- Location
- Religious Affiliation

Information regarding patient’s who opt out of the directory may not be released to anyone, including clergy.
A family member or close friend asking about a patient?

You should only release PHI when it is related to your job responsibilities regardless of who is seeking the information. For example: If you are a student nurse on the unit and are approached by someone inquiring about a patient, only basic directory information can be provided without the patient’s permission. PHI should never be disclosed without verifying the patient’s opt out status in the directory.
Restrictions for Use and Disclosure

- Patients have the right to request restrictions regarding their PHI.
- TRHS is Not required to agree to the restrictions.
- Hospital staff must adhere to restrictions to which you have agreed except in emergency treatment situations.
Restrictions on open records for patients still in our facility must be requested in writing and communicated to the nursing supervisor.

Restrictions on closed records must be submitted in writing and forwarded to the Privacy Officer.
Covered entities are required to permit individuals to request confidential communications of PHI.

Covered health care providers must comply with all reasonable requests.

Individuals may request communications by alternate means or at alternate locations.

Any request for confidential communications must be submitted in writing to the Privacy Officer.
This means the student should refer an individual to Health Information Management department if the individual desires:

- Copies of their medical record or portions of the record for personal use.
- Copies of their medical record or portions of the record sent to another provider.
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.

- How Do I Handle… An individual asking for access to amend their record?
  - *All requests must be submitted to the Privacy Officer in writing using the amendment request form.*
How Do I Handle…

…An individual asking for access to their record?

- Individuals have a right to access their PHI
- Route requests to Health Information Management’s Release of Information Department or to the Nursing Supervisor if the patient is not discharged.
Several Policies are in place at TRHS to assure compliance with HIPAA guidelines related to Release of Information including:

- Release of Information policy
- Access to and Use and Disclosure of PHI of Incompetent Adult
- Release of PHI to Law Enforcement
- Right of Access to and Input Regarding Use and Disclosure of PHI of Deceased Individual
- Right of Access to PHI of Minors
- The organization’s MedNet page provides access to the HIPAA Compliance Manual and policies associated to confidentiality of patient records. Faculty and students who are given access to the electronic patient record may access these resources electronically. Students and faculty who do not have electronic access should talk with the department manager if they desire to review the policies.
Accounting of Disclosures

- Patients have a right to request from a covered entity an accounting of disclosures of PHI. The accounting can include up to 6 years of disclosures. Any request should be forwarded to the Health Information Management Department.
Notice of Privacy Practices

- Patients have a right to receive notice of how covered entities plan to use and disclose their PHI.
- Who do I call if a patient has a question about TRHS’s Privacy Notice? Forward questions to the Privacy Officer.
Faxing of PHI must be restricted to limited situations and must be handled as defined by policy.

- Fax machines receiving PHI will be in secure locations.
- All faxes containing PHI will be accompanied by a cover sheet.
Mitigating Harmful Effects

• TRHS is 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 their supervisor, any manager or by utilizing the compliance hotline.
• Students and faculty are expected to report any inappropriate use or disclosure of PHI in the same manner or directly to the Privacy Officer.
Who should you contact with concerns?

- Compliance Information Management Subcommittee
  - Kathy Alberson
  - Guy McAllister
  - Karen Summerlin
  - Dennis Crum
  - Laverne Cook
  - Mindy McStott
Who should you contact with concerns?

Any Manager

- hipaahotline@tiftregional.com
- Compliance helpline  229–353–6250
What happens if a privacy policy is violated?

- Employees/Students are sanctioned according to TRHS policy “Sanctions for HIPAA Violations”
- Patients have a right to file a complaint with TRHS and/or the DHHS.
- Civil and criminal penalties can result.
- Students may be denied further access to the clinical facility and could be subject to civil and criminal penalties.
What about the Security part of HIPAA?

The HIPAA Security Rule addresses electronic PHI (ePHI) in three distinct areas:

- Confidentiality
  - ePHI is accessible only by authorized people and processes.
HIPAA Security

- **Integrity**
  - ePHI is not altered or destroyed in an unauthorized manner.

- **Availability**
  - ePHI can be accessed as needed by an authorized person.
The HIPAA Security regulations are very complex and include standards and specifications regarding:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
It means that we have to be as diligent about our computer use and other electronic information as we are about our conversational information.
Faxing of PHI from TRHS is restricted to limited situations and is handled as defined by policy.

- Fax machines receiving PHI must be in secure locations.
- All faxes containing PHI must be accompanied by a cover sheet.
Screen Savers: MIS sets desktop screen savers to activate after 5 minutes of inactivity. This protects PHI from being exposed on screens. This does not prevent the information from being accessed, it simply prevents it from being easily read by others standing around the desktop.
Log Off: Critical information systems log users out after a period of inactivity. If a user leaves the desktop, it is imperative that the user log off, otherwise, another individual could access information under the users password. Students & Faculty– Protect yourself by always logging off when leaving a work terminal.
Encryption: All outgoing email from TRHS is automatically scanned for PHI and encrypted as necessary. The employee does not have to worry about how to encrypt information. TRHS’s MIS department personnel assure that this is completed.
Unique User Accounts: All users of information systems at TRHS have a unique username and password assigned to them. These are not to be shared with any other one at any time. Use of the system is monitored by username so if you do not log off when leaving your desktop, there is no way for MIS to determine that you are not the person using the system. Students must keep their MIS passwords and password information secure. Failing to report the loss of your MIS password information could constitute a breach in HIPAA. Report losses immediately to your instructor, TRHS preceptor or the Student Liaison Coordinator (ext. 7793) as soon as you realized the information is missing.
Audits: All critical information systems at TRHS maintain audit trails of the activities of each user in the system. Remember— if someone is in the system under your access, it tracks to you not to the person actually using the system. PROTECT yourself by logging off, never giving your password out and using the system only for clinical related activities.
Suspicion of a Security Breach

- Workforce members, students and faculty should 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.
A student or faculty member can learn more about the HIPAA guidelines and Tift Regional policies by reviewing the HIPAA Compliance Manual.

The HIPAA Compliance Manual can be reviewed by request to the Education Department of the organization. All policies and procedures can be found within the manual. The manual is also available on the hospital’s MedNet under Policies & Manuals.
Things to Remember . . .

1. Data security is serious business at TRHS.
2. HIPAA Security affects only electronic PHI.
3. Never share your username or password.
4. When you are finished at a PC, log out of that system.
5. Be aware of your physical environment when you are viewing PHI on a PC screen.
6. PHI is any information, including demographic information that can be used to identify the patient.

7. Guy McAllister is the HIPAA Security Officer for the organization.

8. Kathy Alberson is the HIPAA Privacy Officer for the organization.
Conclusion

- HIPAA Privacy and HIPAA Security are both a part of the federal HIPAA legislation. While they address different components, together they make up the guidelines for protecting health information.
Conclusion

- For TRHS staff and students and faculty, meeting HIPAA compliance guidelines is a never ending huge process that requires daily diligence. Keeping up your end of the process makes us as a team able to assure our patients’ confidentiality and safety.