HIPAA and EMTALA Legislation

What You Need To Know
Objectives

- Recognize the importance of maintaining patient privacy and confidentiality
- List 5 patient rights under HIPAA privacy law
- Relate the impact of the lack of patient privacy to our business and to customer service
- Define PHI and ePHI
- State ways to secure PHI and ePHI in your work area
- Describe how to create an effective password
- List 5 things that you can do to protect the security of your work area
- Know the location of the HIPAA policies within the organization
- State how to report a Compliance concern
Confidentiality continues to be a concern for all of us especially with the implementation of the Health Insurance Portability and Accountability Act (HIPAA) which was effective on April 14, 2003.
Compliance is not voluntary, it’s mandatory. As an Associate, Volunteer, or member of our workforce, even if you work at home, you must be aware of your role in protecting the privacy and security of our patients.

Every individual makes a difference in applying these privacy and security requirements to health information, and it takes the entire organization working together to address and maintain the privacy and security of patient information.
Remember, patient protected health information (PHI) is any identifiable information (medical record number, age, zip code, social security number, address, etc.,) combined with health information such that the identity of the person would be known. ePHI is any patient protected information in electronic form which includes computer, personal devices, and fax transmissions.

Let's review some of the regulations in more detail ........
HIPAA Humor?

First, a little humor; OK, now on to the serious information...

Nurstoons

I'm sorry, according to HIPAA guidelines I can't give you any information without identification.

Later that day...

Well, these pieces of I.D. convince me of who you are, but not that you're married to the patient.

Later that day...

Okay, your marriage license proves it... your husband was discharged this morning, but got tired of waiting for a ride, so he took a cab home.
Who Must Comply?

The following must comply with HIPAA law; anyone who touches patient PHI or ePHI

- **Health Care Providers** - physician, hospitals, pharmacists, nursing homes, outpatient physical therapy, home health agencies, essentially in a hospital anyone who uses or may see protected health information

- **Health Plan** – HMO’s, Medicare/Medicaid, Insurance Companies, Employee benefit plans

- **Clearinghouses** – billing services, third party administrators (companies that standardize information into the required format for claims processing)

- **Business Associates** – Auditors, accountants, lawyers, consultants, billing firms
Key to becoming knowledgeable about HIPAA legislation is understanding patient rights.
HIPAA provides the following rights to the patient:

- **Right to Inspect and Copy** their medical information
- **Right to Amend** their PHI
- **Right to an Accounting** of disclosures of their PHI
- **Right to Request Restrictions** or limitations on their PHI disclosures
- **Right to Request Confidential Communications**
- **Right to a Paper Copy of the Privacy Notice**
- **Right to File a Complaint**
Exceptions to a patient’s right to access include: behavioral health notes, laboratory results, and information being compiled for legal action. The request is to be made through the PI department.

- We can deny access to the medical record if it would endanger the life or safety of the patient or another.

- Patients can request that the denial be reviewed by a health care professional not involved in their care. Carroll Hospital Center will comply with the outcome of the review.
Right to Amend

Patients can amend what they feel to be incorrect or incomplete information in their records. However, we can deny this request under the following conditions:

- The request is not in writing to the PI department with a reason to support the request.
- The information was not created by the hospital.
- The information is not part of the medical information kept by the hospital.
- The information is not part of the information which the patient would be permitted to inspect and copy.
- The hospital feels the information that is in the medical record is correct.

The denial must be provided to the patient in writing.
Patients have a right to an accounting of how their health information has been used for reasons other than for routine treatment, payment, and health care operations. The patient may request an accounting every 12 months, free of charge.

Let's look at this example: We routinely disclose medical records to the Maryland Health Department to report a sexually transmitted disease as required by law. Because the reporting is mandatory by law, we did not have to get the patient’s written authorization or make them aware of the disclosure at the time of the reporting. We do however, have to keep a record of these disclosures should the patient request an accounting.
There are several types of disclosures we make on behalf of the patient.

**DISCLOSURES that:**
- are required
- are permitted without the patient’s endorsement or written authorization
- require patient endorsement
- require written patient authorization
Disclosures That are Required

- We must provide the patient access to their protected health information, when requested by the patient
- To the Secretary of Health and Human Services (HHS) to comply with a need to investigate our compliance with HIPAA
Disclosures Permitted Without Patient Endorsement or Authorization

- For Treatment, Payment or Health Care Operations (our routine operations to provide care)
- Public Health Authorities such as the Health Department
- Social Services, Protective Agencies
- Health Oversight Agency
- Workers Compensation
- Law Enforcement / Legal Proceedings
- Coroner / Funeral Directors
- Organ and Tissue Donation
Disclosures Permitted Without Patient Endorsement or Authorization

- To Lessen a Serious / Imminent Threat
- Correctional Institution / Correctional Guards
- Research
- Fundraising
- Armed Forces
- National Security and Intelligence
- Protective Services for the President and Others
Disclosures Permitted Without Patient Endorsement or Authorization

- Remember, when possible, use the minimum necessary amount and type of protected health information to accomplish the task or purpose.
- Associates are permitted access to protected health information according to the minimum amount necessary to perform their job responsibilities.
- Associates are only authorized to access protected health information for the patients they are caring for. Associates who fail to adhere to this policy are subject to disciplinary action which may, depending on the infraction, result in termination.
Disclosures That Require Patient Endorsement

• Hospital Directory Information
  It contains the following information: Patient’s name, condition without providing the diagnosis, location within the hospital, and religion (disclosed to clergy only). This information may be provided to clergy or anyone that asks for the patient by name. The patient has the choice to “opt out” or not be listed in the hospital directory.

• Opting Out of the Directory
  When a patient opts out, a restriction agreement is signed, placed in the front of the medical record, and a purple arm band is placed on the patient to alert staff of some sort of restriction.
Disclosures That Require Patient Endorsement

- **Persons Involved in a Patient’s Care / Notification Purposes**
  - Information may be disclosed to a family member, other relative, close personal friend, or significant other named by the patient. We are not authorized to disclose information about the patient to persons not named by the patient.

- **Assignment of Personal Identification Numbers (PIN)**
  - Admitted patients are provided a 4 digit PIN number upon registration. Admitting will record the number on a brochure sent with the patient to the unit. The nurse is to describe the use of the pin number to the patient or designated representative. The patient / designated representative is in charge of giving the PIN number to those to be included in the sharing of patient information. The PIN number should be requested by staff when ever inquiries concerning the patient are made, whether by phone or in person.
Disclosures That Require Written Patient Authorization

Utilization of Behavioral Health Records with the following exceptions:

- if the notes are needed to carry out treatment, payment, or healthcare operations by the originator of the notes
- supervised training of students
- if needed by the hospital to defend legal action
- Used by a medical examiner or coroner
- Requested by the Secretary of Health & Human Services
- The disclosure is required by law
Marketing purposes unless:

- The marketing is done in a face to face communication (such as the 4-H fair) with the patient and/or is a promotional gift of nominal value provided by Carroll Hospital Center
Disclosures and Personal Representatives

If a personal representative has the authority to make decisions or act on behalf of the patient (including emancipated minors), we will disclose protected health information to the patient representative according to applicable state law.
Consider this situation:
When a patient’s husband called to double-check the time of her dental appointment, the receptionist thought it was a perfectly reasonable request and gave him the information. Two hours later, the estranged husband parked outside the dentist’s office and, when the patient arrived, pulled out a gun and shot her.
This is a true story that occurred outside of our state. A seemingly harmless request turned into a tragedy. Circumstances within our society challenge us daily to implement safeguards to protect our patient’s privacy.

We can never be too careful when disclosing patient information, take all necessary precautions to ensure patient privacy and security!
Right to Request Restrictions

- A Restriction Agreement must be completed by the patient.

You can locate the Restriction Agreement on the hospital Intranet site under Departmental Policies, HIPAA.

- We will honor requests to restrict PHI: to family, clergy, the hospital directory.

- If the patient requests that PHI be restricted for treatment, payment, or healthcare operations, we may or may not agree with the request.

- The Restriction Agreement may be terminated by the physician without the patient’s agreement if the information is needed for emergency care or treatment.
Right to Request Confidential Communications

- The patient may request that their PHI be communicated by Carroll Hospital Center to them by an alternative means of communication and/or alternative location.
- This requires a written request by the patient to the PI department. An explanation by the patient is not needed.
- Once the disclosure is determined to be appropriate, the information will be communicated/delivered to the patient in a secure and confidential manner.
Patients must be given clear written explanations of how we may use and disclose their health information. This will be accomplished through the privacy notice.

The Privacy Notice must be clearly displayed in accessible and prominent areas of the hospital, the web site and available for the vision, hearing impaired as well as ...

You may find the Privacy Notice on our internet site at click here:

www.ccgh.com/content/PrivacyNotice.htm
A copy will be given to all patients entering the hospital for the first time. (this is a requirement)

This will be handled during the registration process by the registrars.

In addition,

The registration face sheet has an area that all patients will initial that acknowledges that they have received the Privacy Notice.
Right to File a Complaint

- Patients have recourse if they feel their rights are violated
- They may contact the Director of Performance Improvement for further questions or information
- They may file a written complaint with the PI department.
What to Do if You Feel There Has Been a Violation of HIPAA

- Report the matter to your manager and the Privacy Officer as soon as possible
- Take corrective actions as directed
HIPAA Security
HIPAA Security

- HIPAA Security is concerned with ensuring the security of patient protected health information that is electronic.
- Electronic patient protected health information is called ePHI.
- Before we look at some specifics concerning ePHI, we’ll review some basic information concerning our responsibility when using electronic systems.
The Use of Electronic Systems

- **Human Resources policy # 18.309** details Associate responsibility in using hospital electronic systems: “Carroll Hospital Center provides electronic communications systems as tools to assist in Hospital business communications. These electronic systems are hospital property and are for hospital business only.”

- The policy also states that the hospital may choose to **monitor** the use of these systems at any time. Take the initiative to use electronic systems for hospital use only...it’s about your integrity!
Policy on the Use of E-mail

- Communications of a harassing nature, obscene messages, those that might demean another’s religion, ethnic background, age, sexual orientation, disability, chain letters, illegal unethical activity, commercial activity, gambling, political activity or any activity that would adversely affect the hospital is prohibited.

- Appropriate disciplinary action will be taken against Associates found to have engaged in prohibited use of E-mail. Human Resources can review, audit, and intercept electronic communications without Associate approval.

Now back to HIPAA Security legislation...
There are three components to the HIPAA Security Regulations:

- **Administrative Safeguards**: Include the policies and procedures created to ensure HIPAA Security compliance.
- **Physical Safeguards**: Physical safeguards cover the protection of physical things such as computer systems and high tech equipment as well as the facility where ePHI is located and stored.
- **Technical Safeguards**: Technical safeguards include all of the technology that make the physical safeguards possible. In most cases, our IS department is responsible for these systems.

We’ll take a closer look at each component.
Administrative Safeguards
Administrative safeguards include:

- Rules on workplace security such as who can access ePHI and who cannot
- Security detection systems
- Security policies
- Contingency plans for emergencies or disasters
- ePHI back-up systems
- Audits and ongoing evaluation of our Security compliance

Passwords are included under the Administrative Safeguards. Let’s take a closer look at passwords and password management.
Passwords
Passwords

Some password basics include:

- make up a password that is not easily guessed or cracked by someone else that may rule out passwords associated with family and pet names, or birthdates
- don’t use number strings such as 1234... or 8888, real words, or user ID’s as passwords as these can be easily cracked.
- make a password that you can easily remember, that prevents you from creating a vulnerability to access when you have to write them down to remember them!
How to Create a Good Password

• Pick a subject area of interest to you, such as music, movies, novels, or poetry (keep this a secret)
• For each password choose a line in a song or poem, or the name of a movie or book.
• If your password must be at least 6 alphanumerical characters in length, select the first letter of the first three or four words in that line or name. Then insert a few numbers to make up the full password
Password Security Basics

- Don’t tell anyone your password, including IS Associates.
- Don’t write your password down anywhere.
- When you decide on a password, make sure it can’t be guessed.
- If you think there’s even a chance someone else might know your password, change it.
- Make sure no one is standing near you when you enter your password.
- Change your password every 3 months on systems that contains ePHI.
Physical Safeguards
What is a workstation? You may be surprised. A workstation can be defined as: “an electronic computing device, for example, a laptop or desktop computer or any device that performs similar functions, and electronic media stored in its immediate environment.”

Physical Safeguards include among other things, the security and use of the workstation.
Physical Safeguards

Physical safeguards include:

- Facility access controls (ex. allocation of keys, construction maintenance records) to protect areas where ePHI is stored
- Parking restrictions to control access to certain areas of the facility
- Security guards, Associate ID badges and visitor badges
- Location of work stations away from public areas when possible
- Physical access controls such as workstation guidelines to guard against unauthorized access, including laptops and PDA’s on and off site
- Procedures to ensure the security of ePHI when moving or disposing of hardware or software both inside and outside of the facility
- Automatic log-off
Physical Safeguards

- Do not use our computers and networks for other than approved business functions.
- Never install software on our computers and laptops from home, or download software off of the intranet.
- Do not download files to the “C” drive; it creates a vulnerability for ePHI and in addition, it is not backed up...you could lose files.
- Software purchases and installations must be approved by IS.
- Do not leave a computer unattended and logged-on.
- Protect computer screens with ePHI from view from others.
Physical Safeguards

- Protect ePHI from others when working on a laptop at home
- Log off and turn off all software containing ePHI at the close of the work day
- Portable computing devices, such as flash drives are to obtained from the IS department
- Do not download any ePHI onto any unapproved portable devices without expressed permission by The Security Officer
Technical Safeguards
Technical Safeguards

Technical safeguards include:

- Access controls for electronic systems that hold ePHI
- Integrity controls to protect ePHI from alteration or destruction such as virus-checking software
- Transmission safeguards to protect ePHI transmitted over open networks
- Encryption that converts ePHI into secret code for transmission over public networks
- Authentication policies to verify if the people logging on to the system are who they claim to be
Technical Safeguards

Technical safeguards include:

- Monitoring systems to track who’s logging into the system successfully and who’s trying to log in unsuccessfully.
- Internal system audits and controls to track and record daily activity in information systems and to look for abnormal or suspicious behavior.
- The IS department provides reports to managers as to Associate access to ePHI. Make sure you only access the medical record patients you are caring for.
- Reporting systems and alarms to alert of possible intruders.
Security compliance will not work without you. We have to think differently…think “security first” in the same way we now think “safety first”
Unstable Patient Transfers and Provision of “FREE CARE”
• In 1986, congress passed EMTALA to protect patients and eliminate hospitals from diverting patients needing care to other hospitals because of a lack of insurance or ability to pay.

• This really ensured that those needing care that may not have insurance had a means to get emergency care. This law has also been called the “FREE CARE, or Anti-patient dumping” law.
There are three requirements for Medicare participating hospitals with respect to patients requesting emergency care:

- Hospital must conduct an appropriate **medical screening examination** to determine if a emergency medical condition exists.
- If a medical emergency condition exists, the hospital **must provide the treatment necessary** to stabilize the condition, or comply with requirements to transfer the patient that has a condition that has not been stabilized.
- Adherence to **transfer requirements** for patient conditions that have not been stabilized.
EMTALA

An Unstable patient is transferred under the following conditions:

- MD certifies in writing that the benefits of transfer outweigh the risks
- Patient (legal representative) consents in writing to knowing the risks and benefits of the transfer
- Receiving hospital accepts transfer and has space to take patient
- Transportation occurs with qualified staff as determined by the sending physician
- Medical record sent with patient
- Treatment goal is to minimize risk to the patient
EMTALA law can apply in any area of the hospital, not just the ED:

- When an individual or someone for the patient requests exam or treatment for a medical condition EMTALA law applies
- When a prudent layperson (ex. hospital volunteer) believes, based on appearance or behavior that the person is in need of emergency care
- If the patient arrives in an area that is not the dedicated ED and the two conditions above are met, EMTALA law applies

If these situations were to occur, it is our responsibility to ensure the patient is taken to the ED for evaluation and possible treatment
A patient approaches the front desk of a hospital and states that they have a horrible toothache and asks if someone in the ED can see them. The organization sends the patient away, stating that we don’t provide that service in the ED.

Yes, there is an EMTALA violation. This patient may have been suffering from other health issues and should have been given the opportunity to be seen by a healthcare provider.

You will need to click twice on a section of this slide to see the answer before moving forward.
A patient is admitted to the ED of hospital A with a broken jaw. The patient is later found to be HIV+. Hospital A attempted to transfer the patient to Hospital B. Hospital B refused. Hospital A discharged the patient with cab fare and instructed the patient to go to hospital B.

Yes, there is an EMTALA violation, Hospital A was responsible to treat the patient if it could provide that service. Hospital B could have also been at fault for refusing to accept the patient.

You will need to click twice on a section of this slide to see the answer before moving forward.
A 4 year old was admitted to a hospital in Maryland with a severe dog bite to the eye. A specialist physician was called in to treat the patient and told the nurse the patient could wait when it was realized that they were insured by Medicare. The nurse in frustration told the child's mother to take the child to the Wilmer Eye center at Johns Hopkins. Upon arrival the child was admitted and quickly taken to the operating room.

**YES, there is an EMTALA violation, the nurse should have used the chain of command to resolve the patient care issue.**

You will need to click twice on a section of this slide to see the answer before moving forward.
Protecting our Patient's Privacy and Security is Part of the Quality Care we Provide.

Be sure you know and follow Carroll Hospital Center compliance regulations and procedures in order to protect you, as well as your patient.

You can’t afford not to!

For a Review of Policies and Procedures
Please refer to the following Quick Reference Guides for:
HIPAA Privacy
HIPAA Security
Located on the Hospital Intranet Under the Orientation Access Button

Please answer the questions to receive credit for completing this program