Understanding HIPAA: Privacy and Security Rules

What is HIPAA?

- HIPAA is the acronym for the Health Insurance Portability and Accountability Act that was passed by Congress in 1996. HIPAA does the following:
  - Provides the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs;
  - Reduces health care fraud and abuse;
  - Mandates industry-wide standards for health care information on electronic billing and other processes; and
  - Requires the protection and confidential handling of protected health information

  This portion of the course will cover the HIPAA Privacy and Security Rules

How does HIPAA apply to You?

- Anyone that looks at, uses or shares Protected Health Information (PHI) is affected by HIPAA
- Anyone working in or for Mary Lanning Healthcare is responsible to protect patient information.

HIPAA: Privacy Rule

- Assure that individual's health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being.

- HIPAA is the hospitals obligation to protect any and all information from others who do not have a business reason to view it or discuss it.

What information is Protected?

- Individually identifiable health information held or transmitted in any form or media, whether electronic, paper, or oral.
- This information is called “protected health information” or **PHI**.

PHI (Protected Health Information)

- You must protect an individual's PHI.
  - PHI is information related to a patient's past, present or future physical and/or mental health or condition
  - Can be any form: written, spoken, or electronic (including video, photographs, and x-rays)
  - Includes at least one of the 18 personal identifiers in association with health information (listed on the following slide)

PHI Examples

- Name
- Postal address
- All elements of dates except year
- Telephone number
- Fax number
- Email address
- URL address
- IP address
- Social Security number
- Account numbers
- License numbers
- Medical record number
- Health plan beneficiary #
- Device identifiers and their serial numbers
- Vehicle identifiers and serial number
- Biometric identifiers (finger and voice prints)
- Full face photos and other comparable images
- Any other unique identifying number, code, or characteristic

When Should You

View PHI
Use PHI
Share PHI

Access information only when necessary to perform your job duties

Use only the **minimum necessary** to complete the task

HIPAA: Security Rule

- Covers e-PHI (electronic protected health information).
- Protects individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.

E-PHI

- Security Rule applies to e-PHI the same restrictions that the Privacy Rule applies to all PHI but in addition you must be able to maintain the integrity and availability of e-PHI.
  - Integrity
    - e-PHI is not altered or destroyed in an unauthorized manner
  - Availability
    - e-PHI is accessible and usable on demand by an authorized person

Computer Security

Create a strong password and do not share your username or password with anyone

- Log off your computer terminal when you are done, or if you walk away even for just a few moments

Ensure information on computer screens is not visible to people who pass by your area

- Ensure your system has anti-virus and all necessary security patches and updates.

Verbal Exchanges

- Patients may see normal clinical operations as violating their privacy
- Be aware of your surroundings when talking
- Do not leave PHI on answering machines
- Ask yourself, “what if it was my information being discussed like this?”

Know where you left your paperwork!

- Check printers, faxes, copier machines when you are done using them.
- Ensure paper charts are returned to applicable areas in nursing stations, medical records, or designated file rooms
- Do not leave hard copies of PHI laying on your desk; lock it up in your desk at the end of the day
- Seal envelopes well when mailing

Privacy Breach from Lost, Stolen, or Misdirected Information

- A privacy breach can occur when:
  - Information is physically lost or stolen
    - Paper copies, films, tapes, electronic devices
  - Information is misdirected to others outside of MLH
  - Verbal messages are sent to or left on the wrong voicemail or sent to or left for the wrong person
  - Mislabeled mail, misdirected email
  - Wrong fax number, wrong phone number

Examples of Privacy Breaches

- Talking in public areas, talking too loudly, talking to the wrong person
- Lost/stolen or improperly disposed of paper, mail, films, notebooks
- Lost/stolen laptops, PDAs, cell phones, media devices (video and audio recordings)
- Lost/stolen zip disks, CDs, flash drives, memory drives
- Hacking of unprotected computer systems
- Email or faxes sent to the wrong address, wrong person, or wrong number
- User not logging off of computer systems, allowing others to access their computer or system

Snooping Constitutes a Violation

- As a nurse or a CNA, you may have access to a patient's medical record. But that does not give you the right to look at it if it does NOT pertain to your job.
- You may not access your own records or your family members' record.

By simply working in the hospital, you may see patients you know, see information about a patient, or overhear clinical conversation. You may NOT share this information with others.

THAT IS A VIOLATION!

Reporting Privacy Breaches and Security Incidents

- Immediately report any known or suspected privacy breaches (such as paper, conversations, suspected unauthorized or inappropriate access or use of PHI) to your Supervisor, Manager, Director or the Compliance and Privacy Officer.

How to Report a Violation

CALL or EMAIL: Compliance / Privacy Officer

Jennifer Gaede 402-460-5505 (Ext 5505) jgaede@marylanning.org

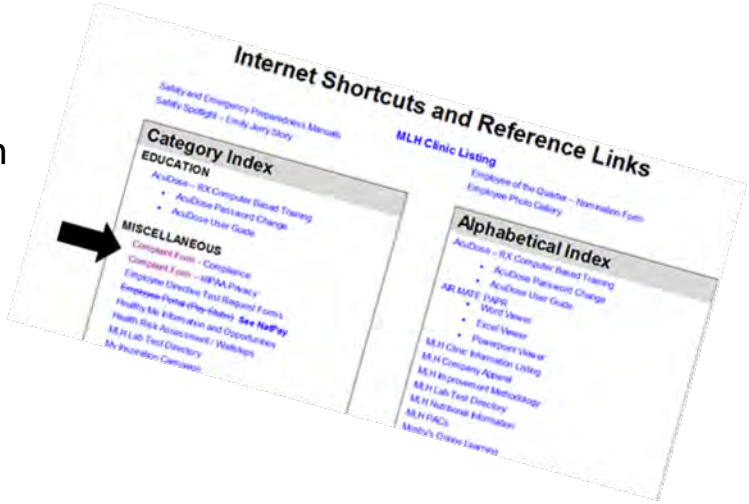
Information Officer

Lisa Nonneman 402-460-5742 (Ext 5742) lnonneman@marylanning.org

Reporting Forms – Located in Internet shortcuts (Icon on MLH Computers' Desktop)
Computers available in the MLH Library located in the basement of the Medical Services Building

Compliant Form – HIPAA Privacy
- HIPAA Violation reporting form

Complaint Form - Compliance
- Compliance complaint/violation reporting form



ANONYMOUS HOTLINE Number

– established to report Compliance issues

- (402) 460-5522
- Monitored daily

Conclusion

- Remember… to the patient, ALL information is private.
- This includes:
  - Personal information
  - Financial information
  - Medical information
  - Protected health information
  - Information in any format: spoken, written, or electronic