Mary Free Bed Rehabilitation Hospital – HIPAA Regulations

The federal government has established comprehensive privacy regulations to protect individually identifiable health information, known as protected health information or "PHI." The privacy regulations are part of the Health Insurance Portability and Accountability Act (HIPAA) that became effective April 2003.

Some aspects of the rule give specific instructions as to what can and cannot be communicated regarding patient information, while other areas of the rule give facilities the ability to establish "reasonable" procedures to protect patient privacy.

Key Elements

The privacy rule governs the ability to use and disclose PHI in any form (electronic, paper, verbally)

Covered entities can use or disclose PHI:

- To the individual
- For treatment, payment or healthcare operations
- For treatment activities of a healthcare provider

Incidental disclosures are permitted (patient's roommate overhears conversation between patient and nurse) as long as "reasonable" measures are taken to prevent this type of disclosure (pull the curtain in the room).

"Minimum Necessary" should be your guide. The privacy rule states that a covered entity must make reasonable efforts not to use or disclose more than the minimum amount of PHI necessary to accomplish the intended purpose, use or disclosure. This means you only access the information you need to do your job. For example, a healthcare worker doesn't need access to the entire medical record if he/she only needs the information on the face sheet in order to do the job. In another example, the entire medical record is not sent to a requestor who really only needs the discharge summary for the purpose of their request.

Just because you have access to information, does not mean you should access that information. It's against our organizational policies to access your patient information or that of a family member. (ie: looking up your own records in Affinity or Cerner.) If you need access to this type of information, contact Health Information Management and we can assist you in obtaining the appropriate authorizations.

Patient Rights

Patients have a number of rights regarding their PHI:

- To authorize the use and disclosure of PHI
- To inspect and receive a copy of their own PHI
- To receive an accounting of certain PHI disclosures

• To request an amendment of their PHI
• To file a complaint about alleged violations
• To request restrictions on use and disclosure of PHI
• To request communications of PHI by alternative means or at alternative locations
• To receive a notice of privacy practices

Important Points to Remember

Protecting patient privacy requires the efforts of all staff. Remember:

• Only access confidential information if you have a "need to know" to do your job
• Do not discuss patient information in public areas (elevators, cafeteria, etc)
• Dispose of confidential patient information in designated "shredding" containers
• Refer privacy related questions or concerns to your supervisor or Jill Bustin at 616.840.8216

HIPAA Security Regulations

The federal government has passed a comprehensive set of HIPAA regulations dealing with the protection of patient health information. This includes privacy regulations and security regulations. The HIPAA security regulations that went into effect on April 20, 2005, deal with securing patient Protected Health Information (PHI) while it's stored in an electronic format.

This Electronic Protected Health Information (EPHI) could be stored on computer systems or other forms of electronic media such as CDs, memory sticks, hard drives, email and portable devices such as laptop computers or PDAs. This EPHI must be secured to assure privacy. The following is a list of things you should understand to help protect of this information.

Protected Health Information (PHI)

Protected Health Information includes any information created or received by a covered entity relating to:

• The health or condition of an individual
• Any healthcare provided to an individual
• Any billing or financial information for healthcare
• Any information that identifies an individual or provides a way to identify an individual (i.e. Social Security number, name, email address, street address, etc.)

Computer Security

• Always lock your workstation or log out of the system when walking away from your work area. This will help prevent others from accessing Protected Health Information.
• NEVER give anyone your login ID or password.
• NEVER allow anyone to access your computer while you are logged into the network. Your login ID is your identity on our network. Access to PHI is audited by your login ID.

• Keep your computer screen turned away from others while accessing PHI so they cannot read over your shoulder.

Electronic File Storage

• Pre-authorization from the IT Department is required to download PHI information to other forms of electronic media such as CDs, memory sticks, laptop computers, etc.
• NEVER download PHI information onto your personal computer.

Emailing PHI

Any email that contains PHI is REQUIRED to be encrypted. You can encrypt email messages by clicking on the "Encrypt ZixSelect" button in your Outlook e-mail.

Auditing Access to PHI

• You should only access the patient information you need to perform your job duties.
• The IT department performs periodic audits to determine access to PHI.

Incident Reporting Process

If you are aware of any HIPAA violations or suspicious activity, you are responsible to report it to one of the following people:

Jeff Burns, Security Officer: 616.840.8338
Jill Bustin, Privacy Officer: 616.840.8216
Compliance Hotline: 616.356.1891