HIPAA REGULATIONS
Privacy and Security Standards

BATES COUNTY MEMORIAL HOSPITAL
Butler, Missouri

TRAINING MODULE: HIPAA REGULATIONS / PRIVACY AND SECURITY STANDARDS

The Health Insurance Portability and Accountability Act, or HIPAA, is a federal rule that was designed to protect patients from the inappropriate disclosure of their protected health information. Included in HIPAA are standards for privacy and security. The *privacy standards* went into effect on April 14, 2003, and the *security standards* went into effect on April 21, 2005.

PRIVACY VERSUS SECURITY STANDARDS

The privacy and security standards addressed in the HIPAA regulations are designed to protect health data without limiting care to patients. The *security standards* deal with the measures that covered entities can take to keep their information safe. An example would be encrypting information before it is sent over the Internet. The *privacy standards* deal with things patients may expect from covered entities in terms of the way health information is used. An example would be limiting who has access to their records.

The HIPAA law is essentially a call to action regarding the sharing of private information, and creates safeguards to guarantee that only those people or entities that have a real need for protected health information have access to it. HIPAA came about as the result of concerns from patients regarding what they saw as breaches in confidentiality.

THE BASICS REGARDING HIPAA

Covered Entity

There are four entities covered by this rule: healthcare providers, health plans, healthcare clearinghouses, and their business associates.

A *healthcare provider* is defined as any person or business that furnishes bills or is paid for healthcare services in the normal course of business. This includes:

Physicians	Licensed healthcare providers
Hospitals	Outpatient physical therapy
Social work services	Certified nurse-midwife services
X-rays completed at home	Home health agencies
Pharmacists	Home dialysis supplies and equipment
Nursing homes	

Essentially, in a healthcare facility, anyone who uses or may see confidential patient information is included. For example, medical staff in a hospital involved in the direct care of a patient will have access to all the medical records in order to provide the best possible care.

A *health plan* is defined to be an individual or group plan that provides for, or pays the cost of medical care. This includes:

HMOs	Medicare/Medicaid	Federal programs – TRICARE
Insurance companies	Employee benefit plans	

A *clearinghouse* receives health information from providers and plans and helps standardize that information into the required format for claims processing. Examples would be billing services, repricing agencies, and third party administrators.

Business Associates are defined as a person or entity that provides certain functions, activities or services for or to a covered entity, but is not a member of the healthcare provider, health plan or other covered entity's workforce. Examples would be auditors, accountants, lawyers, consultants, billing firms, and data processing firms. These business associates must also comply with HIPAA. Plans and providers must have contracts with these associates that state the purposes for which they may use and disclose medical record information. In fact, a contract must be in place before the business associate can see and use protected health information.

Protected Health Information

Health information is defined as any information, whether spoken, electronic or written, that relates to the health of an individual, the health care provided to that individual, or payment for the health care provided. This applies even after it is printed, discussed orally or otherwise changed in any form.

Protected Health Information or PHI is health information created or received by a covered entity, regardless of form, that could be used directly or indirectly to identify the individual. This can be in the form of paper records, electronic files, and video or audiotapes, and includes if it is read off a computer screen and discussed, transmitted over the Internet, photographed or duplicated. For example, in the hospital, the medical records used are considered to be PHI.

PHI includes *Individually Identifiable Health Information (IIHI),* or information that identifies the individual. Information is considered to be de-identified if it does not identify the individual, or if the hospital has no reasonable basis to believe it can be used to identify the individual. When information is de-identified, it is not subject to the HIPAA requirements and can be disclosed. A person is presumed not to be identifiable if all of the following has been removed:

Name	Name of relative or employer
Address	Birth date
City	Telephone number
County	Fax number
Zip code	Social Security number
Finger prints	Voiceprints
Medical record number	Photographs
Account number	Health beneficiary
License number	

Minimum Necessary Requirement

The bottom line is that any information that relates to a patient's health cannot be used unless authorized by either the patient or someone acting on the patient's behalf, or unless permitted by regulation. The facility must limit access to only those individuals who need the information for a legitimate purpose.

With few exceptions, HIPAA ensures that an individual's health information may only be used for health purposes. For example, health information may not be used by employers to make personnel decisions, or used by financial institutions to make decisions regarding an individual, without authorization by the patient.

Under the law, any information that is shared should be limited to the "minimum necessary", that is the least amount of information necessary to accomplish the purpose of the request. For instance, if you want to report a suspected case of child abuse, you would not provide a complete copy of the medical record, but would abstract only that information which is needed such as the dates the child was admitted or treated at the hospital and the relevant information as to why the abuse was suspected.

However, the minimum necessary does not apply to the sharing of medical records for treatment purposes, as physicians and other healthcare providers need full access to medical records in order to provide the best possible care; and it also does not apply when patients authorize disclosures to federal or state agencies or third parties.

In some cases, however, there is a fine line between a person's right to privacy and a facility's responsibility to share private information. In certain situations, it may be in the best interest of the public to disclose specific information. Examples include reporting a person with a communicable disease to the Department of Health; the coroner's involvement in a suspicious death; emergency situations; some law enforcement and research activities; criminal and administrative proceedings; and activities related to national defense and security.

PATIENTS HAVE RIGHTS

Thanks to the HIPAA regulations, patients have rights they have never had before. As a healthcare provider, you must be aware of your patients' rights as well as you role in the process.

- *Patients must be given clear written explanations of how your facility may use and disclose their health information.* This document is known as the facility's Notice of Privacy Practices. It could include a summary of Patients' Rights and when information can be disclosed such as for treatment purposes, for payment. It could also include appointment reminders and special situations such as for law enforcement, court orders, or worker's compensation programs and how their records can be amended.

- *Patients have the right to access their medical records* in order to view and copy information that is used to make decisions about them, and it must be made available within 30 days of a written request. Some exceptions would be psychotherapy notes, laboratory results, and information compiled for use in legal action. Facilities have the right to deny access in the event that the information would endanger the life or safety of the patient or another.

- *Patients have the right to amend incorrect or incomplete information in their records.* The patient can request that the medical record be altered to reflect true and accurate information; however, if the facility believes the information is correct, they can deny this request and they must provide the patient with a notice of a statement of disagreement.

- *Patients have the right to request a free accounting every 12 months of how their health information has been used.* This includes any disclosure made for reasons other than treatment, payment or healthcare operations such as for a court order. This must include the date of disclosure, the name and address of each organization that received the information and a brief description of what was disclosed and the purpose. This must be provided to the patient within 30 days of the request.

Patients must be given notice of their right to be able to restrict who will get information. For example, a patient can request that no information be shared with certain family members.

Patient has recourse if their rights are violated.

- If a patient feels his information was shared inappropriately, he has the right to file a formal complaint with the Department of Health and Human Services (Office of Civil Rights).

- Each facility must designate a contact person to receive complaints of violations and this name must be listed in the privacy notice.

- A complaint must be filed within 180 days of knowing of the act, and a record must be kept of the complaint and how it was resolved.

- If a complaint is not responded to in a timely basis, it is considered a grievance under the Patient Rights standards.

HIPAA IN EVERYDAY USE

HIPAA rules will affect how you use and disclose patient information on a daily basis. Some of these issues are topics that are covered under state law as well. In these circumstances, be aware that weaker state laws are over-ridden by the HIPAA regulations. If state laws are more stringent, then they should be followed.

Patient Directory

Anytime a patient enters a facility, their identity is included in some form in a patient directory. Here are some rules you will need to remember:

- The patient must be given notice that information will be given out in a directory. This can be verbal or written. There must be documentation of the patient's approval and whether this notice was given to them in writing or verbally.
- Professional judgment may dictate that a person's identify be kept confidential; for example, protecting the identity of gang related shooting victim.
- Identities can be disclosed to entities providing relief in disasters, such as the Red Cross, during fires, floods, or terrorist attacks.
- Patients must be given the opportunity to choose not to be included in the patient directory before the information is disclosed.

It is the patient's responsibility to choose not to be included in the patient directory. However, they should be made aware that by doing so the facility will not be giving information to callers and that flowers may not be able to be delivered.

Clergy/Other Religious Personnel

Upon admission, the patient has the right to restrict religious information. For example, the patient may wish not to disclose a religious preference; they may ask that outside clergy not be given their name or location; or they may ask that no visitation by the facility's religious personnel be granted. *When sharing information with clergy, no specific medical information may be shared concerning the patient.*

Passcode Family/Friends

Patients are given the opportunity to receive a passcode which can be given to family and friends. This passcode allows the hospital to disclose oral information to those persons possessing a passcode. No information related to a sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), human immunodeficiency virus (HIV), behavior or mental health services, or treatment for alcohol and drug abuse will be disclosed with a passcode.

Patient Authorization

An authorization form allows for the release of medical information for non-routine disclosures and most non-healthcare purposes, such as employment determinations, marketing and fundraising activities not specified in the regulations as part of healthcare operations.

Parents and Minors

Parents and guardians are considered the "personal representative" of the minor child and have a right to see the minor's protected health information. Generally, a minor cannot consent to treatment; however, by Missouri Statute, a minor can consent for treatment if:

- Married,
- Parent or legal guardian of a minor child,
- In case of pregnancy (excluding abortions), venereal disease, drug or substance abuse.

In an emergency, any adult standing in loco parentis can consent for the treatment of a minor.

Sign-In Sheets

Sign-in sheets, x-ray light boards, and bedside medical charts are not disallowed under HIPAA as long as reasonable precautions are taken to safeguard patient information. When using sign-in sheets, it is strongly recommended to not include private information (such as the reason for the visit) to be included on the sheet.

Missing Persons

Information regarding missing persons can be shared by a facility if the request from police is received in writing or orally; or the media makes an announcement asking for the public's assistance in identifying a suspect. In that case, the following can be disclosed:

- Blood type or Rh factor, along with the time and date of death
- Physical characteristics such as scars, height, weight, gender, race, hair color, eyes, and facial hair – for instance, a beard,
- No dental records or DNA data may be released.

Patient Deaths

If there is a suspicious death of a patient, personnel may report to police the suspicion that the death was the result of criminal conduct. This allows the police to begin an investigation in a timely manner.

Cadaver Donation of Organs

Donation of organs includes organs, eyes, and tissues. Hospitals can disclose protected health information if they are engaged in the procurement, banking or transplantation of the organs.

Law Enforcement

Law enforcement requests must also follow HIPAA regulations. Patient information may be shared if asked to do so by a law enforcement official:

- In response to a court order, subpoena, warrant, summons or similar process;
- To identify or locate a suspect, fugitive, material witness, or missing person;
- About the victim of a crime if, under certain circumstances, the person's agreement is unable to be obtained;
- About a death believed to be the result of criminal conduct;
- About criminal conduct at the facility; and
- In emergency circumstances to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.

ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI)

Providers are required to protect electronic health information (ePHI) under the HIPAA Security Standards. ePHI would include anything that is created, received, maintained, or transmitted electronically. In order to safeguard ePHI, the employee should follow these guidelines:

- Passwords
  - Must be (12) characters long and include non-alphanumeric characters or symbols
  - Must be changed every 60 days
  - Do not share passwords
  - Do not leave passwords where others can access
  - Must contact Information Systems Department if password is lost/compromised
  - Must log off after using computer with your password

- Faxes
  - Must verify fax numbers
  - Must use a fax cover sheet that includes a Confidentiality Notice
  - Fax machines must be located in secure areas

- E-mails
  - Must verify e-mail addresses
  - Must encrypt e-mail (ZSECURE in subject line)
  - Must include confidentiality statement in body of e-mail
  - Sensitive information should not be e-mailed (AIDS/HIV infections, other sexually transmissible or communicable diseases)

REPORTING AND NOTIFICATION OF BREACHES

All suspected privacy breaches are to be reported to the hospital's Privacy Officer for investigation. All suspected security breaches are to be reported to the hospital's Security Officer for investigation. Failure to report a breach can result in termination of employment or other relationship with the provider. Providers are required to notify patients when a determination has been made that a breach of their PHI or ePHI had occurred.

HIPAA REGULATIONS
Privacy and Security Standards

PENALTIES

HIPAA is serious about patient privacy. Anyone who obtains or discloses protected health information for personal or commercial gain or for malicious purposes is subject to sanctions and disciplinary actions such as suspension, termination, criminal and civil penalties.

Violation not known or reasonably known – At least $100 per violation, $25,000 max for identical violations in calendar year.

Violation due to reasonable cause but not willful neglect – At least $1,000 per violation, $100,000 max for identical violations in calendar year.

Violation due to willful neglect, if corrected – At least $10,000 per violation, $250,000 max for identical violations in calendar year.

Violation due to willful neglect, if not corrected – At least $50,000 per violation, $1.5 million max for identical violations in calendar year.

Knowingly obtain or disclose identifiable health information – Up to one year in prison.

Committed under false pretenses – Up to five years in prison.

Intent to sell, transfer, or use for commercial advantage personal gain or malicious harm – Up to ten years in prison.

ACCESS TO POLICIES AND PROCEDURES

Bates County Memorial Hospital's HIPAA policies and procedures can be located on BCMH e-CONNECT. To access these you must go to the *Resources* tab and click on *More Resources.* Then click on the *Policies and Guidelines,* select *HIPAA* and *Policy.*

PRIVACY OFFICER
Doncella Liggins, Director of HIM
660-200-7028

SECURITY OFFICER
Marcia Cook, CIO
660-200-7117