Health Insurance Portability and Accountability Act

(HIPAA) 1996

Presented by
College of Health Sciences and Human Services
at Midwestern State University

3 Main Purposes of HIPAA

- Ensures insurance coverage for workers and their families when they change or lose their jobs.
- Guarantees security and privacy of Protected Health Information (PHI).
- Reduces the cost of health care by standardizing health care transactions.

Rules/Standards to Simplify Transmission of Health Care Info:

HIPAA sets rules/standards in the following areas:

- **Privacy Rules** – to protect the patient's privacy.
- **Security Rule** – to provide a single national standard for computer security.
- **Electronic Transaction Standards** – to mandate the use of Electronic Data Interchange (EDI) standards, allowing computers to automatically exchange without human intervention data about individuals.
- **National Identifiers**

Privacy Rules

- MSU Students must be aware of the Privacy Rules related to **Protected Health Information** (PHI).

Protected Health Information (PHI)

- **Health Information** – any information created or received that relates to the past, present or future physical or mental health of an individual.

- **Protected Health Information** – health information that contains data that may be used to directly or indirectly identify the individual.

Possible Data Elements in PHI

- Name
- Address
- Email Address
- Telephone Number
- Finger or Voice Prints
- Social Security Number
- Vehicle / Device Serial Number
- Health Plan Number
- Certificate / License Number
- Names of Relatives
- Names of Employers
- Fax Number
- Birth Date
- Photographic Images / X-Rays
- Internet (IP) Address
- Medical Record Number
- Account Number
- Web URL

Documents that may contain PHI

- Medical Records
- Laboratory and other test results
- Orders and prescriptions
- Clinician / Instructor Notes
- Patient lists with Dx
- Encounter forms, charge tickets, labels
- Computer screens
- PDAs used in clinical work

Personal Health Information may be used for:

- Treatment
- Payment
- Operations

Treatment

- PHI – may be used for treatment, with NO RESTRICTIONS.

Treatment includes:

- Provision and coordination or management of health care and related services by one or more providers.
- Coordination or management of health care by a health care provider with a third party.
- Consultation between health care providers related to treatment.
- Referral of a patient from one provider to another.

Health Care Operations

(Administrative, Business and Educational Functions)

- Quality Management
- Case management / coordination
- Outcomes evaluation and development of clinical guidelines (if not research)
- Protocol development
- Contacting health care providers and patients regarding treatment alternatives

Health Care Operations (Continued)

- Reviewing qualifications / competence performance of health care professionals
- Conducting training programs for health care students or practioners under supervision to practice or improve their skills as health care providers
- Training non-health care professionals
- Accreditation, certification, licensing and confidentiality

Minimum Necessary

- In payment or health care operations, workers should use only the MINIMUM NECESSARY INFORMATION to perform the task.

- *Example:* A worker should not share a patient's entire medical record with anyone except a health care provider who is giving a care to that patient.

Disclosure of PHI other than treatment must be:

- With patient consent and/or authorization
- With a Human Subject Review Waiver of Consent and/or Privacy Board Waiver of Authorization (research)
- As part of a Limited Data Set with Data Use Agreement
- As required by law
- PHI must be De-identified

De-identified Health Information

- Removal of the 18 identifiers makes the information de-identified
- De-identified health information may always be used or disclosed
- Health information may also be de-identified by documented statistical determination so that the chance of being able to use the information to identify an individual is very small.

Incidental Disclosures related to Treatment

- Incidental disclosures – a by-product of a permissible or required disclosure that cannot be reasonably prevented or is limited in nature

- Incidental disclosures associated with providing treatment are permissible when APPROPRIATE SAFEGUARDS are in place to protect the privacy of PHI.

Patients must be given Notice of Privacy Practices (NPP)

- NPP tells patients about how their PHI is released, describes their rights, and how to make a complaint

- At first instance of care after April 13, 2003:
  - Patients must be provided a Notice of Privacy Practice
  - Institution must receive acknowledgement from patient

NPP

- Patient needs to sign the NPP only once.
- NPP must be posted in prominent locations and provided to patients upon request.
- NPP may be posted on a website so patients may access and print
- In emergency cases, the NPP may be provided after the emergency is over.

Ability vs. Right to Access PHI

- MSU Students have the ABILITY to access patient records and other PHI as part of clinical/practicum experiences.

- Students have the RIGHT to access PHI only for:
  - Providing treatment or other authorized training purposes

Appropriate Incidental Disclosures

- Patient sign-in sheets with only name and check in times
- Calling a patient by name in the waiting room
  (should consider asking patients if they are opposed to this)
- Non-involved persons overhearing a clinician speaking with a patient

To Avoid Disclosure from Overheard Conversations

- Try to schedule conversations with patients in a private place
- When in a place that precludes the ability to assure total privacy, pay special attention to communicating in a way that minimized inadvertent disclosures.
- Speak Quietly

To Avoid Disclosure from Overheard Conversations (Part 2)

- Safeguard PHI on medical records, patient lists for training, scheduling, and billing, billing documents.
- Limit content of information left on answering machines.
- Only mail PHI in envelopes addressed to a specific individual that is clearly marked confidential.

To Avoid Disclosure from Overheard Conversations (Part 3)

- When faxing PHI, verify fax number before sending. If information is highly confidential, verify recipient is present and receives.
- Discard PHI materials, when appropriate, by shredding.
- Lock file cabinets containing PHI and lock doors to offices where PHI is housed.

To Avoid Disclosure from Overheard Conversations (Part 4)

- Follow the HIPAA rules/regulations of the clinical site to which you are assigned.

- KNOW WHAT THEY ARE.

To Avoid Disclosure from Overheard Conversations (Part 5)

- Secure PHI on desk and computer.
  - Lock up sensitive files.
  - Place PHI documents face down.
  - Keep computer passwords safe.
  - Turn monitor away from public view.
  - Log out of computer systems containing PHI if you will be away for a period of time.

To Avoid Disclosure from Overheard Conversations (Part 6)

- Do not leave PHI documents:
  - In a lecture or meeting rooms
  - In cafeteria, lounges, or restrooms

What happens if HIPAA Rules are NOT followed?

- Individual and/or organization may be fined $100/violation, up to $25,000 per person per year for each violation

- Criminal penalties: Up to $250,000 in fines plus prison time for:
  - Malicious acts and/or
  - Profiting from improper disclosure of PHI

References

- Medscape News
- U.S. Department of Health & Human Services
- Children’s Medical Center, Dallas Texas
- School of Allied Health Sciences, UTHSCSA, Recommendations for HIPAA Related Education Curriculum Task Force
- Office of Civil Rights: Standards for Privacy of Individually Identifiable Health Information