HIPAA Privacy

September 21, 2013
The Health Insurance Portability & Accountability Act (HIPAA) requires that the University train all workforce members (faculty, staff, residents and students) about the University’s HIPAA policies and those specific HIPAA required procedures that may affect the work you do for the University.
Overview

• This presentation provides a brief summary of the HIPAA Privacy Rule.

• It lists basic principles that all LSUHSC-NO faculty, staff, residents and students must understand and follow.
What Does HIPAA Do?

HIPAA is the *Health Insurance Portability and Accountability Act*, a federal law that...

- protects the privacy and confidentiality of a patient’s personal and health information.

- provides for electronic and physical security of personal and health information.

- simplifies billing and other transactions.
The Purpose of HIPAA

• To protect and enhance the rights of consumers by providing them with:
  – access to their health information
  – control of the inappropriate use of that information

• The Rule’s goal is to maintain the trust in the health care system and improve the quality, efficiency and effectiveness of health care delivery.

• Promotes the balance of:
  – the use of an individual’s health care information to advance economically prudent health care while protecting the privacy of the individual seeking medical care and treatment.
HIPAA Provides for the Following:

- Implementation of administrative, technical, and physical safeguards to ensure privacy of patient Protected Health Information (PHI).

- Policies and procedures for the protection of health information and individual patient rights.

- Mandatory faculty, staff, resident and student education on privacy policies and practices.

- Complaint process that accepts, records, and investigates patient complaints about the entity's privacy practices.

- Designation of a Privacy Official.
LSUHSC-NO and HIPAA

• LSUHSC-NO has a commitment to protect the privacy of the patient’s health information, in all situations.

• The privacy policies and procedures affect the tasks an employee performs and provides guidance in addressing situations where employees and students encounter PHI unexpectedly.
Training Methods Offered at LSUHSC-NO

- Online Training (KDS)
- Presentation/Classroom training
- Informational packets (Self-Study) for users who do not have network accounts
Who is Covered Under HIPAA?

- LSUHSC-NO, as a health care provider is a “covered entity” under HIPAA.

- This means that LSUHSC-NO must abide by the requirements of the Privacy Rule.

- One of the requirements is for LSUHSC-NO faculty, staff, residents and students to safeguard a patient’s PHI.
Who Has to Follow the HIPAA Law?

EVERYONE!!!!
What Patient Information Must We Protect?

• We must protect an individual’s personal and health information that:
  – Is created, received or maintained by a health care provider, health plan, employer, or health care clearinghouse.
  – Is written, spoken, or electronic.
  – Includes at least one of the 18 personal identifiers.
  – Could be combined with other readily available information to identify a patient.

• HIPAA says that this information is **Protected Health Information (PHI)**.
Examples of Patient Identifiers

- Patient name
- Date of birth
- Social Security number
- Driver’s license number
- Phone and fax numbers
- Mailing address
- Email address
- Hospital account number
- Medical record number
- Insurance identification number
- Medicare/Medicaid ID numbers
- Certificate/License numbers
- Device identifiers and serial numbers
- Vehicle identifiers and serial numbers
- Pictures that identify a patient as a patient
- Biometric identifiers, etc.
What is Protected Health Information (PHI)?

- Protected Health Information (PHI) is when *Patient Identifiers* are combined with:
  - Information about a patient’s health or condition.
  - Information about a patient’s health care.
  - Information about payment for health care services.
  - Genetic information about a patient, including genetic information about a patient’s relatives.

  Ex. Patient’s name and health diagnosis.
Examples of What PHI is NOT...

- **Company proprietary information:**
  - Business plans and strategy
  - Pricing strategies
  - Operating costs

- **Student health records**

- **Information regarding a person who has been deceased for more than 50 years.**

- **Information kept by an Employer:**
  - Name
  - Addresses
  - Salaries
  - Performance Evaluations
  - Medical Information
  - Workman’s compensation records
  - Criminal background checks
Points to Remember about PHI

• PHI can be written (paper, computer printout, email printout, or paper to paper fax, electronic (email or fax), or verbal/sign language.

• PHI reveals the state of a person’s health.

• PHI identifies individuals in such a way that it gives a reasonable basis for determining a person’s identity.

• PHI is created or received by a health care organization.

• Protecting a patient’s PHI is everyone’s responsibility.
Protecting a Patient’s Privacy

- Treat all information as if it were about you or your family.

- Do not discuss confidential patient information in elevators, hallways, cafeteria, restrooms, or other public places, etc.

- Shred documents and disks with PHI before discarding.

- Do not allow unauthorized visitors or patients in staff areas, dictating rooms, chart storage areas, etc.

- Do not discuss patient information with your family, friends, or people in your facility who are not directly involved in the patient's treatment, payment, or operations.

- Do not share your passwords with anyone.

- Set an idle time out on your local workstation.

- Always Log off of your computer when you leave your work area.
Protecting a Patient’s Privacy (cont.)

• Do not leave charts, schedules, or open documents on computer screens that may contain patient information in plain view.

• Conduct telephone conversations or dictation regarding confidential patient information in a discreet manner.

• Access only the information you are officially authorized to access.

Protecting a Patient’s Privacy (cont.)

- Each of us only has authorization to access PHI based on a *need to know basis* for the purpose of fulfilling our *job* responsibilities. Unfortunately, some take advantage of various sources of PHI to satisfy curiosity or other motives instead.

- LSUHSC-NO faculty, staff and students may find themselves working and/or training in facilities that use electronic health record systems that are shared by multiple, independent health care providers. An example of such a system is the PELICAN electronic health record. In such cases, an individual must be granted permission to access the electronic record in writing by the facility that owns the record, in addition to having a job related need to view the information before accessing the electronic record.
Protecting a Patient’s Privacy (cont.)

• No matter why an employee or physician accesses PHI, if there is not a job specific reason to do so, the access is prohibited by hospital policy, LSU policy, and HIPAA regulations!
  - This includes access to family members’ information, including spouses, parents, adult children, siblings, significant others, coworkers, etc.

Any such unauthorized access would be a direct violation of HIPAA regulations, and expose the person who violated them not only to disciplinary action, but also to possible legal action.
Where Can I find The Privacy Policies and Procedures?

The HIPAA Privacy Policies and Procedures are contained in Chancellor’s Memorandum 53 available at:

http://www.lsuhsc.edu/administration/cm/cm-53/
What is a Breach?

• A breach of PHI is the unauthorized access, use, or disclosure of PHI that compromises the security of that information.
What Happens if there is a BREACH of PHI?

• It should be reported immediately to:
  – the Compliance/Privacy Officer in the Office of Compliance Programs at LSUHSC-NO.
  – the appropriate official at the institution where the breach occurred if other than LSUHSC-NO.

• Compliance will conduct a risk assessment to determine if the breach must be reported to the patient and the U.S. Department of Health and Human Services.
Things to Remember about Breaches....

• The Breach Notification Rule establishes notification requirements for the Breach of unsecured PHI.
  - (PHI that is unencrypted.)
• Breaches Happen!!
• Breaches can be deliberate or accidental.
• You can report them anonymously.
• Timely notification of any known Breach is CRITICAL as we only have 60 days from the discovery of the Breach to take the necessary action required by the Breach Notification Rule.
• If you are unsure whether or not an incident is a breach, call the Compliance Office.
Some Examples of a Breach of PHI include, but are not limited to:

- PHI from discarded paper documents, computer hard drives, flash drives, backup tapes and optical disks.
- PHI included in emails sent to the wrong recipient or PHI inappropriately attached to an email.
- PHI stolen and sold for monetary gain
- PHI obtained and disclosed by hackers.
- PHI contained in lost or stolen paper documents, laptops, flash drives, backup tapes or optical disks.
- PHI that is disclosed due to the actions of a computer virus.
- PHI inappropriately posted or to which access is provided on a web server.
Privacy Complaints

• If anyone suspects or knows of mishandling or misuse of patient PHI, a complaint can be made to:
  
  – The LSUHSC-NO Privacy Officer
  
  – The Office of Compliance Programs
  
  – The Office of Civil Rights of Department Health and Human Services
  
  – The appropriate Privacy Officer at the institution if other than LSUHSC-NO
How to Report a HIPAA Violation

• Contact the LSUHSC-NO Privacy Officer or the Office of Compliance Programs via:
  - Telephone at:
    - Office: (504) 568-5135
    - Confidential reporting hotline: (504) 568-2347 or,
  - E-mail at: nocompliance@lsuhsc.edu

• Contact the Privacy Officer or the Compliance department at the LSUHCSD hospital/facility where you work via:
  – Telephone at:
    - HCSD Confidential reporting hotline- (866)-431-4571
Penalties for HIPAA Violations

- **Tier A** - violations that are accidental not intentional-fines of $100 per violation up to $25,000 for violations of an identical type per calendar year.

- **Tier B** - violations due to reasonable cause and not willful neglect- fines of $1000 per violation up to $50,000 for violations of an identical type per calendar year.

- **Tier C** - violations that the hospital corrected, but were due to willful neglect of the policies/procedures-fines $10,000 per violation up to $250,000 for violations of an identical type per calendar year.

- **Tier D** - violations due to willful neglect that the hospital did not correct-fines $50,000 per violation up to $1.5 million for violations of an identical type per calendar year.
Additional Penalties

• Loss of your job or student status.

• Individuals and health care providers (hospitals, etc.) can also face civil and criminal prosecution, depending on the facts of the case.
As a Recap…

- HIPAA provides for the rights of patients in relation to their Protected Health information. It also provides for the privacy and security of that information.

- It is everyone’s responsibility to protect PHI.

- Violations of any of the HIPAA regulations may result in fines from the federal government. Violations of HIPAA privacy regulations can also include civil and even criminal penalties.

- Report breaches of PHI to Compliance immediately.

- If you are found to be deliberately accessing PHI for reasons other than related to performing your job, you will face disciplinary action, up to and including termination your employment or student status.

- Be familiar with the HIPAA Privacy policies wherever you work as they differ from institution to institution.
Resources

• To view HCSD’s HIPAA Privacy Policies ‘7500-HIPAA Policies’, click here.

• To view HCSD’s Compliance Policies ‘8500-Compliance Policies’, click here.

• To view LSUHSC-N.O’.s HIPAA Policies ‘CM 53 HIPAA Policies’, click here.

• To view LSU-HCSD’s webpage, click here.

• To view LSUHSC-NO’s webpage, click here.
Any Questions?
We Are Here to Help!

Office of Compliance Programs OCP
433 Bolivar St.
Suite 807
New Orleans, LA. 70112
504-568-5135
Email nocompliance@lsuhsc.edu