HIPAA Privacy

The Office of Compliance Programs

INTEGRITY • TRUST • PRIVACY • ACCOUNTABILITY

Revised November 13, 2015
The Health Insurance Portability & Accountability Act (HIPAA) requires that the University train all workforce members (faculty, staff, residents, students, volunteers and contractors) 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 defines basic terms and lists basic principles that all LSUHSC-NO faculty, staff, residents and students must understand and follow.
Important HIPAA Privacy Terms

• **Privacy**: is the right of an individual to be informed of and provide input on uses and disclosures of his/her individual personal or health information.

• **Use**: means the sharing, utilization, or examination of **Protected Health Information (PHI)** within or by employees or students of LSUHSC-NO.

• **Disclosure**: means the release, transfer, or provision of access to PHI outside LSUHSC-NO.
• **Authorization**: the mechanism for obtaining permission from a patient for the use and disclosure of their personal health information to an outside agency that does not qualify under one of the exceptions in the regulations.

• **Minimum Necessary**: limits the use, disclosures, and the requests for PHI to the minimum necessary to accomplish the specific purpose of the task at hand.

• **Breach**: is the unauthorized access, use, or disclosure of PHI that compromises the security or privacy of that information.
This Training Program Will Help YOU Understand...

• **What**……is HIPAA?

• **Who**……has to follow the HIPAA law?

• **How**……does HIPAA affect you and your job?

• **Why**……is HIPAA important?

• **Where**…can you get help with HIPAA?
BEFORE HIPAA

In 1972, Democratic presidential nominee, George McGovern selected Senator Thomas Eagleton, (D-MO) as his vice-presidential running mate. Shortly thereafter, despite a long established principle of doctor-patient confidentiality, information about Senator Eagleton’s treatment for depression, including electro-convulsive therapy, was released to the press.

As a result of the outcry about someone who had undergone psychiatric therapy being “a heartbeat away from the presidency”, Eagleton withdrew from the race.

No one was ever prosecuted for breaching Senator Eagleton’s medical information.
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.
An Overview of the Law

HIPAA
Health Insurance and Portability Act of 1996

Title I
Portability

Title II
Administrative Simplification

Title III
Medical Savings Accounts

Title IV
Group Health Plan Provisions

Title V
Revenue Offset Provision

PRIVACY
Use and Disclosure of PHI

Individual Rights

Administrative Requirements

EDI
Transactions

SECURITY
Administrative Procedures

Physical Safeguards

Technical Security Services

Technical Security Mechanisms
HIPAA is the FLOOR

- The HIPAA Privacy regulations set the **minimum standards** for protecting the *privacy* of the Protected Health Information (PHI) of patients, and do not supersede any state, local rules or regulations, or standards that are more stringent.

- It is important to familiarize yourself with any state and/or local laws and regulations that may be more stringent than HIPAA.
Training Methods Offered at LSUHSC-NO

• Online Training (KDS)

• Presentation/Classroom training

• Informational packets (Self-Study) for users who do not have network accounts
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.
Who Is Impacted?

• The organizations covered by HIPAA are defined as “covered entities.”

• A “covered entity” can be any of the following:
  – Health care providers
  – Health plans
  – Health care clearinghouses

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

• This means that the university must abide by the requirements of the HIPAA Privacy Rule.
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
- All elements of Dates (e.g. Date of birth, Date of admission, Date of discharge, Date of appointment, Date of encounter, etc.
- 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.

Click [here](#) to view LSUHSC-NO’s De-Identification Policy
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
Use and Disclosure of PHI

- LSUHSC-NO faculty, staff and students may not use or disclose PHI without a patient’s written authorization unless the use or disclosure qualifies for one of the exceptions in the HIPAA regulations.
Common Disclosures of PHI Allowed without a HIPAA Authorization form are:

- to the *Individual*.
- for *Treatment*, *Payment*, and *Operations* (TPO).
- for *Other Activities*, including but not limited to:
  - Teaching
  - Medical Staff activities
  - Business and Management Operations
  - Disclosures required by Law
  - Public Health and other Governmental reporting

Click [here to view](#) the list of Common PHI Disclosures made without a written authorization.
Treatment, Payment, and Health Care Operations (TPO) are Defined as:

- **Treatment**: includes various activities related to patient care. Some examples include:
  - A primary care provider may send a copy of an individual’s medical record to a specialist who needs the information to treat the patient.
  - A hospital may send a patient’s health care instructions to a nursing home to which the patient is transferred.
  - Two health care providers discussing a patient’s condition to develop a treatment plan.

- **Payment**: includes activities related to obtaining payment for health care. Some examples include:
  - A physician may send an individual’s health plan coverage information to a laboratory who needs the information to bill for services.
  - A hospital emergency department may give a patient’s payment information to an ambulance provider to bill for its treatment.
• **Health Care Operations**: generally means the business operations of health care providers. Some Examples include:
  – Contacting of health care providers or patients with information about treatment alternatives.
  – Case management and care coordination.
  – Clinical education.
  – Activities relating to improving public health or reducing health care cost.
  – Conducting quality assessment improvement activities including outcomes evaluations and development of clinical guidelines.
  – Protocol development.

Click [here](#) to view LSUHSC-NO’s Policy on Treatment, Payment and Healthcare Operations.
Use and Disclosure Exception:
De-identification

- Use and Disclosure restrictions do NOT apply to De-identified information.

- De-identified health information neither identifies nor provides a reasonable basis to identify an individual.

- Removal of ALL specific personal identifiers.

Click here to view LSUHSC-NO’s De-Identification Policy
What is a HIPAA Authorization Form?

• A HIPAA Authorization form, is a form, signed by the patient, which is required for disclosures of PHI to entities outside LSUHSC-NO.


• A HIPAA Authorization form is **REQUIRED** when a patient requests a copy of his or her PHI to be disclosed to a *third party* except in certain limited circumstances.

  To view the related Privacy Policy (Use or Disclosure of Protected Health Information That Require an Individual's Written Authorization), click here. Located in Chancellor’s Memorandum-53, “Privacy Policies and Procedures”, Section T.
Examples of when a HIPAA Authorization is *Required* include, but are not limited to:

- When a patient requests a copy of his or her PHI to be disclosed to an outside entity.
- Release of records to an attorney.
- Release of records to a family member when the patient is over 18.
- Release of patient information to a research study sponsor.

**WHEN IN DOUBT, CHECK IT OUT!!**

*If you are **NOT** sure if a HIPAA Authorization form is required, please contact the Compliance office or Privacy official at the facility where you work.*
Invalid Authorizations

• **An authorization is considered invalid if the document has any of the following defects:**
  - Expiration date has passed or the expiration event is known to have occurred.
  - The authorization is missing one or more core elements of a valid authorization.
  - The authorization is known to have been revoked.
  - The authorization violates a privacy rule standard on conditioning of compound authorizations.
  - Any information recorded on the authorization is known to be false.
Invalid Authorizations (cont.)

- HIPAA Privacy regulations require very specific language be included in authorization documents. For that reason, only the HIPAA authorization forms available on the LSUHSC-NO and HCSD policy web pages or the authorization forms approved by the health care facility where you are working may be used to obtain a patient’s authorization to use or disclose their PHI.

*Use of any other form will result in an Invalid Authorization and a Breach of PHI.*
Who Has Access to PHI?
The “Need to Know” Principles

• PHI should be shared with as few individuals as needed to ensure patient care and then only to the extent demanded by the individual’s role.

• The “Need to Know” Principles
  – Is the information needed for you to do your job?
  – How much do you need to know?
  – How much do other people need to know?
  – The key is to balance the privacy of health information against the need for the information.
How Does “Need to Know” Translate into HIPAA?

• HIPAA requires use of the *Minimum Necessary* concept:
  – Use only the minimum necessary amount of information needed to perform your job.
  – Disclose only the minimum necessary amount of information needed to fulfill a request.

  ➢ **Treatment** is an *EXCEPTION***!!

Never provide more information than what is needed!!

Click [here](#) to view LSUHC-N.O.’s Minimum Necessary Policy.
Minimum Necessary Rule

Exceptions

- The *Minimum Necessary* requirement does **NOT** apply in the following instances:
  - Disclosures to or requests by a health care entity for the purpose of *treating* the patient.
  - Uses or disclosures made to the individual who is the subject of the PHI.
  - Uses or disclosures made pursuant to a valid HIPAA authorization initiated by the individual.
  - Uses or disclosures that are required by law. (However, disclosures are limited by the law’s requirements.)
  - Uses or disclosures required for compliance under HIPAA, including compliance with the implementation specifications for conducting standard data transactions.
HIPAA Requires the University to:

1. Provide a copy of LSUHSC-NO’s Notice of Privacy Practices (NPP) brochure when a patient First Visits an LSUHSC-NO clinic that describes:
   - How the university can use and share his or her protected health information (PHI).
   - A patient’s privacy rights.

2. Ask the patient to *sign* a written acknowledgment that he/she received the *Notice of Privacy Practices*.

To view the designated form, click [here](#). Located in Chancellor’s Memorandum-53, “Privacy Policies and Procedures”, Section A, Attachment B.

3. Post the NPP at the location (ex. in the patient waiting room) and on the location’s website. (Contact the Office of Compliance Programs for NPP posters.)
Patient’s Rights

HIPAA Provides for specific Patient Rights, which include:

1. **Right** to inspect and copy their PHI;
2. **Right** to receive an electronic copy of their PHI if the PHI is already in an electronic format;
3. **Right** to request an Amendment to their PHI;
4. **Right** to receive Confidential Communications at an Alternative address or phone;
5. **Right** to request Restrictions on certain uses and disclosures;
6. **Right** to request an Accounting of Disclosures of their PHI;
7. **Right** to opt-out of a Facility Directory;
8. **Right** to make a complaint about a suspected privacy breach.
Right to Access

• Patient’s have the Right to Access and Copy their PHI.

To view the related Privacy Policy, click here. Located in Chancellor’s Memorandum-53, “Privacy Policies and Procedures”, Section J.

• A “Patient’s Request for Access to and to Obtain a copy of their PHI” form MUST be filled out if a patient requests to Access or Obtain a copy of their PHI.

Right to Request Amendment and Restrict Disclosure

If a patient requests an *Amendment* or *Restriction* of the PHI contained in their medical record, the health care provider must reference the corresponding HIPAA Privacy Policy contained in CM-53 AND contact the LSUHSC-NO Privacy Officer.

To view the related Privacy Policy, click [here](#). Located in Chancellor’s Memorandum-53, “Privacy Policies and Procedures”, Section I.

To view the related Privacy Policy, click [here](#). Located in Chancellor’s Memorandum-53, “Privacy Policies and Procedures”, Section K.
Right to Request Amendment and Restrict Disclosure (cont.)

• LSUHSC-NO must agree to the request of an individual to restrict disclosure of PHI about the individual to a health plan if:
  
  – The disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law, and,

  – The PHI pertains solely to a health care item or service for which the individual or person other than the health plan on behalf of the individual has paid LSUHSC-NO in full.
Right to an Accounting of Disclosures

A patient has the right to receive an accounting of certain types of disclosures of Protected Health Information made by LSUHSC-NO for up to six (6) years prior to the date on which the accounting is requested. This includes any disclosures for reasons other than treatment, payment or operations.

To view the related Privacy Policy, click here. Located in Chancellor’s Memorandum-53, “Privacy Policies and Procedures”, Section C.
Where Can I find The Privacy Policies and Procedures?

- At LSHSC-NO, the HIPAA Privacy Policies and Procedures are contained in Chancellor’s Memorandum 53 available at: http://www.lsuhsc.edu/administration/cm/cm-53/
How Does HIPAA Privacy Affect Providers?
LSUHSC-NO Providers and HIPAA

- LSUHSC-NO has a commitment to the privacy of the patient’s health information, in both medical and billing records.

- The privacy policies and procedures affect the tasks a provider performs, including aspects of physical security of PHI and the minimum necessary standard.
Protecting a Patient’s PHI is Your Responsibility

• PHI can be compromised in many different ways. It is your responsibility to protect PHI in all situations so that you do not expose a patient’s PHI.

• A patient’s PHI can be breached in any of the following ways. (This is not an inclusive list, but rather examples of various risks to PHI.)
  – 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.
Protecting a Patient’s PHI is **Your Responsibility**

- 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, etc.
Simple acts can have serious consequences. Whenever you share electronic or paper PHI with someone, you must make sure that the right information is going to the right recipient!

### Protecting PHI: Misdirected Information

<table>
<thead>
<tr>
<th>Types of Misdirected Information</th>
<th>How To Protect PHI</th>
</tr>
</thead>
</table>
| **Faxes**                        | • Verify that you have the correct information before you send it.  
                                 | • Verify that the fax number you are using is current and correct. 
                                 | • Always use a fax cover sheet.  
                                 | • If it is a frequently used number, consider pre-programmed numbers (once they are verified).  
                                 | • Call to make sure the intended recipient received the fax.  
                                 | • Only send the required information.  
                                 | • Make sure to update pre-programmed numbers on a regular basis. |
| **Mailings**                     | • Only send the minimum information necessary.  
                                 | • Verify that the right information is being sent to the right person. |
| **Information Handed Directly to the Patients** | • Verify that you have the correct information going to the correct recipient.  
                                 | • Use two identifiers to ensure you have the right patient.  
                                 | • Thumb through the papers being sent to make sure one patient's information is not "stuck" to another. |
Protecting PHI
Unsecured Paper

• Loose pieces of paper being transported from one place to another should be secured in an envelope or folder to prevent them from slipping out.
• Papers with PHI should not be left lying around in unsecured areas.
• Papers with PHI should not be brought outside the hospital unless they are being transported from one place of business to another in a secure manner.
• Always dispose of paper PHI in the shred bin.
• If you use a shredder in your office, it must be cross cut shredder (think of an "X" shape) to be HIPAA compliant.
• Don't bring paper with PHI home.
• If you have documents with PHI in your work area, make sure that they are placed face down or otherwise concealed when not in use.

• Make sure that any room that has medical records in it is always attended by an employee. If there is not an employee with the records, store the medical records in a locked room or cabinet.
• If medical records are transported from one location to another, ensure that they are secured, cannot be dropped during the transport, and are not left unattended in hallways, patient waiting areas, parking garage of the hospital etc.
• Be aware that written PHI can show up in places other than paper. For example, a view box with an x-ray can also show PHI since the patient's name is usually noted on the x-ray.
• Be cautious of printed patient information, billing sheets, lab reports, notebooks with handwritten notes, report sheets for notes about patients, etc. These are items that are often left unattended in areas that are accessible by patients. They are also items that are often accidentally dropped and found by others.
Protecting PHI
On Computers and Other Portable Devices

• Do not write your password down and place it around the computer for others to use or discover.
• Do not share your password with others.
• Do not download patient information onto jump drives or personal mobile devices that are not encrypted.
• Do not download patient information into folders that are not secured by LSU HCSD/HSC-NO Information Technology staff.
• If you have a laptop, do not store patient information on it unless it has been encrypted.
• Do not store PHI on personal laptops without expressed knowledge and permission of the healthcare institution.
• If you carry a mobile device that has access to patient PHI, it should be password protected.
• If possible, face your computer monitor away from public viewing, or use a privacy screen over the monitor.
• Do not leave screens that contain patient information if you are not actively working on the computer.
• Ideally, PHI should not be stored on thumb drives or other removable storage devices since they are easily lost or stolen unless the device(s) are encrypted.
• All electronic devices should be secured at all times. Lost or stolen electronic devices account for the majority of reported HIPAA breaches in the United States.
• The best defense is to not store PHI on such devices unless the device(s) is encrypted.
Protecting PHI

Verbal

- A great deal of PHI is discussed in the course of business at LSU LSUHSC-NO.
- When discussing any patient information, take precautions to make sure that the PHI has as little exposure as possible.
- For example:
  - Don't discuss patient cases in the hallways, elevators, waiting areas, and other public areas of the hospital where other patients or visitors can hear you.
  - Be aware of the VOLUME of your voice. Speak in softer tones, especially in semi-private rooms and other similar areas.
  - Be sure to ask the patient if it is okay before discussing sensitive information in front of anyone that is present in their room (e.g. family members, friends, visitors, other patients, housekeeping, etc.).
  - Close exam room doors or pull curtains in patient rooms when patients are being examined/treated.
  - Remember, curtains do not sound proof a room, so use caution about voice tone and information shared in such areas.
  - Try not to use patient identifying information when using cell phones to call into the hospital to discuss a case.
Protecting PHI

Proper Disposal

• Special care should be taken anytime any item/device that contains PHI is discarded.
  - Check with Information Security for the disposal of computers and portable storage devices such as thumb drives.
  - Verify that processes are in place to ensure PHI is wiped from the hard drive memory of copy machines and biomedical equipment (the vendor may be contracted to do this for you).
  - PHI may be found on items such as arm bands, prescription bottles, and IV bags. Make sure that none of these are discarded in the regular trash. IV bags should have pull away labels that once torn from the bag can be disposed of in the shred bin.
Protecting PHI
Proper Disposal (cont.)

• Paper PHI should be disposed of in shred bins. A few points about shred bins:
  - Make sure that any shred bin that you use is locked.
  - Keys should not be left in the shred bin.
  - If the shred bin is so full that you can pull papers out of it, immediately notify the department that is responsible for emptying the shred bin.
  - For those emptying the shred bin, make sure that any bags of paper are in a secure, locked location while awaiting pick up from the shredding company.
  - When working with disposal companies, verify the identity of the disposal company employee before turning over any PHI.
  - **REMEMBER**: The paper in the shred bin has patient PHI, and is just as important to secure as a patient's medical record.
Protecting PHI

Email and Secure Folders

• If a large amount of patient information needs to be shared, you can use secure computer folders or links. Contact your IT department for more information on this option.

• To share large files securely with outside entities, use LSU Health File$ (File-Sharing Solution).

• If you do use folders in Public Folders, or on certain drives on your local workstation, remember that identifiable patient information should not be stored there unless the folder has sufficient security set up so that only those who need to access the information can.
Protecting PHI
Pictures of Patients

• Check the policy at the institution you are working regarding photographing patients to fully understand what is or is not acceptable when it comes to taking pictures of patients.

• In many cases, the patient must provide written consent before a picture may be taken.
Protecting PHI

 Stranger Danger

• Hospitals and health care facilities are bustling places, with people moving quickly about everywhere.
• In such an environment, it would be easy for someone to go unnoticed while attempting to steal PHI.
• Should anyone come to you that you are not familiar with asking for access to PHI, or to restricted areas within the hospital or health care facility where you work, it is important to verify their identity.
• If you have not been notified by your supervisor that there is someone who will need access to an area or information, verify with your supervisor, Security, Hospital Administrator or the Compliance department at the hospital or health care facility where you are working before granting them access. This is true, even if the person appears to have proper identification.
Protecting PHI

Accessing Records

• 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 PHI

Accessing Records (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 LSU policy, and the HIPAA regulations!
  - This includes access to family member’s 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.
If you are the caregiver of a family member or friend and need access to PHI, then a release of information form signed by the patient should be given to medical records so that you can be given information on the patient by medical records.
Protecting PHI

Possession of Records

• What identified patient information do you have in your possession?
• To whom does this information belong?
  – The patient
  – The hospital or other healthcare institution
• Do you have right to have that information in your possession?
  – If you are treating the patient.
  – If you have written authorization from the patient or the hospital to possess this information.
• When should patient information in your possession be destroyed, de-identified or turned over to the healthcare institution?
  – When the treatment relationship ends.
    • Change in rotation
    • Change in employment
  – In certain instances, at the end of the research study, if these are research records. (see CM-53 Section S)
LSUHSC-NO recognizes that social networking websites and applications (i.e. Facebook, Twitter, and YouTube, etc.) are an important and timely means of communication.

However, LSUHSC-NO faculty, staff, residents, and students who use these websites and applications, must be aware that the protections of patient information required by HIPAA apply to social media as well.

While it is popular to share events that happen at work or school on social media outlets in the form of posts, pictures, and/or videos, employees and students of LSUHSC-NO must be vigilant to ensure that patient information is NOT compromised in the process.
Protecting PHI
Use of Social Media (cont.)

• Removal of the individual’s name **DOES NOT** by itself constitute proper de-identification of protected health information.

• You must also ensure that **All** personal identifiers are removed (e.g. age, gender, race, before and after photographs and/or tattoos), and are **NOT** inadvertently included in **any** social media.
Specific Social Media Institutional Policies

• All LSUHSC-NO faculty, staff, residents and students at private hospitals need to be familiar with the institutions social media policy.

• In the absence of a policy, care must be exercised when posting information for educational purposes to ensure that any information posted combined with other readily available information (ex. address, telephone number, etc.) will NOT result in the identification of the patient.

• Some institutions include very specific restrictions in their policies. For example, LSU HCSD System hospital requires that any pictures taken of patients be done with a hospital secured camera and not personal cell or smartphones.
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! (Yes, it can happen to you!)

• 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.
Role of the Privacy Officer

- Responds to HIPAA privacy complaints
- Implements privacy policies and procedures
- Conducts educational programs
- Reviews LSUHSC-NO’s privacy program
- Investigates violations of LSUHSC-NO’s privacy policies
- Is available to answer any privacy questions or concerns
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
  – Office of Compliance Programs
  – Office of Civil Rights of Department Health and Human Services
  – appropriate Privacy or Compliance official 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 hospital/facility where you work.
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 in all formats.

- Violations of any of the HIPAA regulations may result in fines from the federal government. 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 can face disciplinary action, up to and including termination and/or expulsion.

- Be familiar with the HIPAA Privacy policies wherever you work as they differ from institution to institution.
Any Questions? Contact Us...

Office of Compliance Programs
433 Bolivar St.
Suite 807
New Orleans, LA. 70112
568-5135