

Health Insurance Portability
and
Accountability Act of 1996
(HIPAA)

LSUHSC-New Orleans Self-Study
Guide for HIPAA Privacy Regulations

What is HIPAA?

In 1996, the U. S. Congress passed the Health Insurance Portability and Accountability Act. This law:

- allows for the portability of insurance
- guarantees issuance of health insurance for small groups
- provides for mental health parity
- mandates privacy standards for patient confidentiality
- standardizes electronic transactions
- requires data security

What are the most significant Privacy Rule requirements?

- 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 employee 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

What is a Notice of Privacy Practices?

The Notice of Privacy Practices (NPP) describes how the patient's medical information may be used or disclosed and how the patient can get access to that information.

The NPP must be given to each patient and must be posted at each provider site.

LSUHSC-N.O. must make a good faith attempt to obtain a written acknowledgement that the patient has received the Notice of Privacy Practices, or document the reason why an acknowledgement was not obtained.

What is Protected Health Information?

Protected Health Information is **individually identifiable health information**.

Individually identifiable health information means identifiers of the individual or of relatives, employers, or household members of the individual, specifically, any one or combination of the following:

- names
- addresses
- all elements of dates (*e.g.* birthdate, date of service, date of death, etc.)

- telephone numbers
- fax numbers
- email addresses
- Social Security numbers
- medical record numbers
- health plan beneficiary number or member number.
- account numbers
- certificate or license numbers
- vehicle identification numbers or license numbers
- device identifiers and serial numbers (*e.g.* medical device numbers)
- Universal Resource Locators (URL)
- Internet Protocol Addresses (IP)
- biometric identifiers, including voice and fingerprints
- full face photographic images or any other comparable image; or
- any other unique identifying number, characteristic, or code.

To help you identify PHI, remember these points:

- 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.

What is a Covered Entity?

A Covered Entity is a health care clearinghouse, health plan, or health care provider who transmits PHI electronically in connection with a covered transaction (*e.g.* billing, Medicare eligibility, etc.)

What is a Business Associate?

A Business Associate is often an outside vendor whom we have hired to do work for us that may involve the disclosure or exchange of PHI. The federal Privacy Rule at 160.103 defines a business associate as someone who:

- will use protected health information on behalf of the covered entity, or
- creates or obtains information on behalf of the covered entity, in the following manner:
 - uses or discloses PHI on behalf of the covered entity for functions such as claims processing, claims administration, data analysis, processing or administration, utilization review, quality review, quality assurance, billing, benefit management, practice management and re-pricing, (*e.g.* some software vendors, etc.)

- or**
- provides specific services to the covered entity and those services involve the disclosure of PHI by the covered entity to the business associate, in the following manner:
 - provides legal, actuarial, or financial services to or for the covered entity which requires the covered entity to disclose PHI to the business associate. (*e.g.* law firms, etc.)

Not all of our outside vendors will be business associates for purposes of the privacy rule. **The key to remember is *use or disclosure of PHI in our business arrangement with that outside vendor.*** For example, we may have a contract or agreement with the U.S. Postal Service to provide our postage meters, but the Post Office does not use or disclose PHI on our behalf.

An exception to the business associate standard is disclosure of PHI by a covered entity to a health care provider for treatment of a patient. For example, a physician is not required to have a business associate contract with a laboratory as a condition of disclosing PHI for referral of that patient for tests.

Please check with the Privacy Officer or the Compliance Officer if you need clarification.

What does Use and Disclosure of PHI mean?

Use of PHI takes place **within the covered entity** that maintains the PHI. According to the Privacy Rule §164.501, **use includes sharing, employment, application, utilization, examination or analysis** of such information. When PHI is shared between members of the LSUHSC-NO workforce, this constitutes use.

Disclosure of PHI takes place **outside of the entity** holding the PHI. According to the Privacy Rule §164.501, **disclosure includes the release, transfer, provision of access to or divulging in any other manner** of such information. When PHI is shared with individuals or entities outside of the LSUHSC-NO workforce, this constitutes disclosure.

Why do I need to know this information?

All reasonable efforts must be made not to disclose more than the **minimum necessary** information needed to accomplish the intended purpose. Staff access to PHI is based on specific job duties and roles. The **minimum necessary** standard does not apply to disclosures for treatment purposes.

What are some things I can do to protect our patients' 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.

- 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 leave charts, schedules, or open documents on computer screens that may contain patient information in plain view
- Shred documents and disks with PHI before discarding
- Access only those systems you are officially authorized to access
- Do not share your passwords with anyone
- Set a idle time out or log off on your computer
- Access only information you need to do your job
- Do not allow unauthorized visitors or patients in staff areas, dictating rooms, chart storage areas, etc.
- Conduct telephone conversations or dictation regarding confidential patient information in your area in a discreet manner

What are some examples of disclosures of PHI that *require* a written authorization from the patient?

- To release psychotherapy notes
- For marketing or fundraising purposes
- To release health information to an employer as part of a background check
- To release information to an insurance company at the patient's request for underwriting or eligibility for benefits (e.g. life or disability insurance)
- To release the results of a fitness test to a prospective employer
- For certain research purposes

What disclosures of PHI are permitted, *without* written authorization from the patient?

- To an individual, when requested under, and as required by the access or accounting requirement of the HIPAA Privacy Regulations
- When required by the Secretary of the Department of Health and Human Services to investigate or determine LSUHSC-NO's compliance with the HIPAA Privacy Regulations

What uses and disclosures of PHI are permitted, *without* a written authorization from the patient?

- To the patient
- For treatment reasons to obtain payment for health care business operations
- Pursuant to an oral agreement with the patient to make such disclosures to a relative or friend or other about an individual whom LSUHSC-NO reasonably believes to be a victim of abuse, neglect or domestic violence

- In judicial or administrative proceedings
- To a law enforcement official for the purpose of law enforcement
- In response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person
- In response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime
- In response to a law enforcement official's request for information about an individual who has died as a possible result of criminal conduct
- To the Coroner
- To Funeral Directors
- To organ procurement organizations
- As authorized by and to the extent necessary to comply with Louisiana Workers' Compensation statutes.

If LSUHSC-NO, in good faith, believes the use or disclosure a) is necessary to prevent or lessen a serious and imminent threat to the health safety of a person or the public; b) is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or c) is necessary for law enforcement

What rights do patients have under the HIPAA Privacy Regulations?

- To inspect and copy their PHI
- To request an amendment to their PHI
- To receive confidential communications (e.g., at an alternative address or phone)
- To request restrictions on certain uses and disclosures
- To request an accounting of disclosures

Where can I find LSUHSC-NO's Privacy Policies and Procedures?

Please see the Summary of Privacy Policies and Procedures attached to this email. The full text of the Privacy Policies and Procedures will be posted on the LSUHSC-NO website in the near future.

What are the penalties for disclosure of PHI?

There are no penalties for incidental disclosures of PHI. However, **negligent and/or intentional** disclosures may subject LSUHSC-NO to civil money fines of \$100 per violation/day, up to \$25,000/year for all violations of an identical type. Negligent or intentional disclosures of PHI may subject LSUHSC-NO to exclusion from the Medicare and/or Medicaid programs. Additionally, certain public officials may be subject to fines and/or imprisonment for violation of any HIPAA rule as follows:

- knowingly—\$50,000 and/or one year jail (*e.g.* using patient data for your child's school project)

- false pretenses—\$100,000 and/or five years jail (*e.g.* accessing patient information for personal use)
- for profit, gain, or harm—\$250,000 and/or 10 years (*e.g.* selling patient information to the media)

Incidental PHI disclosures can occur when we are not conscious of our environment or those around us. For example, we may accidentally talk about a member in the lunchroom or on the elevator when we think we cannot be overheard. Negligent PHI disclosures occur when we “should have known better” than to be talking about a member, such as at a restaurant or on a cell phone while waiting in an airport or while using a laptop computer at a conference. Negligent disclosures can become intentional disclosures if a pattern is established.

Both negligent and intentional PHI disclosures can subject LSUHSC-NO employees to disciplinary policies, up to and including termination of employment. While legal penalties and fines for HIPAA violations do not directly affect most employees, we are required to have and enforce disciplinary policies on this subject.

Who is our Privacy Officer?

Privacy Officer: Leigh Lamonica , Esq.

Where do I call, if I have any questions regarding HIPAA or the Privacy Policies and Procedures?

| Office of Compliance Programs
433 Bolivar St.
Suite 811
New Orleans, LA. 70112

Where do employees, patients, or the general public report complaints about HIPAA privacy violations?

Compliance Hotline
(504) 568-2347
or
nocompliancehotline@lsuhsc.edu

LOUISIANA STATE UNIVERSITY SYSTEM

SUMMARY OF HIPAA POLICIES

These policies apply to all LSU System health care facilities and providers, including, but not limited to, hospitals, physician clinics, labs, etc., which are referred to in this policy as LSU System facilities.

The following policies may be viewed in their entirety in the individual LSU System facility HIPAA manual or on the website of the individual LSU System campus.

1. Notice of Privacy Practices Policy. All LSU System health care facilities and providers must provide an adequate Notice of Privacy Practices to patients. LSU System facilities must also inform the patients of their rights with respect to Protected Health Information and LSU System's legal duties. The LSU System facilities must obtain the patient's acknowledgement of receipt of the notice.
2. Privacy Official and Complaint Contact. Each LSU System-affiliate must designate a Privacy Official to oversee and implement each LSU System facility's privacy policies and procedures and work to ensure LSU System facility's compliance with the requirements of the HIPAA Privacy Regulations. The Patient Advocate may also be responsible for receiving complaints about matters of Patient Privacy.
3. Accounting of Disclosures of Protected Health Information. All LSU System health care facilities and providers must provide patients with a right to request and receive an accounting of the uses and disclosures of their Protected Health Information by any LSU System health care facility or health care provider.
4. Minimum Necessary Uses and Disclosures of Protected Health Information. The LSU System is committed to ensuring the privacy and confidentiality of protected health information that is used or disclosed by the LSU System facility's workforce during the course of their work while ensuring that the LSU System facility has access to the information that is required to accomplish its mission, goals and objectives. The LSU System facility will make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request as required under the Privacy regulation and other applicable federal, state and local laws and regulations.
5. Whistleblower/Non-Retaliation. It is the responsibility of all LSU System facility employees to report perceived misconduct, including actual or potential violations of state and federal laws and regulations, internal policies and procedures, Permanent Memoranda of the LSU System, and Chancellors' Memoranda.

The LSU System facility will maintain an "open-door policy" at all levels of management to encourage employees to report problems and concerns.

The LSU System facility will follow all necessary procedures to protect against any retaliation toward any employee, faculty, staff, or other individual, including a patient of its facilities, for exercising their rights or participating in any process pursuant to internal policies, applicable law, or regulation.

Any employee who commits or condones any form of retaliation will be subject to the LSU System facility Human Resources' policies on discipline up to, and including, termination.

6. Mitigation After Improper Protected Health Information Use or Disclosure. The LSU System facility has a duty to ensure the proper use and/or disclosure of PHI. To the extent practicable, the LSU facility will mitigate (lessen or alleviate) any harmful effect that becomes known to the LSU System facility as a result of a use or disclosure of PHI in violation of the LSU System facility's policies and procedures or applicable law.
7. Training and Education Requirements For Members of the LSU System Facility Workforce. All LSU System health care facilities and providers must provide members of its workforce with education and training on the LSU System policies and procedures on Health Information Privacy and the HIPAA Privacy Regulations.
8. Documentation Requirements. All LSU System health care facilities and providers will have to adhere to all documentation requirements as stated in 45 C.F.R. 164.530(j) and other applicable federal, state, and/or local laws and regulations.
9. Patient's Request For Restriction of Uses and Disclosures of Their Protected Health Information. All LSU System health care facilities and providers must provide patients with a right to request a restriction of the uses and disclosures of their Protected Health Information that is contained in a Designated Record Set. The HIPAA Privacy Regulations require health care providers to provide patients with a right of access to inspect and obtain a copy of their Protected Health Information.
10. Patient's Right of Access to and Obtain a Copy of their Protected Health Information. All LSU System health care facilities and providers must provide patients with a right of access to inspect and obtain a copy of their Protected Health Information about the individual in a Designated Record Set of any LSU System health care facility or health care provider.
11. Patient's Right to Request an Amendment to their Protected Health Information. All LSU System health care facilities and providers must provide patients with a right to request an amendment as required by the HIPAA Privacy Regulations. A

patient's request for an amendment should be handled in accordance with this policy and any applicable federal or state laws or regulations.

12. Patient's Right to Request and to Receive Confidential Communications by Alternative Means or at Alternative Locations. All LSU System health care facilities and providers must provide patients with an opportunity to request and receive confidential communications by alternative means or at alternative locations of their Protected Health Information and must accommodate reasonable requests.
13. Safeguards. The Louisiana State University (LSU) System health care facilities and providers will have the appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information and to minimize the risk of unauthorized access, use, or disclosure as described herein and pursuant to 45 C.F.R. 164.530(c) and other applicable federal, state, and/or local laws and regulations.
14. Limited Data Set. To provide guidance to the health care facilities and providers affiliated with the LSU System in the following areas:
 - To outline the process for reviewing and responding to requests for limited data sets.
 - To provide guidance on how to create a limited data set.
 - Define requirements of a Data Use Agreement for use and disclosure of a limited data set.
15. De-Identification of Protected Health Information. All LSU System health care facilities and providers should comply with the applicable requirements of the HIPAA Privacy Regulations when de-identifying an individual's Protected Health Information.
16. Use and Disclosure of Protected Health Information for Payment, Treatment and Health Care Operations. All LSU System health care facilities and providers should follow the requirements of the HIPAA Privacy Regulations when using or disclosing Protected Health Information as outlined in this policy to carry out treatment, obtain payment for services, or to conduct certain health care operations.

For the purposes of this policy, workforce is defined as employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the facility, is under the direct control of such facility, whether or not they are paid by the facility. This includes full-time, part-time, or PRN staff, regularly scheduled contract workers, volunteers, students, and others defined by the health care facility.
17. Use and Disclosure of Protected Health Information for Facility Directory

- Purposes. All LSU System health care facilities and provide patients with the opportunity to agree to or prohibit the use or disclosure of their Protected Health Information in a facility's directory.
18. Use and Disclosure of Protected Health Information For Marketing Purposes. All LSU System health care facilities and providers must obtained an individual's signed authorization before using or disclosing the individual's Protected Health Information for marketing purposes as defined in this policy.
 19. Use and Disclosure of Protected Health Information for Research. All Louisiana State University Health Sciences health care components, facilities and providers, including, but not limited to health sciences schools, IRB's and/or Privacy Boards established there under hospitals, physician/faculty practices and clinics will provide guidance for the use and disclosure of protected health information (PHI), as described in the Health Insurance Portability and Accountability Act (HIPAA) of 1996, for research purposes including:
 - Instances where a written authorization is required before PHI may be used or disclosed;
 - Instances where written authorization of the patient is not required before PHI may be used or disclosed, but a review of the use or disclosure of PHI must be performed and approved by a the IRB; and
 - Instances where written authorization of the patient is not required before PHI may be used or disclosed, but the researcher must provide written assurances that the PHI will be protected.
 20. Use or Disclosure of Protected Health Information That Require and Individual's Written Authorization. All LSU System health care facilities and providers must obtain a patient's written authorization.
 21. Use and Disclosure of Protected Health Information to Persons Involved in the Patient's Care and For Notification Purposes. All LSU System-affiliated health care facilities and providers should provide a patient with an opportunity to agree to or object to the disclosure of their Protected Health Information to family members or other persons identified by the patient, or for notification purposes.
 22. Use and Disclosure of Protected Health Information to Business Associates. All LSU System health care facilities and providers must enter into a business associate contract with any Business Associates as provided in this policy.
 23. Use and Disclosure of Protected Health Information for Fundraising. All LSU health care facilities and providers may use or disclose an individual's Protected Health Information for fundraising purposes as described in this policy.
 24. Uses and Disclosures of PHI: General. All LSU health care facilities and providers must adhere to the general requirements of uses and disclosures of

Protected Health Information regarding patients.

25. Employee Conduct and Disciplinary Sanctions (LSUHSC-NO campus) Faculty, staff, and students will adhere to policies and procedures and state and federal law. Progressive discipline will be used so that performance may be corrected.

HIPAA PRIVACY ATTESTATION FORM

I hereby certify that I have received the LSUHSC-NO Self Study Basic Training Guide. I understand that I will be accountable for the information contained therein. I also understand that this acknowledgement will be maintained as a record of my participation in the HIPAA Privacy training program and may be reviewed by the federal government.

Print Name (Legal Name): _____

Signature _____

Date ___/___/___

Employee or Student (Please Circle One)

Department: _____

Department Telephone Number: _____

Please return this signed page to:

Office of Compliance Programs
c/o Kelly Guth
433 Bolivar
Suite 811
New Orleans, LA 70112