LOUISIANA STATE UNIVERSITY
HEALTH CARE SERVICES DIVISION
BATON ROUGE, LA

POLICY NUMBER: 7521-24

CATEGORY: HIPAA Policies

CONTENT: Administrative, Technical and Physical Safeguards

APPLICABILITY: This policy is applicable to Health Care Services Division Administration and Lallie Kemp Medical Center to include employees, physician/practitioner practices, vendors, agencies, business associates and affiliates.

EFFECTIVE DATE:

Issued:	April 14, 2003
Revised:	July 25, 2013
Revised:	February 26, 2015
Revised:	February 29, 2016
Reviewed:	September 1, 2017
Reviewed:	September 9, 2019
Reviewed:	January 9, 2020
Reviewed:	January 13, 2023
Reviewed:	March 5, 2024

INQUIRIES TO: Health Care Services Division
Compliance Section
Post Office Box 91308
Baton Rouge, LA 70821-1308

Note: Approval signatures/titles are on the last page

LSU HEALTH CARE SERVICES DIVISION
ADMINISTRATIVE, TECHNICAL AND PHYSICAL SAFEGUARDS

I. POLICY STATEMENT

This policy will provide guidance to Health Care Services Division health care facilities and providers, acting as a Covered Entity under the HIPAA Privacy Rule, to ensure the appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI) and to minimize the risk of unauthorized access, use, or disclosure.

Note: Any reference to Health Care Services Division (HCSD) also applies and pertains to Lallie Kemp Medical Center.

II. IMPLEMENTATION

This policy and subsequent revisions to the policy shall become effective upon approval and signature of the HCSD Chief Executive Officer (CEO) or Designee.

III. RESPONSIBILITY

A. General

HCSD healthcare facilities and providers will take reasonable steps to safeguard information from any intentional or unintentional use or disclosure that is in violation of the privacy policies. Information to be safeguarded may be in any medium, including paper, electronic, oral, and visual representations of confidential information.

It is the responsibility of all workforce members to protect patient health information by using applicable administrative, physical, and technical safeguards. Department managers shall put in place reasonable safeguards to ensure that their department is regularly reviewed for compliance with such safeguards, and that any vulnerabilities are immediately addressed. Documentation reflecting any finding, corrective action plan as well as result of the same shall be the responsibility of the department manager.

B. Safeguarding confidential information – Administrative Safeguards

Administrative safeguards include administrative actions and policies and procedures, to manage the conduct of the HCSD's workforce in relation to the

protection of confidential information. The policies and procedures implemented are designed to prevent, detect, contain and correct any security violations.

Administrative safeguards that have been implemented within the HCSD include, but are not limited to:

1. New hire and annual HIPAA privacy and security training for workforce members, as well as ongoing HIPAA security education.
2. Regular assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic PHI.
3. Institution of management techniques to identify potential areas of vulnerability with internal processes and address the same in risk assessments.
4. Provision of a HIPAA Security Official who is responsible for the development and implementation of policies and procedures to protect PHI.
5. Sanctions for those workforce members who choose to violate HCSD's safeguard policies for PHI.
6. Regular review of records of information system activity, such as audit logs, access reports, and security incident tracking reports.
7. Provision of controlled, systematic access to PHI as the workforce member's role warrants.
8. Termination of access to PHI when the employment or contract of a workforce member ends.
9. Procedures for creating, changing, and safeguarding passwords to applications and data bases containing ePHI.
10. Provision of a systematic response to identified suspected or known security incidents, including mitigating, to the extent practicable, the harmful effects of such incidents.
11. Institution of a contingency plan should a natural disaster strike.
12. Provision of a business continuity and contingency plan in the event of a disruption or security incident.
13. Institution of Business Associate Agreements, Data Use Agreements, and other assurance documents to ensure the protection of PHI when PHI is accessed, used, disclosed, or transmitted by external affiliates.
14. Periodic assessment of the criticality of specific applications and data as it relates to business operations.
15. Policies and procedures for specific risk areas such as faxing PHI, disposing of PHI, and overall HIPAA Security protections, etc.
16. HIPAA internal reviews, such as HIPAA walk-throughs and department checklists to evaluate and improve the effectiveness of current safeguards.
17. Detailed HIPAA Privacy and HIPAA Security policies that outline the requirements of the federal and state regulations governing patient PHI.

C. Safeguarding confidential information – Physical Safeguards

Physical safeguards are physical measures, policies and procedures to protect a Covered Entity's electronic, paper and oral information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Physical safeguards that have been implemented within the HCSD include, but are not limited to:

1. Storage of paper medical records in locked areas, accessible only by authorized medical records personnel.
2. Access to electronic systems is role-based, managed by an authorization approval process, and guarded by passwords.
3. Locked and access controlled environments for HCSD's servers.
4. Data backup and storage of historical data.
5. The adoption of a facility security and facility contingency plan.
6. Strategic location of computer workstations with consideration of both staff needs as well as physical security.
7. Secured biomedical equipment.
8. Secure disposal of electronic media such as hard drives, USBs, etc.
9. Provision of privacy screens for monitors that display PHI in areas where such information may be vulnerable to shoulder surfing.
10. Files and documents awaiting disposal are properly labeled and kept in locked locations, including locked shred bins.
11. A process to reinforce accurate patient identification, for any papers containing PHI, given to or mailed to the patient.
12. Provision of enclosed offices or interview rooms for verbal exchange of confidential information.
13. Logging off or locking of computer workstations when leaving the vicinity of the workstation.
14. Ensuring that fax machines are kept in secure areas, and that faxes are promptly removed from the fax machine.
15. Locating security cameras in areas that may be prone to PHI security incidents.
16. Locked data closets or rooms.
17. For work spaces with paper containing PHI, ensuring that such paper is kept face down or in secured cabinets or drawers.
18. Responsibility given to users to maintain the physical security of mobile devices in their possession at all times. This includes, but is not limited to, ensuring that the device is either physically within the user's control, or locked in an area where unauthorized users cannot access it.
19. Environmental control systems are established to maintain temperature,

humidity, and electrical values that support a stable computing environment.

D. Safeguarding confidential information –Technical Safeguards

Technical safeguards are the technology and the policy and procedures for its use that protect electronic protected health information (ePHI) and control access to it.

Technical safeguards that have been implemented within the HCSD system are outlined in HCSD Policy 7701, and include, but are not limited to:

1. Encryption of hospital issued mobile devices, including laptops, USBs, and smart phones.
2. Assignment of a unique user name for identifying and tracking user identity.
3. Provision for emergency access to critical applications and systems in the event of an emergency.
4. Use of an automatic logoff that terminates an electronic session after a predetermined amount of inactivity.
5. Implementation of hardware, software, and other mechanisms that records and makes available the examination of activity in information systems containing ePHI.
6. Provisions for user authentication.
7. Implementation of access audits to primary ePHI systems, and the capability to pull an access audit on other ePHI systems.
8. Implementation of technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

IV. EXCEPTION

The HCSD CEO or designee may waive, suspend, change, or otherwise deviate from any provision of this policy deemed necessary to meet the needs of the agency as long as it does not violate the intent of this policy, state and/or federal law, Civil Service Rules and Regulations, LSU Policies/Memoranda, or any other governing body regulations.

Document Metadata

Document Name:	7521- 24 Administrative Technical and Physical Safeguards.doc
Policy Number:	7521
Original Location:	/LSU Health/HCSD/7500 - HIPAA
Created on:	04/14/2003
Published on:	03/26/2024
Last Review on:	03/05/2024
Next Review on:	03/05/2025
Effective on:	04/14/2003
Creator:	Townsend, Kathy *HCSD Human Resources Director*
Committee / Policy Team:	Main Policy Team
Owner/SME:	Simien, Tammy *Staff Attorney*
Manager:	Reeves, Rebecca *Compliance and Privacy Officer*
Author(s):	Wicker, Claire M. *PROJECT COORDINATOR* Reeves, Rebecca *Compliance and Privacy Officer* Simien, Tammy *Staff Attorney*
Approver(s):	Wilbright, Wayne *Chief Medical Informatics Officer* Reeves, Rebecca *Compliance and Privacy Officer* Simien, Tammy *Staff Attorney*
Publisher:	Wicker, Claire M. *PROJECT COORDINATOR*

Digital Signatures:

Currently Signed

Approver:
Reeves, Rebecca
Compliance and Privacy Officer

03/26/2024

Approver:
Simien, Tammy
Staff Attorney

03/26/2024

Approver:

Wilbright, Wayne
Chief Medical Informatics Officer

03/26/2024