LOUISIANA HEALTH SCIENCES CENTER- HEALTH CARE SERVICES DIVISION
BATON ROUGE, LA

POLICY NUMBER:	7521-15
CATEGORY:	HIPAA Policies
CONTENT:	Administrative, Technical and Physical Safeguards
EFFECTIVE DATE:	April 14, 2003
REVISED:	July 25, 2013 February 26, 2015
INQUIRIES TO:	**LSU HCSD** **Compliance Section** **Post Office Box 91308** **Baton Rouge, LA 70821-1308** **Telephone: 225-354-7032**

Deputy Chief Executive Officer
LSU Health Care Services Division

4/2/15
Date

I. SCOPE

This policy is applicable to all workforce members of the LSU Health Care Services Division facilities, including employees, physician/practitioner practices, vendors, agencies, business associates and affiliates.

II. PURPOSE

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 © and other applicable federal, state, and/or local laws and regulations.

III. POLICY

1. General

Louisiana State University (LSU) System 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.

2. Safeguarding confidential information –LSU workplace practices

a) Paper

i) Each LSU System workplace will store files and documents in locked rooms or storage systems.

ii) In workplaces where lockable storage is not available, LSU System staff will take reasonable efforts to ensure the safeguarding of confidential information.

iii) Each LSU System workplace will ensure that files and documents awaiting disposal or destruction in desk-site containers, storage rooms, or centralized waste/shred bins, are appropriately labeled, are disposed of on a regular basis, and that all reasonable measures are taken to minimize access.

iv) Each LSU System workplace will ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements.

v) Whenever paper with PHI is mailed or handed off to someone, the person sending the paper to its destination shall go through each piece of paper to ensure that the correct patient's information is going to the correct destination. For example, if a nurse is handing five pages of discharge instructions and prescriptions to a patient, the nurse shall use two identifiers to ensure she has the correct patient, and that each piece of paper belongs to that patient.

b) Oral

i) LSU System staff will take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs.

ii) Each LSU System workplace will make enclosed offices and/or interview rooms available for the verbal exchange of confidential information.

Exception: In work environments structured with few offices or closed rooms, such as in the hospitals, home-based offices, or open office environments, uses or disclosures that are incidental to an otherwise permitted use or disclosure could occur. Such incidental uses or disclosures are not considered a violation provided that the LSU System has met the reasonable safeguards and minimum necessary requirements.

iii) Each LSU System workplace must foster employee awareness of the potential for inadvertent verbal disclosure of confidential information.

c) Visual

i) LSU System staff must ensure that observable confidential information is adequately shielded from unauthorized disclosure on computer screens and paper documents.

(A) Computer screens: Each LSU System workplace will make every effort to ensure that confidential information on computer screens is not visible to unauthorized persons.

(B) Paper documents: LSU System staff must be aware of the risks regarding how paper documents are used and handled, and must take all necessary precautions to safeguard confidential information.

3. Safeguarding confidential information – LSU System administrative safeguards

a) Implementation of role-based access and the Minimum Necessary Policy will promote administrative safeguards.

i) Role Based Access (RBA) is a form of security allowing access to data based on job function in accordance with LSU System security procedures. Employees shall be assigned to an RBA group that will give members access only to the minimum necessary information to fulfill their job functions.

b) Conducting internal reviews periodically will permit LSU System to evaluate the effectiveness of safeguards.

i) LSU System managers and supervisors will use the LSU System Safeguards Assessment Tool to conduct annual reviews in order to evaluate and improve the effectiveness of their current safeguards.

c) Development and implementation of department-wide security policies will enhance administrative safeguards.

i) LSU System staff will be required to sign a document that constitutes a formal commitment to adhere to the department-wide security policies.

IV. PROCEDURE

1. General

There are no accompanying procedures.

2. Safeguarding confidential information – LSU System workplace practices

a) Paper

i) Files and documents being stored:

(A) Lockable desks, file rooms, open area storage systems must be locked.

(B) Where the LSU System has desks, file rooms, or open area storage systems that are not lockable, reasonable efforts to safeguard confidential information must be implemented.

ii) Files and documents awaiting disposal/destruction:

(A) Desk-site containers: The LSU System workplace must ensure that confidential information awaiting disposal is stored in containers that are appropriately labeled and are properly disposed of on a regular basis.

(B) Storage rooms containing confidential information awaiting disposal: Each LSU System workplace must ensure that storage rooms are locked after business hours or when authorized staff are not present.

(C) Centralized waste/shred bins: Each LSU System workplace must ensure that all centralized bins or containers for disposed confidential information are clearly labeled "confidential", sealed, and placed in a lockable storage room.

(D) Each LSU System workplace that does not have lockable storage rooms or centralized waste/shred bins must implement reasonable procedures to minimize access to confidential information.

iii) Files and documents in use:

(A) Documents that are not in immediate use but needed for the day's Work should be placed face down, or in a folder that conceals the PHI.

iv) Shredding of files and documents authorized consistent with record retention requirements.

(A) LSU System staff: Must ensure that shredding is done timely.

(B) Outside contractors: LSU System must ensure that such entity is under a written contract that requires safeguarding of confidential information throughout the destruction process.

(C) Papers awaiting shredding should be kept in locked shred boxes or other similar secure areas, and should not be kept in areas that would be easily confused with regular trash.

b) Oral

i) LSU staff must take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs, and should be aware of risk levels.

(A) Locations of verbal exchange with various risk levels:

(I) Low risk: interview rooms, enclosed offices, and conference rooms.

(II) Medium risk: employee only areas, telephone, and individual cubicles.

(III) High risk: public areas, reception areas, the emergency department, and shared cubicles housing multiple staff where clients are routinely present.

c) Visual

i) LSU System staff must ensure that observable confidential information is adequately shielded from unauthorized disclosure.

ii) Computer screens: LSU System offices must ensure that confidential information on computer screens is not visible to unauthorized persons. Suggested means for ensuring this protection include:

(A) Use of polarized screens or other computer screen overlay devices that shield information on the screen from persons not the authorized user;

(B) Placement of computers out of the visual range of persons other than the authorized user;

(C) Clearing information from the screen when not actually being used;

(D) Locking-down computer work stations when not in use; and

(E) Other effective means as available.

(F) All outgoing email messages must use the Confidentiality statement approved by their facility campus.

iii) Paper documents: LSU System staff must be aware of the risks regarding how paper documents are used and handled, and must take all necessary precautions to safeguard confidential information.

(A) LSU System staff must take special care to ensure the protection and safeguarding of, and the minimum necessary access to, paper documents containing confidential information that are located on:

(I) Desks;
(II) Fax Machines;
(III) Photocopy machines;
(IV) Portable electronic devices (e.g., laptop computers, PDAs, etc.);
(V) Computer printers; and
(VI) Common areas (e.g., break rooms, cafeterias, restrooms, elevators, etc.).

3. **Safeguarding confidential information – LSU System administrative safeguards**

a) Role Based Access (RBA): Roles must be created and defined based on the information LSU System owns and where it is located and how it is used and why. A determination of who should have access to the specific data must be established.

i) LSU System managers and supervisors must decide the role of each of their staff and request exceptions based on the needs of their office.

ii) Managers are responsible for allowing access to enough information for their staff to do their jobs while holding to the minimum necessary standard.

b) LSU System managers and supervisors will:

i) Ensure that workforce members receive security awareness as part of initial employee training and refresher training programs.

ii) Conduct a thorough assessment to ensure that their department practices are compliant with HIPAA rules and regulations..

iii) Foster a more secure atmosphere and enhance the belief that confidential information is important and that protecting privacy is key to achieving LSU System goals.

iv) Managers will update the safeguards in place each year, seeking to achieve reasonable administrative, technical, and physical safeguards.

c) Employ strict security measures to safeguard online transactions. All financial transactions must be done on a secured server and all personal information must be stored in a secured database and must be sent in an encrypted format.

d) Utilize the Security Policies to augment safeguard procedures.

Reference: LSU Security Policies

Revision History
February 26, 2015

- On page 3, #2.a. , added "(ii) Whenever paper with PHI is mailed or handed off to someone, the person sending the paper to its destination shall go through each piece of paper to ensure that the correct patient's information is going to the correct destination. For example, if a nurse is handing five pages of discharge instructions and prescriptions to a patient, the nurse shall use two identifiers to ensure she has the correct patient, and that each piece of paper belongs to that patient."
- On Page 5, added "(iii) Files and documents in use: (B) Documents that are not in immediate use but needed for the day's work should be placed face down, or in a folder that conceals the PHI."
- On Page 6, iv. added " (C) Papers awaiting shredding should be kept in locked shred boxes or other similar secure areas, and should not be kept in areas that would be easily confused with regular trash."
- On Page 6 , b (i) (A) (iii), added "the emergency department" as a high risk area.