LSUHealthNewOrleans
Office of the Chancellor

PRIVACY POLICY AND PROCEDURES Policy #: 2100.13
LSU Health Sciences Center New Orleans
Date Effective: April 14, 2003
Patient Information Policy
Administrative, Technical, and Physical Safeguards

SCOPE:
All Louisiana State University (LSU) System health care facilities and providers including, but not limited to hospitals, physician practices, clinics, schools, etc. on the LSU Health Sciences Center New Orleans Academic Campus.

Nota Bene: All LSU System health care facilities and providers including, but not limited to hospitals, physician clinics, schools, etc. on the LSU Health Sciences Center New Orleans Academic Campus, are referred to in this policy as LSUHSC-NO.

PURPOSE:
LSUHSC-NO 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.

POLICY:
LSUHSC-NO 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.
Safeguarding confidential information –LSU workplace practices:
Paper:
- Each LSUHSC-NO workplace will store files and documents in locked rooms or storage systems.
- In workplaces where lockable storage is not available, LSUHSC-NO staff will take reasonable efforts to ensure the safeguarding of confidential information.
- Each LSUHSC-NO 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.
- Each LSUHSC-NO workplace will ensure that shredding of files and documents is performed on a timely basis, consistent with record retention requirements.

Verbal:
- LSUHSC-NO staff will take reasonable steps to protect the privacy of all verbal exchanges or discussions of confidential information, regardless of where the discussion occurs.
- Each LSUHSC-NO 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 LSUHSC-NO has met the reasonable safeguards and minimum necessary requirements.

- Each LSUHSC-NO workplace must foster employee awareness of the potential for inadvertent verbal disclosure of confidential information.

Visual:

- LSUHSC-NO staff must ensure that observable confidential information is adequately shielded from unauthorized disclosure on computer screens and paper documents.
- Computer screens: Each LSUHSC-NO workplace will make every effort to ensure that confidential information on computer screens is not visible to unauthorized persons.
- Paper documents: LSUHSC-NO 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.

Safeguarding confidential information – LSUHSC-NO administrative safeguards:

- Implementation of Least Privilege Administration and the Minimum Necessary Policy will promote administrative safeguards.
- LSUHSC-NO managers and supervisors will conduct ongoing reviews in order to evaluate and improve the effectiveness of their current safeguards.
- Development and implementation of department-wide security policies will enhance administrative safeguards.
- LSUHSC-NO staff will be required to sign a document that constitutes a formal commitment to adhere to the department-wide security policies.

DEFINITIONS:

Least Privilege Administration - A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks they are authorized to perform, and no others.

PROCEDURE:

1.0 Safeguarding confidential information – LSUHSC-NO workplace practices

1.1 Paper

1.1.1 Files and documents being stored:

- Lockable desks, file rooms, open area storage systems must be locked.
- Where the LSUHSC-NO has desks, file rooms, or open area storage systems that are not lockable, reasonable efforts to safeguard confidential information must be implemented.

1.1.2 Files and documents awaiting disposal/destruction:

- Desk-site containers: The LSUHSC-NO 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.
- Storage rooms containing confidential information awaiting disposal: Each LSUHSC-NO workplace must ensure that storage rooms are locked after business hours or when authorized staff are not present.
- Centralized waste/shred bins: Each LSUHSC-NO 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.
- Each LSUHSC-NO workplace that does not have lockable storage rooms or centralized waste/shred bins must implement reasonable procedures to minimize access to confidential information.
- Shredding of files and documents authorized consistent with record retention requirements.

- LSUHSC-NO staff: Must ensure that shredding is done timely.
- Outside document destruction contractors: LSUHSC-NO must ensure that such entity is under a written contract that requires safeguarding of confidential information throughout the destruction process.

1.2 Verbal

1.2.1 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.

1.2.2 Locations of verbal exchange with various risk levels:

1.2.2.1 Low risk: interview rooms, enclosed offices, and conference rooms.

1.2.2.2 Medium risk: employee only areas, telephone, and individual cubicles.

1.2.2.3 High risk: public areas, reception areas, and shared cubicles housing multiple staff where clients are routinely present.

1.3 Visual

1.3.1 LSUHSC-NO staff must ensure that observable confidential information is adequately shielded from unauthorized disclosure.

1.3.2 Computer screens: LSUHSC-NO offices must ensure that confidential information on computer screens is not visible to unauthorized persons. Suggested means for ensuring this protection include:

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

1.3.4 Placement of computers out of the visual range of persons other than the authorized user;

1.3.4.1 Clearing information from the screen when not actually being used;

1.3.4.2 Locking-down computer work stations when not in use; and

1.3.4.3 Other effective means as available.

1.4 All outgoing email messages must use the Confidentiality statement approved by their facility campus.

1.5 Paper documents: LSUHSC-NO 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.

1.6 LSUHSC-NO 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:

- Desks;
- Fax Machines;
- Photocopy machines;
- Portable electronic devices (e.g., laptop computers, palm pilots, etc.);
- Computer printers; and
- Common areas (e.g., break rooms, cafeterias, restrooms, elevators, etc.).

1.7 All outgoing faxes must use the Confidentiality statement approved by their facility/campus.

2.0 Safeguarding confidential information – LSUHSC-NO administrative safeguards.

2.1 Least Privilege Administration: A determination of who should have what level of access to the specific data must be established.

2.2 LSUHSC-NO managers and supervisors must decide the level of access for each of their staff based on the needs of their office.

2.3 Managers are responsible for allowing access to enough information for their staff to do their jobs while holding to the minimum necessary standard.
2.4 LSUHSC-NO managers and supervisors will:

- Ensure that workforce members receive security awareness as part of initial employee training and refresher training programs.
- Conduct a thorough assessment.
- Foster a more secure atmosphere and enhance the belief that confidential information is important and that protecting privacy is key to achieving LSUHSC-NO goals.

2.5 Managers will update the safeguards in place each year, seeking to achieve reasonable administrative, technical, and physical safeguards.
2.6 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.
2.7 Utilize the Security Policies to augment safeguard procedures.

REFERENCE:
LSU Security Policies