Safeguards for Protected Health Information Policy

Policy #:	HP013.1
Policy Type:	University
Responsible Executive:	VPAA
Responsible Office:	Academic Affairs
Originally Issued:	November 8, 2023
Latest Revision:	November 8, 2023
Effective Date:	November 8, 2023

I. Policy Statement

The University of Louisiana at Monroe's Safeguards for Protected Health Information Policy states that all ULM 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.

II. Purpose of Policy

ULM 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.

III. Applicability

This policy is applicable to all faculty and staff.

IV. Definitions

<u>Least Privilege Administration</u> - 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.

V. Policy Procedure

1.0 Safeguarding confidential information – ULM 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 ULM 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 ULM 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 ULM workplace must ensure that storage rooms are locked after business hours or when authorized staff are not present.
- Centralized waste/shred bins: Each ULM 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 ULM 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 is consistent with record retention requirements.

- ULM staff must ensure that shredding is done in a timely manner.
- Outside document destruction contractors: ULM 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 ULM 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:

- Low risk: interview rooms, enclosed offices, and conference rooms.
- Medium risk: employee only areas, telephone, and individual cubicles.
- High risk: public areas, reception areas, and shared cubicles housing multiple staff where patients and clients are routinely present.

1.3 Visual

1.3.1 ULM staff must ensure that observable confidential information is adequately shielded from unauthorized disclosure.

1.3.2 Computer screens: ULM 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 containing PHI must use the Confidentiality statement approved by their facility campus.

1.5 Paper documents: ULM 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 ULM 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, IPads, etc.);
- Computer printers; and
- Common areas (e.g., break rooms, cafeterias, restrooms, elevators, etc.).

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

2.0 Safeguarding confidential information – ULM 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 ULM managers and supervisors must decide the level of access for each of their workforce based on the needs of their office/clinic.

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 ULM managers and supervisors will:

- Ensure that workforce members receive privacy and security awareness as part of initial employee training and refresher training programs.
- Conduct a thorough risk assessment.
- Foster a more secure atmosphere and enhance the belief that confidential information is important and that protecting privacy is key to achieving ULM goals.

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

2.6 Utilize ULM Security Policies to augment safeguard procedures.

VI. Enforcement

The Vice President of Academic Affairs will be responsible for enforcement of this policy.

VII. Policy Management

The Vice President of Academic Affairs will be responsible for enforcement of this policy.

VIII. Exclusions

None

IX. Effective Date

This policy is effective upon the date signed by the University President.

X. Adoption

This policy is hereby adopted on this 8th day of November 2023.

Recommended for Approval by:

Mark Arant
____
Dr. Mark Arant, Provost

Approved by:

Ron Berry
____
Dr. Ronald L. Berry, President

XI. Appendices, References and Related Materials

N/A

XII. Revision History

Original Adoption Date: November 8, 2023.