SAINT LOUIS UNIVERSITY

STORAGE OF PROTECTED HEALTH INFORMATION (PHI)

Policy Number: OUC-049 **Version Number: 2.0**
Effective Date: 04/14/2003
Responsible University Official: Privacy Officer
Approved By: Executive Staff
Legal and Compliance Committee

1.0 INTRODUCTION

Saint Louis University (hereinafter the "University") is committed to provide services in compliance with all state and federal laws governing its operations, incorporating the highest levels of business and professional ethics. HIPAA requires the implementation of reasonable safeguards for storage of protected health information (PHI) whether in paper or electronic format. Storage of documents and files containing PHI need to be kept in secure locations such as offices and storage areas that and be locked with limited access or lockable desk drawers.

Reasonably safeguarding electronically stored PHI requires that such information is maintained on systems and devices with limited access. Storage of electronic PHI may be located on the University's systems, servers, network attached devices, PC workstations or electronic storage media such as CDs, diskettes, cartridge tapes, and other external storage devices. Storage of electronic PHI shall utilize appropriate safeguards to limit access including unique password protected user accounts, locked storage locations, and the use of encryption when feasible.

2.0 PURPOSE

The purpose of this policy is to provide guidance to workforce regarding the storage of protected health information.

3.0 PERSONNEL AFFECTED

This policy applies to all regular full-time and part-time faculty and staff and volunteers within all divisions of the University, including employees, professional staff members, residents, agents, representatives and consultants with access to patients' protected health information.

4.0 DEFINITIONS

Protected Health Information (PHI): Any individually identifiable health information transmitted or maintained in any form or medium, including oral, written, and electronic. Individually identifiable health information relates to an individual's health status or condition, furnishing health services to an individual or paying or administering health

care benefits to an individual. Information is considered PHI where there is a reasonable basis to believe the information can be used to identify an individual.

Workforce: Employees, volunteers, trainees, contractors, and other persons under the direct control of the covered entity, whether or not paid by the covered entity, who have access to confidential information.

5.0 POLICY

Saint Louis University has a duty to protect the confidentiality and integrity of confidential medical information as required by law and professional ethics. This policy defines the guidelines and procedures that must be followed for the storage of PHI. All personnel must strictly observe the following standards relating to the storage of PHI:

University personnel must ensure that, outside of regular working hours, all desks and working areas that contain PHI are properly secured, unless the immediate area can be secured from unauthorized access.

When protected health information is being released through electronic medium such as teleconference, video feed, or over the Internet, University personnel must treat the protection of PHI is the same manner as PHI recorded on paper, securing and limiting access to the PHI to authorized personnel only.

PHI stored in medical equipment (e.g. EKG, Ultrasound machines) must be kept secure and disposed of according to *Disposal of PHI* policy.

When not in use, PHI must always be protected from unauthorized access. When left in an unattended room, such information must be appropriately secured.

If PHI is to be stored on the hard disk drive or other internal components of a personal computer or electronic device, it must be protected by appropriately protected by password, encryption, and other necessary means of access control. Unless encrypted, when not in use, this media must be secured from unauthorized access.

If PHI is stored on diskettes, CD-ROM or other removable data storage media, it cannot be commingled with other electronic information.

6.0 SANCTIONS

Individuals who fail to comply with this policy and the procedures associated with it will be subject to disciplinary actions guided by the University's Staff Performance Management Policy, Faculty Manual, or Student Guidelines.

Non-compliance in this Policy can result in disciplinary action, including but not limited to, restricted incentive payments, suspension or termination. It may also result in the enforcement of a corrective action plan, as well as notification of the suspected misconduct and/or violation to government regulatory agencies.

This Policy does not limit the University's ability to impose greater sanctions or impose immediate action against serious violations. Disciplinary actions appropriate to the severity of the infraction will be carried out as needed.

7.0 CHANGES TO THIS POLICY

Changes to this policy may be necessary from time to time. At a minimum, the policy and all other program policies, procedures and guidelines will be reviewed on an annual basis.

8.0 RELATED POLICIES & DOCUMENTS

- Institutional Statement on Living the Mission: Standards of Conduct for the Common Good
- Compliance Hotline Reporting Policy
- Anti-Fraud Policy

REVISION HISTORY

EFFECTIVE DATE	VERSION NUMBER	MODIFICATION
4/14/2003	1.0	New Policy
7/01/2008	1.1	Review & Change Format
3/01/2015	1.2	Review & Change Format
	2.0	Ownership Shifted from Provost to General Counsel