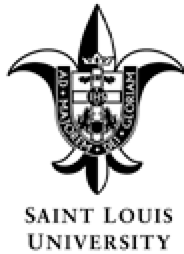

SAINT LOUIS UNIVERSITY

DISPOSAL OF PROTECTED HEALTH INFORMATION (PHI)

Policy Number: OUC-039 **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 that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information (PHI), in any form. Reasonable safeguards must be implemented to limit uses and disclosures of PHI including situations that involve the disposal of such information.

2.0 PURPOSE

The purpose of this policy is to provide management and workforce members with the procedures for the proper disposal 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

Degaussing: Degaussing a hard drive or magnetic tape means that data has been erased leaving random patterns, thereby rendering previous data unrecoverable. Hard drives cannot be re-used after degaussing.

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.

5.0 POLICY

It is the duty of Saint Louis University to protect the confidentiality and integrity of confidential medical information as required by law and professional ethics. Protected health information may only be disposed of by means that assure that it will not be accidentally released to an outside party. Management must assure that appropriate means of disposal are reasonably available and operational. This policy is to define the guidelines and procedures that must be followed when disposing of information containing PHI.

Summary of Disposal Policy

All personnel must strictly observe the following standards relating to disposal of hardcopy and electronic copies of PHI:

PHI must not be discarded in trash bins, unsecured bags, or other publicly-accessible locations. This information must be personally shredded or placed into secure recycling containers for proper disposal of confidential documents.

Printed material and electronic data containing PHI shall be disposed of in a manner that ensures confidentiality.

It is the individual's responsibility to ensure that the document has been secured or destroyed. And it is the office manager and supervisor's responsibility to ensure that all employees are adhering to the policy.

6.0 PROCEDURES

Destruction of Convenience Copies and Original Documents (Day-to-Day Destruction)

1. Saint Louis University management and supervisor(s) shall provide users with access to shredders or secured recycling containers for proper disposal of confidential printouts containing PHI.

2. Users may elect to use shredders or use secure recycle containers for later destruction of convenience copies, as long as the destruction is in accordance with this policy.

Electronic Copies

1. Secure methods will be used to dispose of electronic data and output. Any questions of appropriateness of action or carrying out of this procedure should be brought to the attention of the University Compliance Office, Privacy Officer, or Security Officer. Disposal of electronic data may consist of the following methods:

   a. Deleting on-line data using the appropriate utilities;
   b. "Degaussing" computer tapes to prevent recovery of data;

c. Removing PHI from mainframe disk drives being sold or replaced, using the appropriate initialization utilities;

d. Erasing diskettes or disk drivers to be re-used using a special utility to prevent recovery of data; or

e. Destroying discarded diskettes, CDs, or other removable data forms.

Hardcopy (Bulk Destruction)

1. Secure methods will be used to dispose of hardcopy data and output.

2. PHI printed material shall be shredded and recycled by a firm specializing in the disposal of confidential records or be shredded by an employee of University authorized to handle and personally shred the PHI.

3. Microfilm or microfiche must be cut into pieces or chemically destroyed.

4. After documents have reached their retention period, all PHI must be securely destroyed.

5. If hardcopy PHI (paper, microfilm, microfiche, etc.) cannot be shredded, it must be incinerated.

Documentation of Destruction

1. To ensure successful destruction is performed, University personnel or a bonded destruction service must carry out the destruction of PHI.

2. If a bonded shredding company undertakes the destruction, the bonded shredding company shall provide Saint Louis University with the document of destruction that contains the following information:

   Date of destruction,
   Method of destruction,
   Description of the disposed records,
   Inclusive dates covered,
   A statement that the records have been destroyed in the normal course of business, and
   The signatures of the individuals supervising and witnessing the destruction.

7.0 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.

8.0 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.

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