SAINT LOUIS UNIVERSITY

Privacy and Incident Response Reporting

Policy Number: OUC-059 **Version Number: 1.0**
Effective Date: 07/31/2015
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.

In order to protect the integrity, availability, and confidentiality of business information including protected health information, systems, and applications, the University has established policies and procedures that address privacy and security including the reporting and response to incidents.

2.0 PURPOSE

This policy identifies the requirement for reporting privacy and security incidents and establishes procedure for coordinating response involving appropriate personnel involved in discovery, containment, assessment, mitigation, and notification requirements.

3.0 PERSONNEL AFFECTED

The scope of this policy applies to all University workforce members who become aware of a privacy or security incident and individuals responsible for carrying out processes in response to incidents.

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 when there is a reasonable basis to believe the information can be used to identify an individual.

Personally Identifiable Information (PII): Individually identifiable information that is protected by law from disclosure to the general public. Examples of PII include personal information in combination with data elements such as Social Security Number, financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Restricted Data: University maintained electronically stored data for which inappropriate use or access presents a high reputational and/or business risk to the University. Restricted Data typically is subject to significant legal requirements for the protection of the data and includes data/information such as social security numbers, medical records, information related to students, human resources, donors or prospective donors, financial data, contracts, credit

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 workforce members shall promptly report any suspected privacy or information security incidents to the IT Security (Information Security Team) or the Compliance Department (Privacy Officer).

IT Security and the Compliance Department will coordinate investigations of privacy and information security incidents in accordance with the Information Technology Services Department's procedure for Information Security Incident Response.

5.1 Privacy and Information Security Incidents

5.1.1 Privacy Incidents

Privacy incidents include the acquisition, access, use, or disclosure of protected health information in a manner not permitted by HIPAA which compromises the security or privacy of protected health information.

Privacy incidents can involve protected health information in all forms, including electronic, paper, and oral. Privacy incidents can also be security incidents. Following are examples of possible privacy incidents:

- Faxes, emails or regular mail containing restricted information are sent to the wrong people or addresses.
- Documents containing restricted information left unattended in conference rooms, the cafeteria, a parking lot, and other public locations.
- Documents containing restricted information thrown away in regular trash or recycling bins.
- Patient information, including photos, shared publicly on websites or in brochures, presentations or videos without obtaining a patient authorization.
- Accessing the medical record of a co-worker, colleague, friend, family member, supervisor or celebrity when not authorized to do so for a work related task.
- Loss or theft of a laptop, USB flash drive, CD, or DVD with unencrypted restricted information.

- Workforce member tells friend, family, or reporter information about patients or otherwise discloses such information without the patient's authorization.
- Restricted information is posted to public view on social media or other websites.
- Patient information is collected for research use without required approvals and consents.

5.1.2 Security Incidents

Security incidents involve only electronic information. They may also qualify as "privacy" incidents under HIPAA/HITECH. Following are examples of possible security incidents:

- Loss or theft of a laptop, USB flash drive, CD, or DVD with unencrypted restricted information.
- Unauthorized Access: A person gains logical or physical access without permission to a network, system, application, data, or other resource.
- Corruption of a computer system and/or data.
- Copiers, scanners, computers, are discarded without first securely wiping any restricted information.
- Violating Saint Louis University's Appropriate Use Policy.
- Sharing login and password information.

5.2 Reporting

Missouri law requires notification under certain circumstances for the unauthorized access to and unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality, or integrity of the personal information.

Notifications will be sent to individuals, the media, and the Department of Health and Human Services in the case of a breach of unsecured protected health information in accordance with the requirements of HIPAA 45 CFR § 164.400. Timeliness of notifications will be in accordance with applicable state and federal laws.

5.2.1 External Reporting

State and federal reporting requirements will be performed in collaboration with IT Security and the University Compliance Department. Submission of notice to the Secretary of Health and Human Services for a breach of unsecured protected health information shall be performed by the University Privacy Officer.

5.2.2 Internal Reporting

Incident details will be maintained in a log for no less than six years. The log of security incidents and follow-up actions shall be managed and maintained by IT Security. A log of HIPAA privacy incidents and follow-up actions shall be maintained by the University Privacy Officer.

5.3 Mitigation

Coordination of remediation steps and post-incident activities will be conducted by IT Security in response to security incidents. Risk mitigation of privacy incidents that do not involve electronic information or security will be conducted by the University Privacy Officer.

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 AND DOCUMENTS

- Information Security Incident Response Procedure
- Acceptable Use Policy

REVISION HISTORY

EFFECTIVE DATE	**VERSION NUMBER**	**MODIFICATION**
	1.0	New Policy