SAINT LOUIS UNIVERSITY

Business Associates Agreement Policy

Policy Number: OUC-057 **Version Number: 2.0**
Effective Date: 05/18/2010
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.

The HIPAA Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it creates, receives, maintains or transmits electronically on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

2.0 PURPOSE

The purpose of this policy is to provide guidelines for compliance with Health Insurance Portability and Accountability Act (HIPAA) and the Privacy regulation relating to "Business Associates".

3.0 PERSONNEL AFFECTED

This policy applies to all University workforce involved with obtaining contracted business services that use or disclose protected health information (PHI).

4.0 DEFINITIONS

Business Associate: A person who is not a member of the covered entity's workforce, and who performs any function or activity involving the use or disclosure of protected health information or who provides services to a covered entity that involves the disclosure of protected health information.

Business Associate Agreement (BAA): An agreement for services between a covered entity and another organization or person that addresses the concepts and requirements set forth in the HIPAA Privacy & Security Rule. This agreement includes provisions for uses and disclosures of protected health information and requirements for safeguarding of such information.

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.

5.0 POLICY

Saint Louis University requires that all business associates, as defined by HIPAA, sign a written agreement/contract that provides satisfactory assurances the business associate will use the information only for the purposes for which it was engaged to perform, will safeguard the information from misuse, and will assist the University in compliance of certain duties required under the Privacy Rule.

The Business Associate Agreement, contract, or other written arrangement with the business associate must contain the following elements:

- Describe the permitted and required uses of protected health information by the business associate.

- Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law.

- Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

- Require that any subcontractor to a Business Associate who receives, maintains, or transmits PHI on behalf of the covered entity must agree to the same restrictions and conditions that apply to the business associate with respect to such information.

- Require reasonable steps to cure a breach or end a violation when the University knows of a material breach or violation by the business associate of the contract or agreement. If such steps are unsuccessful, to terminate the contract or arrangement.

The Privacy Officer, in coordination with the Office of General Counsel, will be responsible for implementation and oversight of business associate agreements/contracts involving safeguarding of protected health 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 AND DOCUMENTS

- Business Associate Agreement – Saint Louis University (template form)

REVISION HISTORY

EFFECTIVE DATE	VERSION NUMBER	MODIFICATION
5/18/2010	1.0	New Policy
3/11/2015	1.1	Review & Change Format
	2.0	Ownership Shifted from Information Technology Services to General Counsel