SAINT LOUIS UNIVERSITY

DE-IDENTIFICATION OF PHI

Policy Number: OUC-036 **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. The Privacy Rule was designed to protect individually identifiable health information through permitting only certain uses and disclosures of PHI provided by the Rule, or as authorized by the individual subject of the information. However, in recognition of the potential utility of health information even when it is not individually identifiable, §164.502(d) of the Privacy Rule permits a covered entity or its business associate to create information that is not individually identifiable by following the de-identification standard and implementation specifications in §164.514(a)-(b). These provisions allow the entity to use and disclose information that neither identifies nor provides a reasonable basis to identify an individual. The Privacy Rule provides two de-identification methods: 1) a formal determination by a qualified expert; or 2) the removal of specified individual identifiers as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to identify the individual.

2.0 PURPOSE

The purpose of this policy is to outline the requirements for de-identification of protected health information as defined by HIPAA. Data that has been de-identified can be used or disclosed without restriction and is not regulated by HIPAA.

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 protected health information.

4.0 DEFINITIONS

Institutional Review Board (IRB): A committee group comprised of Saint Louis University personnel and community representatives with varying backgrounds and professional experience that review and approve the research protocol involving human subjects.

Authorized User: An individual that is granted access to PHI for patients through an authorization, IRB waiver or who is performing an activity related to health care operations.

Health Care Operations: Activities related to Saint Louis University's functions as a health care provider, including general administrative and business functions necessary for the University to remain a viable health care provider.

Protected Health Information (PHI): Individually identifiable health information transmitted or maintained in any form or medium, including oral, written, and electronic communications. 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.

Limited Data Set: PHI that excludes 16 categories of direct identifiers, which may be used or disclosed, for purposes of research, public health, or health care operations, without obtaining either an individual's Authorization or a waiver or an alteration of Authorization for its use and disclosure with a data use agreement. The only potentially identifiable information allowed in a limited data set is: dates, ages, and zip codes.

5.0 POLICY

Saint Louis University has a duty to protect the confidentiality and integrity of PHI as required by law, and professional ethics. Whenever possible, de-identified PHI should be used. De-identified PHI is rendered anonymous when identifying characteristics are completely removed. PHI must be de-identified prior to disclosure to non-authorized users. This policy defines the guidelines and procedures that must be followed for the de-identification of PHI.

6.0 PROCEDURES

All workforce members must strictly observe the following standards relating to the de-identification of PHI:

De-identification requires the elimination not only of primary or obvious identifiers, such as the patient's name, address, date of birth (DOB), and treating physician, but also of secondary identifiers through which a user could deduce the patient's identity. For information to be de-identified the following identifiers of the individual must be removed:

- Names
- Address information smaller than a state, including street address, city, county, zip code
  (except if by combining all zip codes with the same initial three digits, there are more than 20,000 people)
- Names of relatives and employers

- All element of dates (except year), including DOB, admission date, discharge date, date of death; and all ages over 89 and all elements of dates including year indicative of such age except that such ages and elements may be aggregated into a single category of age 90 or older
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security Number (SSN)
- Medical record number
- Health beneficiary plan number
- Account numbers
- Certificate/License Number
- Vehicle identifiers, including license plate numbers
- Device ID and serial number
- Uniform Resource Locator (URL)
- Identifier Protocol (IP) addresses
- Biometric identifiers
- Full face photographic images and other comparable images
- Any other unique identifying number characteristic or code.

Whenever possible, de-identified PHI should be used for quality assurance monitoring and routine utilization reporting.

PHI used for research, including public health research, should be de-identified at the point of data collection for research protocols approved by the IRB, unless the participant voluntarily and expressly consents to the use of his/her personally identifiable information or an IRB waiver of authorization is obtained.

If an authorized user wishes to encrypt PHI when creating de-identified information the authorized user must ensure that:

The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

Anyone involved in the research project does not use or disclose the code or other means of record identification and does not disclose the mechanism to accomplish re-identification.

If removal of any identifiers is not practical or does not meet business needs, and the use of PHI is still required, approval must be obtained from the University Privacy Officer.

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