

Office of Compliance Programs
PRIVACY POLICY AND PROCEDURES

LSU Health Sciences Center New Orleans
Date Effective: September 23, 2009
Date Revised: September 23, 2013

Patient Information Policy

Breach Mitigation and Notification Policy

Policy #: 2100.25

Page: 1

SCOPE:

All Louisiana State University (LSU) System health care facilities and providers including, but not limited to hospitals, physician practices, clinics, schools, etc. on the LSU Health Sciences Center New Orleans Academic Campus.

Note Bene: All LSU System health care facilities and providers including, but not limited to hospitals, physician clinics, schools, etc. on the LSU Health Sciences Center New Orleans Academic Campus, are referred to in this policy as LSUHSC-NO.

PURPOSE:

To provide guidance to the health care facilities and providers affiliated with LSUHSC-NO on the requirements of the Health Insurance Portability and Accountability Act, the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164, Gramm-Leach-Bliley Act, the Louisiana Database Security Breach Notification Law (LA R.S. 51:3071) and any other applicable state or Federal laws or regulations regarding appropriate steps to take in the event of Breach or suspected Breach of Protected or Restricted Information as defined by PM-36.

POLICY:

All LSUHSC-NO-affiliated health care facilities and providers and students should notify the Privacy Officer immediately upon discovery of a Breach or suspected Breach of Protected or Restricted Information so that LSUHSC-NO may take appropriate steps to mitigate any harm that may possibly occur. Costs related to mitigation and notification of any Breach will be allocated to the department in which the Breach occurred.

DEFINITIONS:

Breach – For purposes of this policy means the acquisition, access, Use, or Disclosure of Protected or Restricted Information which compromises the security or privacy of the Protected or Restricted Information.

Disclosure – For purposes of this policy, means the release, transfer, or provision of access to Protected or Restricted Information outside of LSUHSC-NO. A disclosure of Protected or Restricted Information may occur orally or in writing.

Protected Information – For purposes of this policy means information that shall have extraordinary controls over its use and disclosure due to the sensitivity of its content. Examples of Protected Information include but are not limited to, Protected Health Information (PHI), employment records, background checks, student records, personal financial records, trade secret information and classified government information.

Office of Compliance Programs
PRIVACY POLICY AND PROCEDURES

Policy #: 2100.25

Page: 2

LSU Health Sciences Center New Orleans

Date Effective: September 23, 2009

Date Revised: September 23, 2013

Patient Information Policy

Breach Mitigation and Notification Policy

Restricted Information - For purposes of this policy means information of such a sensitive nature that access is limited to those individuals designated by management as having a need to know. Examples of Restricted Information include, but are not limited to, ongoing investigations, pending litigation, psychotherapy notes, and disciplinary actions.

Use - For purposes of this policy, means with respect to Protected or Restricted Information, the sharing, utilization, or examination of Protected or Restricted Information.

PROCEDURE:

1.0 Discovery of Breach

1.1 Immediately upon discovery of a Breach or suspected Breach, any LSUHSC-NO employee or student shall notify the Privacy Officer of the circumstances of the Breach or suspected Breach including but not limited to:

- A brief description of what happened, including the date of the Breach or suspected Breach and the date of the discovery of the breach, if known;
- A description of the types of unsecured Protected or Restricted Information that were involved in the Breach or suspected Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved), if known;

2.1 Investigation and Risk Assessment.

2.1 The Privacy Officer will conduct an investigation to establish the pertinent facts of the breach. Based upon the results of that investigation, the Privacy Officer will perform a risk assessment to determine the probability that the Protected or Restricted Information has been compromised.

2.2 The risk assessment will include at a minimum:

- Whether an unauthorized person to whom the disclosure of Protected or Restricted Information was made would not reasonably have been able to retain such information.
- The nature and extent of the Protected or Restricted Information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the Protected or Restricted Information or to whom the disclosure was made;
- Whether the Protected or Restricted Information was actually acquired or viewed; and
- The extent to which the risk to the Protected or Restricted Information has been mitigated.

2.3 Based upon the results of the risk assessment and review of the applicable laws and regulations, the Privacy Officer will either determine whether the reported incident constitutes a Breach under this policy and applicable laws.

2.4 If the Privacy Officer determines that a Breach has, in fact, occurred, the Privacy Officer will develop a Mitigation and Notification Plan to mitigate any adverse effects of the Breach. Each Plan will be developed on a case by case basis to specifically address the issues identified in the investigation and risk assessment. Such a plan may include but is not necessarily limited to:

- Notifications to individuals affected
- Notifications to government officials
- Notifications to mass media
- Notifications posted on the LSUHSC-NO website

Office of Compliance Programs
PRIVACY POLICY AND PROCEDURES

LSU Health Sciences Center New Orleans

Date Effective: September 23, 2009

Date Revised: September 23, 2013

Patient Information Policy

Breach Mitigation and Notification Policy

Policy #: 2100.25

Page: 3

- Considerations of law enforcement
- Provision of credit monitoring services to affected individuals
- Timeframes for completion of elements of the plan based upon applicable legal and regulatory requirements

2.5 Costs associated with the Mitigation and Notification Plan (postage, advertising, credit monitoring services, clerical support, etc.) will be allocated to the department in which the breach occurred.

REFERENCE:

45 CFR § 164.400

16 CFR §314

LA R.S. 51:3071 et seq.

PM-36 Ch. 12