LSU Health NEW ORLEANS
Office of the Chancellor

PRIVACY POLICY AND PROCEDURES Policy #: 2100.6
LSU Health Sciences Center New Orleans Page: 1
Date Effective: September 23, 2009
Date Revised: September 23, 2013
Date Revised: November 30, 2017
Patient Information Policy
Breach Mitigation and Notification Policy

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. This policy supersedes the Breach Mitigation and Notification Policy revised on September 23, 2013 (CM-53 Section Y) and the Mitigation Policy effective April 14, 2003 (CM-53 Section F).

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 Permanent Memorandum #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 (if the Breach was a result of an act or omission of an employee) or the school (if the Breach was a result of an act or omission of a student) 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.
Home Page – The default page of the LSUHSC-NO website which is the first page visitors see when navigating to the LSUHSC-NO Web site and login page for existing account holders.
Notification – Announcement of a Breach.
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.
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, sole possession 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;

2.0 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 (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. Depending upon the requirements of the applicable laws and regulations as well as the circumstances of the Breach, each Plan shall include some or all of the following elements:

2.4.1. *Notifications to Individuals Affected* – LSUHSC-NO shall notify each individual whose information has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of the Breach.

2.4.2. *Manner and Method of Notification to Individuals* – The manner and method used to notify individuals affected by a Breach shall provide reasonable assurance that all affected individuals were notified of the Breach and shall comply with applicable laws and regulations.

2.4.3. *Notifications to Government Officials* – Where it is required by applicable laws and/or regulations, the appropriate government officials shall be notified of the Breach in the manner specified in the applicable laws and regulations.

2.4.4. *Notifications to mass media* – If it is required by applicable laws and/or regulations or if the Privacy Officer determines it is necessary to ensure that all individuals are adequately notified of the Breach, Notifications, in the form of press releases, shall be sent to mass media outlets (television and radio stations, newspapers, etc.) serving the communities where the affected individuals reside or are believed to reside sufficient to reasonably ensure that all affected individuals are notified.

2.4.5. *Notifications posted on the LSUHSC-NO website* – If it is required by applicable laws and/or regulations or if the Privacy Officer determines it is necessary to help insure that all affected individuals are adequately notified of the Breach, Notification shall be posted on the LSUHSC-NO website. The Notification must be conspicuous and posted for at least 90 calendar days. The Notification may be placed directly on the LSUHSC-NO Home Page, if feasible, or a hyperlink to the Notification may be placed on the Home Page. If a hyperlink is used on the Home Page to convey the Notification, the hyperlink should be prominent so that it is conspicuous given its size, color, and graphic treatment in relation to other parts of the page, and it should be worded to convey the nature and importance of the information to which it leads. The hyperlink shall:

- Be in the format of "{*description of affected individuals*}, please click here for important information about a possible Breach of your {*description of information Breached*}". (Example: "Patients of the Family Practice Clinic, please click here for important information about a possible Breach of your PHI.")
- Encompass the entire message described above (i.e. if the user clicks anywhere on the message, it will redirect them to the Notification.)
- Be located on the Home Page in the position ordinarily reserved for emergency notices. If an emergency notice is present on the Home Page, the Notification shall appear below the emergency notice.
- Have a unique text color and background color that are not shared by any other text or background on the Home Page.
- Have a text size equal to or greater than the hyperlinks for prospective students, alumni/donors and other patient care hyperlinks.
- Have text attributes (bold, underline, italics, etc.), other than color, identical to the attributes of the hyperlinks for prospective students, alumni/donors and other patient care hyperlinks.

2.4.6. *Content of Notification* – The content of the Notifications to affected individuals, government officials, mass media and Notifications posted on the LSUHSC-NO website as described above shall be written in plain language and include but not be limited to:

- A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
- A description of the types of Protected and/or Restricted information that were involved in the Breach;
- Any steps individuals should take to protect themselves from potential harm resulting from the Breach;
- A brief description of what LSUHSC-NO is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches; and

- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

2.4.7. *Timeframes for completion of elements of the plan* – Each element of the Plan shall be completed without unreasonable delay and in no case later than the timeframes specified in the applicable laws and regulations except for delays due to Considerations of Law Enforcement.

2.4.8. *Considerations of Law Enforcement* - If a law enforcement official states to LSUHSC-NO that a Notification, notice, or posting required under this policy would impede a criminal investigation or cause damage to national security, LSUHSC-NO shall:

- If the statement is in writing and specifies the time for which a delay is required, delay such Notification, notice, or posting for the time period specified by the official; or
- If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the Notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

2.4.9. *Mitigation Steps* – LSUHSC-NO shall take appropriate actions to mitigate any harmful effects resulting from the Breach. Depending upon the requirements of applicable laws and regulations and the circumstances of the Breach, such actions may include but are not limited to:

- Provide methods of contact including but not limited to a toll-free telephone number and email address for use by affected individuals to ask questions and request further assistance.
- Providing credit monitoring services to affected individuals.
- Assuring or obtaining written assurances that the Breached information has been rendered unreadable and unrecoverable.
- Corrective actions to prevent a recurrence of the Breach.

2.4.10. *Administrative Support and Resources* – The department in which the Breach occurred shall cooperate with the Privacy Officer to ensure that the appropriate resources (e.g. staff, funds, etc.) are provided to ensure the successful and timely implementation of the plan.

2.5 Costs associated with the Mitigation and Notification Plan (postage, telecommunications, advertising, credit monitoring services, clerical support, etc.) will be allocated to the department (if the Breach was a result of an act or omission of an employee) or the school (if the Breach was a result of an act or omission of a student) in which the Breach occurred.

REFERENCES:

45 CFR § 164.400 *et seq.*
45 CFR §164.530(f)
16 CFR §314
LA R.S. 51:3071 *et seq.*
PM-36