POLICY AND PROCEDURE MANUAL

Pennington Biomedical	**POLICY NO. 415.00**	**ORIGIN DATE: 02/04/13**
IMPACTS:	**ALL PERSONNEL**	**LAST REVISED: 08/21/14**
SUBJECT:	**STATE BREACH NOTIFICATION**	**EFFECTIVE: 03/17/14**
SOURCE:	**LEGAL AND REGULATORY**	**VERSION NO. 1**

LA RS 51: 3071 -- 3077 (Louisiana Database Security Breach Notification Law) provides notification to individuals who may have had their privacy, financial, or other personal information compromised.

In addition, there are several other Federal laws that provide for notification when there is a data breach, such a FERPA, HIPAA and Gramm Leach Bliley, etc.

In a situation where the data breach is not covered by the Louisiana Database Security Breach Notification Law, Computing Services must check with the Director of Legal and Regulatory to ensure that notification of the breach is not required under another Federal or State law.

Louisiana Database Security Breach Notification Law (LDSBN)

LDSBN requires Pennington Biomedical following discovery of a breach in the security of the system containing **personal information,** notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

For the purposes of this law, **personal information** means an individual's first name or first initial, and last name in combination with any one or more of the following data elements, when the name of the data element is not encrypted or redacted:

- Social security number
- Driver's license number
- Account number, credit 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

Security Breach Threshold for Notification

Deciding Whether or Not to Notify

Computing Services should notify and defer to the Director of Legal and Regulatory Compliance regarding whether or not to notify individuals.
Some factors to consider are listed below in making a determination to notify individuals victimized by data breach incidents subject to state or federal notification requirements.

Herein, "the information," refers to data that would fulfill the notification requirement. A name in combination with Social Security Number, driver's license number, and/or financial account numbers (such as bank account or credit/debit card numbers) would qualify as notification-triggering information. Notification is required when information that could be used to commit identity theft has been breached.

1. Is the information in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information?
2. Is there evidence that information has been downloaded, copied, or otherwise accessed? (For example: an ftp log that contains the name of a file bearing notice-triggering information)
3. Was the compromised account privileged (e.g., root or administrator) or non-privileged (e.g., one with access to privileged information)?
4. Was a single system or multiple systems compromised?
5. Is the identity of the attacker known or unknown? If known, was the attacker a disgruntled insider, or an unaffiliated third party? Were multiple attackers involved?
6. Are there indications that the information was used by an unauthorized person, such as fraudulent account openings or reports of identity theft? Did the unauthorized person have access to the information for an extended period of time?
7. What was the time between compromise start and compromise discovery?
8. Did the compromise indicate a directed attack, such as a pattern showing the machine itself was targeted, versus an automated attack?
9. Did the attack appear to seek and collect the information?
10. Did the attack appear to include tampering with records (e.g., changing grades)?
11. Did the attacker attempt to cover up his or her activity?
12. Did the attacker release information about the nature or scope of the attack?
13. Was the information encrypted? Would the encryption method effectively prevent the information from being accessed?
14. What is the potential damage to individuals if notification is not given?
15. What is the potential damage to institutional credibility in the case of notification?
16. What is the potential damage to institutional credibility in the case of failure to notify?

Notification

Once the decision to notify has been made, notification shall be made in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement and any measures necessary to determine the scope of the breach, prevent further disclosures and restore the reasonable integrity of the data system.
Notification may be provided by:

1. Written notification
2. Electronic notification, if the notification provided is consistent with the provisions regarding electronic records and signatures set forth in 15 USC 7001.
3. Substitute notification, if an agency or person demonstrates that the cost of providing notification would exceed two hundred fifty thousand dollars or that the affected class of person to be notified exceeds five hundred thousand or the agency does not have sufficient contact information.
    a. Substitute notification shall consist of the following:
        i. Email notification when the agency has an email address for the individual
        ii. Conspicuous posting of the notification on the Internet site of the agency, if an Internet site is maintained.

Failure to disclose in a timely manner a security breach resulting in the disclosure of the individual's personal information can result in a civil action to recover actual damages.

Notice to Attorney General:

Louisiana Administrative Code Title 16, Part III § 701 requires that the agency provide written notice detailing the breach of security of the system, including names of all Louisiana citizens affected by the breach to Consumer Protection Section of the Attorney General's Office. Notice to the Attorney General shall be deemed timely if received within 10 days of the distribution of notice to Louisiana citizens. See Admin Code for more information.

PENNINGTON BIOMEDICAL RESEARCH CENTER LSU

Policy Committee Secretary's Attestation

Date of Policy Committee Meeting: 8/21/2014

Policy #: 415.00 – State Breach Notification Policy

Date of Approval: 8/21/2014

Publication Date: 9/3/2014

Effective Date: 8/21/2014

Anne Duke

Anne Duke, Policy Committee Secretary

9/2/14

Date

Approval by the Executive Director

William T. Cefalu

William T. Cefalu, MD
Executive Director

9/4/14

Date