LOUISIANA STATE UNIVERSITY
HEALTH CARE SERVICES DIVISION
BATON ROUGE, LA

POLICY NUMBER: 8515-21

CATEGORY: Compliance Policies

CONTENT: Breach Notification

EFFECTIVE DATE: February 1, 2011

REVISED/REVIEW DATE: September 14, 2011
November 9, 2012
September 19, 2013
July 17, 2014
October 26, 2015
February 22, 2016
April 25, 2016
August 29, 2017
February 11, 2019
January 24, 2020
March 31, 2021
June 21, 2021

INQUIRIES TO: **LSU HCSD Compliance**
Post Office Box 91308
Baton Rouge, LA 70821-1308
225-354-4840

Note: Approval signatures/titles are on the last page

Breach Notification Policy

I. Purpose

To provide for notification procedures as it relates to a breach of unsecured protected health information discovered by LSU HCSD, Lallie Kemp Medical Center, or their Business Associates as prescribed in the Health Information Technology and Clinical Health Act (HITECH) of the American Recovery and Reinvestment Act (ARRA), Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act (Omnibus Rule), as well as any other federal or state notification law.

II. Scope

Applies to all unsecured protected health information within the LSU HCSD system, including its PHI used by its Business Associates. Unsecured PHI can be in any form, including electronic, paper, or oral.

III. Definitions

Breach – the acquisition, access, use, or disclosure of Protected Health Information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI and is presumed to be a breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment that contains factors identified in the Omnibus Rule.

Covered Entity – A health care provider, health care clearinghouse, or health plan that transmits any health information electronically in connection with a covered transaction, such as submitting health care claims to a health plan. LSU HSCD and Lallie Kemp Medical Center are Covered Entities.

De-identified protected health information – health information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.

Limited Data Set – A subset of protected health information that excludes certain direct identifiers listed in LSU HCSD HIPAA Policy 7509. Limited data sets are treated as PHI if the data set includes zip codes or dates of birth, since there is the risk of re-identification of this information.

Organized Health Care Arrangement – means, in part, a clinically integrated care setting in which individuals typically receive health care from more than one health care provider. An example is a hospital setting where physicians are on staff at the hospital.

Protected Health Information (PHI) –for purposes of this policy means individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. Includes demographic data that relates to:

a. The individual's past, present or future physical or mental health or condition;
b. The provision of health care to the individual, or;
c. The past, present, or future payment for the provision of health care to the individual, and that identified the individual or for which there is a reasonable basis to believe it can be used to identify the individual. PHI includes many common identifiers such as name, address, birth date, social security number, etc.

Redaction- the process whereby sensitive information has been expunged (i.e., to delete, black out, or blot out sensitive information).

Unauthorized – an impermissible use or disclosure of PHI under the HIPAA Privacy or Security rule.

Unsecured protected health information – protected health information (PHI) that is <u>not</u> rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of HHS, as published on the HHS website, www.hhs.gov.

Workforce members – employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the hospital, is under the direct control of such entity, whether or not they are paid by the hospital.

IV. Policy and Procedure Statements

<u>Chapter 1 – Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.</u>

Covered Entities and Business Associates that implement the specified technologies and methodologies with respect to PHI under HITECH are not required to provide notifications in the event of a breach of such protected information. The United States Department of Health and Human Services (HHS) has described *encryption* and *destruction* as the two technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. The encryption and destruction must be in accordance with the instructions given by HITECH to qualify. If the safeguarding of the PHI

does not take one of these two forms and is breached, the Covered Entity must follow the breach notification rule of HITECH.

It is important to note that HHS has provided some clarifying points that must be considered to determine if breached PHI is reportable under the breach notification rule.

- Paper records must be destroyed in such a manner that it is no longer readable, usable, or decipherable. This means that redaction is not an acceptable method to secure paper records.
- Encryption alone will not satisfy the HITECH rule. HITECH follows the HIPAA Security rule that states that encryption keys must be kept on a separate device from the data that they encrypt or decrypt.

In order to meet the standards that would provide the level of protection discussed in the HITECH rule, the Covered Entity would have to enact the recommendations made by the National Institute of Standards and Technology (NIST) for encryption and destruction of electronically stored data.

Policy Statement 1.1.1
Taking into consideration the current resources available to LSU HCSD and to the risks posed to PHI, LSU HCSD will make every reasonable effort to provide for the security of its patients' PHI.

Chapter 2- Determining if a Reportable Privacy/Security Breach Occurred

An impermissible use or disclosure of PHI must meet certain standards to be considered a reportable breach under the HITECH Act. In general, seven standards must be considered to determine if a reportable breach has occurred.

1. Did the incident involve *impermissible* use or disclosure of PHI under the HIPAA Privacy Rule?
2. Did the incident involve *unsecured* PHI, as defined by HITECH?
3. Was the incident *intentional or unintentional* in relation to acquisition, access, or use of unsecured PHI?
4. Was the incident an *inadvertent* disclosure of unsecured PHI?
5. Was the person(s) to whom the PHI disclosed reasonably able to retain that PHI?
6. Can the Covered Entity demonstrate that there is a low probability that the PHI has been compromised based on a risk assessment?

Subunit 1 – Determining if breach involved *impermissible* use or disclosure of PHI under the HIPAA Privacy Rule.

In order to determine if a reportable breach has occurred, the Privacy Officer or his designee must first determine if the acquisition, access, use, or disclosure violates the HIPAA Privacy Rule. Such violations may include accessing PHI that is not related to the work function of the workforce member, PHI being disclosed to an individual or entity that has no right to that information, or accessing more information than is minimally necessary to perform the function of the workforce member or Business Associate.

Examples of *impermissible* uses or disclosures of PHI under the HIPAA Privacy Rule include, but are not limited to:

- Accessing CLIQ to read about an acquaintances' medical condition;
- Reading a patients' medical record out of curiosity;
- Telling a family member about the diagnosis of a neighbor;
- Accidently sending a fax about a patient's appointment to the wrong location that is not governed by the HIPAA Privacy Rule.
- Ignoring department procedure by throwing a patient's sensitive lab results in the trash can, which is then discovered at the local landfill.

Subunit 2 – Determining if the breach involved unsecured PHI, as defined by HITECH.

Unsecured PHI is PHI that is not secured through the use of technology (i.e., encryption) or methodology (i.e., destruction) that renders the PHI unusable, unreadable, or indecipherable to unauthorized individuals.

Policy Statement 2.2.1 – Analysis of the security of the PHI
The Privacy Officer or his designee must determine if the PHI was unsecured when conducting an analysis of the breach incident.

A. Electronic PHI - In conducting an analysis, it is understood that any electronic data must have been encrypted according to the National Institute of Standards and Technology (NIST) to qualify as an exception to the breach notification requirements. Those standards provide that encryption is an acceptable means to secure electronic PHI, as long as the decryption key is on a separate device. It is also understood that access controls (e.g., password enabled laptop or PDA) are not considered adequate controls to secure PHI.

B. Written PHI – In conducting an analysis, it is understood that unless the written PHI is destroyed in a manner that renders it unreadable, it is not considered secure. Redaction is not an adequate method of securing written PHI.

C. Oral PHI – In conducting an analysis, it is understood that there are instances in which an incidental disclosure is allowed under the HIPAA Privacy rule. In conducting an analysis of an oral breach of PHI, the investigator must determine if there were adequate policies to safeguard the PHI, and if these policies were reasonably followed.

Policy Statement 2.2.2 – Final determination of security of PHI

If the Privacy Officer or his designee determines that the PHI was unsecured, then the analysis needs to be taken further to determine if a reportable breach has occurred. If the analysis shows that the data was properly secured, no further action is warranted in relation to satisfying the HITECH requirements.

Subunit 3 – Determination if PHI of the breach was intentionally or unintentionally acquired, accessed, or used or disclosed.

The HITECH Act provides an exception to its breach reporting rule if the PHI was *unintentionally* acquired, accessed, or used by a member of its workforce or a person acting under the authority of the facility or its Business Associate. In order to qualify for this exception, not only must the access be unintentional, but the access must also:

- Be done in good faith (i.e., not intentionally trying to access PHI for purposes other than what is allowed by the HIPAA Privacy rule)
- Be done within the course and scope of the workforce member's authority; and
- Not be further used or disclosed in a way that violates the HIPAA Privacy rule.

An example of an unintentional access that meets these criteria would be a nurse that intends to access the CLIQ records of a patient under her care, but unintentionally accesses another patient's information by mistake. The nurse immediately realizes her mistake and gets out of the account she has mistakenly accessed.

NOTE: This exception does <u>not</u> include any unintentional <u>disclosures</u>. But it does provide for *inadvertent* disclosure of PHI in certain circumstances. See Subunit 5.

Policy Statement 2.3.1

The Privacy Officer must determine if all of the components under this section are met in the case of a breach in which PHI was acquired, accessed, or used. If the access is found to be intentional, or not meet one of the components, then the analysis must continue. If the analysis shows that the breach was unintentional

and meets the exceptions noted, then no further action is warranted in relation to satisfying the HITECH requirements.

Subunit 4 – Determining if the breach was an inadvertent disclosure.

The HITECH Act does not consider a breach reportable if the following criteria are met:

- The person who originally accessed the PHI was authorized to do so; and
- The PHI was disclosed to another person authorized to access PHI at the same Covered Entity or the same Business Associate, or within an organized health care arrangement in which the Covered Entity participates; and
- The PHI was not further used or disclosed in a way that violates the HIPAA Privacy rule.

Note that an organized health care arrangement includes the hospital, and the health care providers who have staff privileges at the hospital. Therefore, a disclosure from the hospital to one of its medical staff members is not considered a reportable breach if the criteria under this section are met.

Policy Statement 2.4.1

The Privacy Officer or his designee must determine if all of the components under this section are met in the case of an inadvertent disclosure of unsecured PHI. If the criteria are found to be met, no further action is required under the HITECH Act. If the criteria are not met, and there was an inadvertent disclosure, then further analysis is required.

Subunit 5 – Determining if an unauthorized person to whom PHI was disclosed would reasonably have been able to retain the information.

The HITECH Act does not consider a breach reportable if the unauthorized person who received the information was not able to access or retain the information. For example, if an appointment notice was mailed to the wrong patient, and the notice returned unopened, it would be reasonable to state that no one accessed or retained the PHI enclosed in the mailing.

Policy Statement 2.5.1

The Privacy Officer or his designee must determine if anyone was able to access and retain the PHI involved in the breach. If the PHI was not able to be retained, then no further action is required under the HITECH Act. If the PHI was able to be retained, then further analysis is required.

Subunit 6 – Determining the probability that the PHI has been compromised based on a risk assessment.

If it is determined that PHI has indeed been breached, and that all other criteria related to a reportable breach have been met, a risk assessment must be completed to determine the probability that the PHI has been compromised.

The risk assessment must review the following factors:

1. **The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification** – The type of PHI involved in the breach should be considered, including if the PHI was more sensitive in nature.

    a. Financial data would be considered more sensitive if the information increases the risk of identity theft or financial fraud. Social security numbers and credit card numbers would be examples of highly sensitive data.
    b. Clinical data would be considered more sensitive if there is significant clinical data that was breached and the detail of that data. It is important to note that clinical information that is considered sensitive is more than just data related to sexually transmitted diseases, mental health, and substance abuse.
    c. The Covered Entity should consider the probability that the PHI breached could be used by an unauthorized person in a manner adverse to the patient or otherwise used to further the unauthorized recipient's own interests.
    d. In situations where minimal direct identifiers were breached, Covered Entities should determine whether there is a likelihood that the PHI released could ever be re-identified based on the context and the ability to link the information with other possibly available information.

2. **The unauthorized person who used the PHI or to whom the disclosure was made –** Does the unauthorized person have obligations to protect the privacy and security of the PHI? If so, then there is a less likely probability of compromise to the PHI.

3. **Whether the PHI was actually acquired or viewed** – Was there an actual acquisition/viewing of PHI, an opportunity for such viewing, or was there no access at all.

4. **The extent to which the risk to the PHI has been mitigated** – Covered Entities should attempt to mitigate the breach if possible, by obtaining the unintended recipient's satisfactory assurances that the information will not

be further used or disclosed (through a confidentiality agreement or similar means), will be destroyed, etc. It is important to note that assurances by a person governed by HIPAA would be more satisfactory than certain third parties who are not governed by such laws.

HITECH requires that each risk assessment be documented, so that the Covered Entity can demonstrate, if necessary, that no breach notification was required following an impermissible use or disclosure of PHI. It is important to note that the Covered Entity has the burden of proof of explaining why a breach would not be considered a reportable breach. HITECH does not require a documented risk assessment to determine the probability that PHI has been compromised if the Covered Entity has already made the decision that the breach should be reported.

Policy Statement 2.6.1

The Privacy Officer, with the assistance of other departments if needed, shall conduct a documented risk assessment to determine the level of probability of compromised PHI in relation to the privacy/security breach. If the breach is found to have greater than a low probability of compromised PHI, and all other analysis indicates that the breach is a reportable event, then the Privacy Officer, or his/her designee, shall move forward with notification procedures. If the breach is determined to be of low probability to compromise the PHI of the patient, then no further action other than documenting the analysis is required under HITECH. Note: Additional factors may also be considered in determining the probability of compromise to the PHI, based on the circumstances of the case.

Subunit 7 – Documentation of analysis/risk assessment of privacy/security breach incident

HITECH maintains that a Covered Entity has the burden of proof for showing why a breach notification was not required. Therefore, the Covered Entity must document its decision making process when it determines that a breach is not to be reported.

Policy Statement 2.7.1

The Privacy Officer, with assistance from other departments as warranted, will conduct an analysis/risk assessment to determine if a reportable privacy/security breach has occurred. The analysis will consider the standards noted in this chapter. Any analysis conducted must be documented and kept on file for a minimum of ten years.

Chapter 3 – Notification of Breach to Individuals

If a reportable breach has been determined to have occurred, it is the responsibility of the Covered Entity to notify each of the individuals affected by that breach. The HITECH Act specifies how that notification should occur.

Subunit 1 – Timeliness of Notification

Individuals must be notified of the breach of their unsecured PHI no later than sixty (60) days after the discovery of the breach. A discovery of a breach is defined as occurring once the covered entity has knowledge of the breach, or by exercising reasonable diligence, would have known that the breach had occurred. A breach shall be treated as discovered by a Covered Entity or by a Business Associate as of the first day on which such a breach is known to the Covered Entity or Business Associate. HITECH recognizes that the person who committed the breach may not report it. Therefore, the discovery of a breach is not considered known by the Covered Entity if the only member of the workforce who knows about the breach is the workforce member who committed the breach.

In addition, a breach is considered discovered when the incident becomes known, not when the Covered Entity or Business Associate's investigation of the incident is complete. This is the case even if it is initially unclear whether the incident constitutes a breach as defined in this policy.

The actual date of the breach must also be identified and documented.

HITECH does allow up to sixty calendar days after discovery to notify individuals of the breach. However, such notification must be made without reasonable delay. Therefore, if the covered entity has all of the information it needs to notify individuals of reportable breach, the Covered Entity must do so at that time, and not postpone notification up until the sixtieth day.

Policy Statement 3.1.1

LSU HCSD entities must notify any individual(s) impacted by a reportable breach as soon as possible without reasonable delay, but in no case later than sixty days of the discovery of the reportable breach.

Subunit 2 – Method of Notification

In any case of a reportable breach, the individual(s) whose PHI was compromised must be notified in writing by first-class mail to the last known address of that individual. The written notification may be sent to the patient's personal representative in cases that contact information specifies that the patient's personal representative acts on behalf of the patient. In cases in which the PHI

has been compromised on deceased individuals, the written notification may be sent to the last known address of next of kin.

If there is reason to believe that the patient's PHI is in imminent danger of misuse, the Covered Entity may choose to send written notification via first-class mail and contact the patient by other means such as phone or email. However, in all cases, one of the methods of contacting the patient must be written notification via first-class mail.

Policy Statement 3.2.1

The Covered Entity will notify any patients of a reportable breach through a written notification sent first-class mail. If there is reason to believe that the patient's information is in imminent danger of being misused, the Covered Entity will attempt to contact the patient via phone in addition to sending a written notification.

Subunit 3 – Insufficient Contact Information for Less than Ten Patients

If the Covered Entity does not have sufficient contact information for less than ten individuals affected by the breach, or if less than ten mailed notices are returned as undeliverable, the Covered Entity must provide substitute notice to the unreachable individuals. The substitute notice should be provided as soon as reasonably possible after the Covered Entity is aware that it has insufficient or out-of-date contact information for one or more affected individuals. Whatever form of substitute notice is provided (e.g., phone call, email address, posting on facility web site), the notice must contain all of the elements of an initial notice stated in Subunit 7 of this chapter. With respect to decedents, however, the Covered Entity is not required to provide substitute notice for the next of kin or personal representative in cases where the Covered Entity does not have contact information nor has out-of-date contact information for the next of kin or personal representative. It is also not appropriate to send breach notifications to a deceased individual's emergency contact where such a person is not a personal representative or next of kin of the decedent.

Policy Statement 3.3.1

If the mailed breach notice is returned indicating that the last known address was insufficient or inaccurate, an attempt will be made to contact the patient via the last known phone number of the patient. If the phone number is found to be inaccurate or no longer in service, the Privacy Officer or designee will attempt to locate the patient via contact persons listed by the patient, taking care not to further breach PHI. Every effort will be made to contact the patient via these methods.

The fact that the mailed breach notice was returned, and the steps taken to contact the patient must be documented.

Subunit 4 – Insufficient Contact Information for Ten or More Patients

If the Covered Entity has insufficient or out-of-date contact information for ten or more individuals related to any one specific reportable breach, the Covered Entity must provide substitute notice through either a conspicuous posting of the breach on its home page of its web site (landing or log-in page) for ninety days, or place a notice of the breach in major print or broadcast media in geographic areas where the individuals affected by the reportable breach likely reside. These substitute notifications must be provided in a manner that is reasonably calculated to reach the affected individuals. This substitute notice must contain a toll-free phone number, active for a minimum of ninety days, where an individual can learn whether the individual's unsecured PHI may be included in the breach.

Note that it is acceptable for the Covered Entity to attempt to update the contact information so that they can provide direct written notification, in order to limit the number of individuals for whom substitute notice is required, and thus, potentially avoid the obligation to provide substitute notice through a web site or major print or broadcast media. However, the notification through this method has to occur as soon as possible, but in no case later than sixty days from the discovery of the breach.

Policy Statement 3.4.1

If any one particular breach has ten or more individuals who cannot be contacted via their contact information listed in the covered entities' system, then every reasonable attempt should be taken to update the information. However, if after a reasonable period of time it becomes evident that such information will not be able to be updated for ten or more individuals impacted by the breach, then the facility must determine which alternate method of notification (e.g., posting on the facility's website or notification through major media) will be used to reasonably reach those whose PHI has been breached. This notification must occur as soon as possible, but no greater than sixty days from the discovery of the breach.

Subunit 5 – Notification to the Media When More than 500 Patients are Involved in the Breach.

HITECH requires that whenever there is a reportable breach that involves 500 persons or more in any given State or jurisdiction, that major media outlet that serve those States or jurisdictions be notified of the reportable breach. This notification of the media is in addition to the individual notice requirements outlined in Chapter 3, Subunit 2.

Such notification of the media is required to occur within sixty calendar days after the discovery of the breach.

The notice to the media must contain the same information as required under the individual written notification, found in Subunit 7 of this Chapter.

Policy Statement 3.5.1

When a reportable breach involves 500 or more patients from a particular State or jurisdiction, the major media outlet in that area will be sent a press release of the reportable breach, outlining the required elements of a breach notification.

Subunit 6 – Notification of the Reportable Breaches to the United States Secretary of the Department of Health and Human Services (HHS)

HHS requires that Covered Entities report any breaches meeting the criteria in the HITECH Act as reportable breaches to their office. This reporting requirement is in addition to the notifications already described in this chapter. The timing of the notification depends on how many individuals are impacted in any one breach incident.

If any one breach involves 500 or more patients from a particular State or jurisdiction, the notice to HHS must be sent without reasonable delay but in no case later than sixty calendar days following the discovery of the breach. Notification to the Secretary of HHS should be contemporaneous to the notification of media and to those impacted.

If any one breach involves less than 500 individuals from a particular State or jurisdiction, the Covered Entity must maintain a log of the reportable breaches and annually submit the information from the log to HHS for the preceding year. This information must be submitted no later than sixty days after the end of each calendar year. For calendar year 2009, the Covered Entity is only required to submit information to HHS for reportable breaches occurring on or after September 23, 2009.

Policy Statement 3.6.1

The Privacy Officer will maintain a log of all reportable breaches in the access data base that logs all compliance contacts. All required information that must be reported to HHS will be stored in this data base for each reportable breach. At the end of the calendar year, the information related to the reportable breaches will be entered into the HHS website no later than sixty days after the end of each calendar year.

In any instance of a breach that involves 500 or more patients from a particular State or jurisdiction, the Privacy Officer will contact HHS in the method prescribed by the HHS web site to notify them of the breach.

Subunit 7 – Content of the Notice of the Reportable Breach

The HITECH Act prescribes the contents of written notification of reportable breaches that must be sent to individuals whose PHI has been compromised. The written notification must contain:

- A brief description of what happened
- The date of the breach
- The date of the discovery of the breach
- The types of unsecured PHI that were involved in the breach (not the actual information itself)
- The steps the individual should take to protect themselves from potential harm (e.g., contacting credit reporting agencies)
- What the Covered Entity is doing to investigate the breach, mitigate the harm to the individual, and to protect against any further breaches
- The contact procedures for individuals to ask questions or learn additional information. A toll-free telephone number, an email address, web site or postal address must also be included.

This notice must be written in plain language, as well as provide effective communication for all individuals involved in the breach (e.g., in their native language, or to account for any disability that they may have).

Policy Statement 3.7.1

The Privacy Officer shall provide a letter for distribution that provides the information content required in the HITECH Act. The Covered Entity shall provide resources to complete the mailing of any such notification, particularly in cases where multiple patients are involved in a reportable breach. A template of this letter may be found in Appendix A (NOTE: The template letter is written with Lallie Kemp Medical Center as the Covered Entity, but LSU HCSD may be substituted if the breach occurs at LSU HCSD.

Subunit 8 – Law Enforcement Delay

HITECH provides that if a law enforcement official determines that a notification, notice, or posting required by the Rule would impede a criminal investigation or cause damage to national security, such notification may be delayed in the same manner as provided under 45 CFR 164.528(a)(2) of the HIPAA Privacy rule. In this case, the Covered Entity or Business Associate would be required to temporarily delay the notification.

If the law enforcement official provides a statement in writing that the delay is necessary for a specific period of time because notification would impede a criminal investigation or cause damage to national security, the Covered Entity is required to delay the notification for the time period specified by the official.

If the law enforcement official states orally that a notification would impede a criminal investigation or cause damage to national security, the Covered Entity is required to document the statement and the identity of the official. In such cases, the notification may only be delayed for up to thirty (30) days, unless a written statement meeting the above requirements is provided during that time.

Subunit 9 – Notification to Patients Who May React with Anguish or Severe Distress

In situations where a health care provider believes that a written breach notification to a patient may cause extreme anguish or distress, based on the patient's mental state or other circumstances, the health care provider may telephone the patient prior to the mailed breach notification or have the patient come to the health care provider's office to discuss the situation. However, the breach notification must still be mailed without delay and in accordance with this policy.

Chapter 4 – Reportable Breaches by Business Associates

The HITECH Act also holds Business Associates responsible for the breach notification rules. HITECH requires all Business Associates to notify the Covered Entity of the breach. It is then the Covered Entity's responsibility to follow through on notifying the individuals or authorities, as outlined in this policy.

Subunit 1 – Timeliness of Notification

The HITECH states that a Business Associate must provide notice of a breach of unsecured PHI to a Covered Entity without reasonable delay and in no case later than sixty days following the discovery of the breach.

If a Business Associate is acting as an agent of the Covered Entity, the Covered Entity must meet the notification requirements outlined in this policy from the date the breach is discovered by the Business Associate.

If the Business Associate is an independent contractor of the Covered Entity (i.e., not an agent), then the Covered Entity must provide notifications as described in this policy based on the time the Business Associate notifies the Covered Entity of the breach.

Because of the time limitations of breach notification, LSU HCSD will require its Business Associates to notify it immediately upon discovery of the breach, but in no case later than ten calendar days, with limited exceptions.

The Business Associate Agreement will outline the contact person that the Business Associate must contact when a reportable breach discovery is made. In most cases, the contact person will be the Privacy Officer and Hospital Administrator (or designee) of the individual LSU HCSD hospital that has contracted with the Business Associate. In the case of LSU HCSD system contracts, a Privacy Officer will be named in the agreement for processing purposes, as well as a LSU HCSD Senior Manager (or designee).

Subunit 2 – Information Provided by Business Associate to the Covered Entity

A Business Associate must provide the following information (to the extent possible) to the Covered Entity when a reportable breach has occurred within the Business Associate's operations:

- The identity of each individual whose unsecured PHI has been, or is reasonably believed to have been breached.
- Any other available information that the Covered Entity is required to include in its notification to the individual, either at the time it provides notice to the Covered Entity of the breach or promptly thereafter as information becomes available. Note that a Business Associate should provide this information even if it becomes available after notifications have been sent to affected individuals or after the sixty day notification period has elapsed.

Policy Statement 4.1

LSU HCSD will require a Business Associate Agreement (BAA) for all of its Business Associate contracts. The BAA will include requirements related to notifying LSU HCSD of any reportable breach, as well as assurances that the Business Associate is meeting the requirements of the HIPAA Privacy, Security and HITECH regulations.

Subunit 3 – Notification to Covered Entities When LSU HCSD is the Business Associate Responsible for a Breach

LSU HCSD may function as a Business Associate in certain circumstances. If a breach occurs in the course of performing its Business Associate functions, LSU HCSD must send written notification to the Covered Entity. Such notification will include the required elements outlined in Subunit 2.

Chapter 5 – Notification of Relators in Grievances When There is No Confirmation of a Breach

Though the Breach Notification regulations only require Covered Entities to send a letter when there is a confirmation of a reportable breach, it is the policy of LSU HCSD to communicate the final findings to the relator of any HIPAA grievance brought to the Privacy Officer's attention as it would a formal patient or patient representative grievance. However, due to the nature of HIPAA investigations, the Privacy Officer has sixty (60) days from the date of the initial notification of the concern to send such a letter.

Policy Statement 5.1

LSU HCSD will send a letter to the relator of any HIPAA concern brought to the Privacy Officer's attention as it would a formal patient or patient representative grievance, within sixty (60) days from the initial notification of the HIPAA concern. The grievance may initially be brought to the Hospital's Patient Advocate, or may come directly to the Privacy Officer. In either instance, the Privacy Officer will send a letter to the relator when the concern cannot be validated, or is not considered a reportable breach.

Policy Statement 5.2

The content of such a letter will contain the following, if applicable, to the complaint situation:

- A brief description of what happened
- The date of the alleged breach
- What the Covered Entity is doing to investigate the breach, and to protect against any further breaches
- An explanation as to why the breach could not be validated
- Action to mitigate the harm to the individual, including an apology to the relator
- The contact procedures for individuals to ask questions or learn additional information. A toll-free telephone number, an email address, web site or postal address must also be included.

Chapter 6 – Additional Requirements of the HITECH Act

Subunit 1 – System to Detect Reportable Breaches

Because a Covered Entity or Business Associate is liable for failing to provide notice of a reportable breach when the Covered Entity or Business Associate did not know - but by exercising reasonable diligence would have known – of a breach, it is important for such entities to implement reasonable systems for the discovery of breaches.

Policy Statement 6.1.1

Each LSU HCSD entity shall develop procedures to reasonably detect reportable breaches. Breaches related to faxes, electronic health record data bases or billing systems, paper medical records should be considered, as well as other identified risks as they become known. Any detection of a breach as a result of these systems shall be reported immediately to the entity's Privacy Officer.

Subunit 2 – Training of Workforce

HITECH states that once a member of the Covered Entity or Business Associate's workforce becomes aware of a potential breach, the clock begins on the amount of time the entity has to make the notifications required by the Rule. Therefore, the Covered Entity must ensure that their workforce members and other agents are adequately trained and aware of the importance of timely reporting of privacy and security incidents and the consequences of doing so.

Policy Statement 6.2.1

Each LSU HCSD entity shall ensure that its workforce members and agents attend training concerning their role in the HITECH Rule requirements on at least an annual basis.

Subunit 3 – Accounting of Disclosure

HITECH requires that the Covered Entity maintain an accounting of disclosure as a result of a reportable breach.

Policy Statement 6.3.1

Each LSU HCSD entity shall ensure that there is an accounting of any disclosure that occurs as a result of a reportable breach in a manner that is consistent with recording other disclosures.

Subunit 4 – Complaints

All Covered Entities must provide a process for an individual to complain about its compliance with the Breach Notification Rule.

Policy Statement 6.4.1

Each LSU HCSD Facility has named a Patient Advocate whose responsibility includes addressing complaints and concerns related to patient privacy. This would include complaints and concerns about the Facility's compliance with the Breach Notification Rule.

Subunit 5 – Sanctions

All Covered Entities are required to sanction workforce members for failing to comply with the Breach Notification Rule.

Policy Statement 6.5.1

Workforce members are trained to notify the Privacy Officer in the case of an impermissible use or disclosure. Failure to comply with any section of the HIPAA regulations may result in disciplinary action. The action taken depends on the circumstances of the failure to comply.

Subunit 6 – Refraining from Retaliatory Acts

Covered Entities are required to have policies and procedures prohibiting retaliatory acts against those who report a Breach Notification violation, for those who exercise their rights under the Breach Notification Rule, for those who assist in an investigation by HHS or other appropriate authority, and for those who oppose an act that the person believes in good faith violates the Breach Notification Rule.

Policy Statement 6.6.1

Each LSU HCSD Facility has procedures in place to protect individuals who, in good faith, report violations in federal or state law, or LSU HCSD policy. LSU HCSD Compliance Policy 8505 outlines these protections. In addition, no patient or other individual exercising his or her rights under HIPAA, shall be penalized in any way.

Subunit 7 – Waiver of Rights

Covered Entities are prohibited from requiring an individual to waive any rights under the Breach Notification Rule as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Policy Statement 6.7.1

LSU HCSD never requires any individual to waive any rights under HIPAA, including the Breach Notification Rule in any circumstance.

Chapter 7 – Notification of LSU HCSD Senior Leadership of Reportable Breaches

Whenever it has been determined that a reportable breach has occurred at the LSU HCSD hospital level, it is the responsibility of the Privacy Officer to notify Senior Leadership of the breach. If the breach occurs at Lallie Kemp Medical, the Hospital Administrator, in turn, shall notify LSU HCSD Senior Leadership of the reportable breach. LSU HCSD Senior Leadership, at a minimum, is defined as the Deputy Chief Executive Officer, and the Medical Director.

Chapter 8 – Louisiana Security Breach Notification Law

The State of Louisiana has the "Database Security Breach Notification Law", R.S. 51:3071- 51:3075, that requires notification to any Louisiana resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized persons as a result of a security breach. This law must be considered any time there is a potential compromise of computerized data.

This law may come into play if there is a breach of personal information that is not considered PHI, but rather PII (personally identifiable information not related to health data as defined by HIPAA).

In this law, **personal information** is defined as 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 or 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.
- Passport number.
- Biometric data, defined as data generated by automatic measurements of an individual's biological characteristics, such as finger prints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

In this law, a **security breach** is a compromise of the security, confidentiality, or integrity of computerized data that results in, or there is reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal

information. Good faith acquisition of personal information by an individual is not a breach of the security of the system, provided that the personal information is not used for, or subject to, unauthorized disclosures.

Notification under this law must be made in the most expedient time possible and without reasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system. Such notification shall be made no later than sixty days from the discovery of the breach unless there is a legitimate delay to meet law enforcement needs. If notification must be delayed at the written request of law enforcement, LSU HCSD must provide written notification to the Louisiana Attorney General within the sixty days from the discovery of the breach.

Notification is not required if after a reasonable investigation it is determined that there is no reasonable likelihood of harm to customers.

Chapter 9 – Additional Notification Requirements

Louisiana R.S. 24:523 requires immediate written notification of the Louisiana legislative auditor and the district attorney of the parish in which the agency (i.e., LSU HCSD) is domiciled, of any possible misappropriation of public assets. Cyberattacks and other potential large breaches where there is a potential of monetary liabilities are considered a misappropriation of public assets.

V. Consequences

Any employee, faculty, staff, or agent of LSU HCSD found to be in violation of the provisions of the LSU HCSD HIPAA Privacy Policies, LSU HCSD Information Security Policy, the LSU HCSD Breach Notification Policy, or other policies that provide for the security of patients' protected health information, will be subject to appropriate disciplinary action, up to and including termination of employment, enrollment, or contract.

Appendix A- Notification Letter Template -

Appropriate Letterhead

Date

Name and Address of Impacted Individual

Dear (*fill in name of impacted individual),*

Lallie Kemp Medical Center has become aware of the fact that your Protected Health Information (PHI) has been (*inappropriately accessed or disclosed).* Under the Health Insurance Portability and Accountability Act (HIPAA), we are obligated to alert you in an instance where we believe your PHI has been breached.

The breach was discovered (*date of discovery)* (*brief description of what happened that caused the breach).* The breach occurred *(date of the breach).* The PHI that was available for view included *(list all PHI that was breached).*

(List the actions taken by Lallie Kemp to investigate the breach). (List the actions taken by Lallie Kemp to protect against any similar breaches in the future). (List the actions that should be taken by Lallie Kemp to mitigate potential harm caused the breach). (List actions that should be taken by the patient to protect himself/herself from potential harm).

Lallie Kemp Medical Center sincerely regrets any inconvenience or concern that this incident may cause you. Lallie Kemp Medical Center has strict privacy and security policies in place concerning HIPAA. Employees are mandated to attend training upon hire and annually thereafter, and are continuously reminded about the importance of the confidentiality of patient information.

Should you have any questions or need to speak to someone at Lallie Kemp Medical Center, please contact our Compliance/Privacy Officer, at 985-878-. You may also call our Compliance Hotline at 1-800-735-1185.

Sincerely,

Chief Executive Officer – Lallie Kemp Medical Center

cc: Compliance and Privacy Officer

Document Metadata

Document Name:	8515 - 21 Breach Notification.doc
Policy Number:	8515
Original Location:	/LSU Health/HCSD/8500 - Compliance
Created on:	01/24/2020
Published on:	07/06/2021
Last Review on:	06/21/2021
Next Review on:	06/21/2022
Effective on:	02/01/2011
Creator:	Reeves, Rebecca *Compliance and Privacy Officer*
Committee / Policy Team:	Main Policy Team
Owner/SME:	Simien, Tammy *Staff Attorney*
Manager:	Reeves, Rebecca *Compliance and Privacy Officer*
Author(s):	Wicker, Claire M. *PROJECT COORDINATOR*
Approver(s):	Simien, Tammy *Staff Attorney* Buie, Lanette *Chief Operations Officer*
Publisher:	Wicker, Claire M. *PROJECT COORDINATOR*

Digital Signatures:

Currently Signed

Approver:
Buie, Lanette
Chief Operations Officer

07/06/2021

Approver:
Simien, Tammy
Staff Attorney

07/06/2021