LOUISIANA HEALTH CARE QUALITY FORUM

POLICY: Data Breach Notification and Investigation	**EFFECTIVE: 10-01-2011**
DEPARTMENT: LHCQF; LaHIE	**REVISED:**

PURPOSE

To facilitate compliance with the Health Information Technology for Economic and Clinical Health Act (HITECH) component of the American Recovery and Reinvestment Act of 2009 (ARRA) breach notification and investigation of unsecured protected health information (PHI) requirements.

DEFINITIONS

The following definitions apply to all of LHCQF's privacy and security policies and procedures:

1. **Breach** – Unauthorized acquisition, access, use, or disclosure of unsecured, unencrypted protected health information which compromises the security or privacy of such information and poses a significant risk of financial, reputational, or other harm to the individual. To determine if a notification is required, a risk assessment must be performed to determine if the security or privacy of the PHI has been compromised (see Appendix A). The term 'breach' does not include:
    a. Any unintentional acquisition, access, or use of PHI by a workforce member or individual acting under the authority of a covered entity or business associate if
        i. Such acquisition, access, or use was made in good faith and within the course and scope of authority;
        ii. Such information is not further used or disclosed in a manner not permitted; or
        iii. Any inadvertent disclosure by a person who is authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates; and any such information received as a result of such disclosure is not further used or disclosed in a manner not permitted; or
        iv. A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2. **Protected Health Information** – Any oral, written or electronic individually-identifiable health information collected or stored by a covered entity or business associate. Individually-identifiable health information includes demographic information and any information that relates to past, present or future physical or mental condition of an individual.

3. **Unsecured PHI** - Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology

specified by the U. S. Secretary of the Department of Health and Human Services (HHS). At this time, the only technology is encryption; the only methodology is destruction.

PROCESS

1. Any Participant and/or LHCQF employee and/or support personnel in the case of a breach of unsecured PHI must notify LHCQF Executive Director or designee upon suspicion or knowledge of a breach within 24 hours.

2. If notification is received from a LHCQF employee or support personnel and the breach involves a customer's PHI, the Executive Director shall coordinate with the appropriate LHCQF Client Executive to provide notification to the customer's Compliance and/or Privacy/Security Officer without unreasonable delay.

3. A breach is considered discovered as of the first day on which the breach is known by the Participant and/or LHCQF employee or support personnel.

4. If a law enforcement official determines that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, such notification, notice or posting shall be delayed in the same manner as provided under §164.528(a)(2) of title 45, Code of Federal Regulations.

5. If a data breach occurs involving a customer's PHI, LHCQF's Executive Director or her designee will provide the same information as in the Content of Notification (below) to the customer's Compliance and/or Privacy Officer without unreasonable delay for completion of the risk assessment and determination of notification.

6. Participants and LHCQF/LaHIE are responsible for immediately investigating and mitigating to the extent possible, any privacy and/or security breach that they become aware of. They shall immediately:
    a. Investigate the scope and magnitude of the breach.
    b. Identify the root cause of the breach.
    c. Mitigate the breach to the extent possible.
    d. Notify all appropriate parties, i.e. LHCQF Executive Director, Participant's Privacy and Security Officers, etc., within 24 hours of actual knowledge and the potential impact of the breach.
    e. In the event that the breach involves or may involve more than one Participant, Participants shall cooperate with LaHIE and other Participant(s) in investigating and mitigating the breach, including but not limited to sharing any information that may be

necessary in connection with such investigation and/or mitigation, subject to all applicable laws and regulations.

f. Notify regulatory agencies and customers in compliance with all applicable state and federal laws, rules and regulations.
g. Notify individuals affected by the breach as required by HIPAA.

7. LHCQF Health IT Director will provide a report of the breach and mitigation actions to the LHCQF Executive Director, its Legal Counsel, and LHCQF Board of Directors.

8. LHCQF shall maintain a log of any breaches meeting the HITECH definition that occur during a calendar year. This documentation must be retained for a period of six years.

Content of Notification

The notice of the breach must include:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

2. A description of the type of unsecured PHI that were involved in the breach, such as full name, Social Security Number, date of birth, home address, account number, diagnosis code or disability code. Only the generic type of PHI should be listed in the notice (i.e., date of birth rather than the patient's actual birth date).

3. The steps the individual should take to protect themselves from potential harm resulting from the breach.

4. A brief description of what LHCQF is doing to investigate the breach, mitigate harm to the individual, and to protect against further breaches.

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

APPROVAL:

Cindy Munn
Executive Director
Louisiana Health Care Quality Forum

LOUISIANA HEALTH CARE QUALITY FORUM

GENERAL BREACH PROCESS INFORMATION FOR COVERED ENTITIES

Breach Notification Process

Patient Notification

1. After a complete investigation, no later than 60 days from breach discovery, the covered entity must provide written notice to the patient or:
    a. If the patient is deceased, the next of kin or personal representative.
    b. If the patient is incapacitated/incompetent, the personal representative.
    c. If the patient is a minor, the parent or guardian.

2. Written notification must be in plain language at an appropriate reading level with clear syntax and language with no extraneous materials. Americans with Disabilities Act (ADA) and Limited English Proficiency (LEP) requirements must be met.

3. Written notification must be sent to the last known address of the patient or next of kin, or if specified by the patient, by encrypted electronic mail. The template letter in the HITECH Breach Notification Reporting Process must be used when sending written notification to a patient, personal representative, or next of kin.

4. In the case where there is insufficient or out-of-date contact information:
    a. For less than ten (10) individuals that precludes direct written notification to the patient, a substitute form of notice shall be provided such as telephone call.
    b. In the case that there are ten (10) or more individuals for which there is insufficient or out-of-date contact information and contact information is not obtained, the covered entity must:
        i. Post a conspicuous notice for 90 days on the homepage of their website that includes a toll-free number; or
        ii. Provide notice in major print or broadcast media in the geographic area where the patient can learn whether or not their unsecured PHI is possibly included in the breach. A toll-free number must be included in the notice.

5. If the covered entity's Compliance Officer, in concert with the Legal Department/Team, determines a patient should be notified urgently of a breach because of possible imminent misuse of unsecured PHI, the covered entity may, in addition to providing notice as outlined in steps 2-4 above, contact the patient by telephone or other means, as appropriate.

Media Notification

1. In the case where a single breach event affected more than 500 residents of the same State or jurisdiction, notice shall be provided to prominent media outlets. A jurisdiction is defined as a geographic area smaller than a state (e.g., city, county). For example, if a single breach event

affects 200 patients in Texas and 400 patients in Louisiana, a notice to the media is not required because there were not more than 500 patients in the same State or jurisdiction affected. However, if a single breach event affects 500 patients in Texas and 500 patients in Louisiana, a media notice is required in both Texas and Louisiana.

2. The covered entity's Compliance Officer shall work with the Legal Department/Team and the Chief Executive Officer to coordinate the notification.

HHS Notification

1. Notice must be provided by the covered entity without reasonable delay and in no case later than 60 days from the breach discovery to the U. S. Secretary of the Department of Health and Human Services (HHS) if a single breach event was with respect to 500 or more individuals regardless of the State or jurisdiction. The covered entity must use the electronic form available on the HHS website when notifying HHS of breaches involving 500 or more individuals.

2. If a breach is with respect to less than 500 individuals, the covered entity must use the electronic form available on the HHS website and submit to HHS no later than 60 days after the end of the calendar year in which the breach occurred.

3. The covered entity must maintain a log of any breaches meeting the HITECH definition that occur during a calendar year. This documentation must be retained for a period of six years.

LOUISIANA HEALTH CARE QUALITY FORUM

APPENDIX A

Assessment of the Risk of Harm to the Individual

from a Violation of the Privacy Rule under HIPAA and the HITECH Act

Violations of the HIPAA Privacy Rule are evaluated for the potential for significant risk of financial, reputational, or other harm to the individual whose information was compromised. This risk assessment is completed and documented for every violation of the Privacy Rule involving unauthorized acquisition, access, use or disclosure of unsecured PHI that does not fit within an exception defined in the HITECH Act. When a violation is determined to result in significant risk of harm to the individual, notification to the individual and to the Secretary of HHS is required.

The following general framework is used to assess for risk depending upon the specific facts associated with the risk in order to determine whether breach notification is required.

1. Who are the parties involved in the incident?

   a. Is the individual who impermissibly used/disclosed the information an LHCQF employee?

Lo	(1)	LHCQF employee otherwise authorized to access the PHI
Lo	(1)	LHCQF employee not otherwise authorized to access the PHI
Med	(2)	Non LHCQF employee accessed/used/disclosed the PHI

   b. Who received the disclosed PHI?

Lo	(1)	Another LHCQF employee not defined in the exceptions to breach
Lo	(1)	An individual that is a covered entity or a business associate
Med	(2)	An individual that is not bound by HIPAA and external to LHCQF

2. What type(s) of information was disclosed?

   a. Limited Data Set

N/A	(0)	Not a Limited Data Set
Lo	(1)	16 HIPAA defined identifiers removed and also either no date of birth (DOB) or no zip code
Lo	(1)	16 HIPAA defined identifiers removed and age or zip codes do not create identifiable populations
Med	(2)	16 HIPAA defined identifiers removed, but ages or zip codes make re-identification possible

b. Direct Patient Identifiers

	N/A	(0)	No direct identifiers were disclosed
	Lo	(1)	Full name or partial name, but no contact demographic information (such as address or phone), may include medical record number but no Social Security number (SSN) or DOB
	Med	(2)	Name with phone number or address but no SSN or DOB
	Med	(2)	Full name with DOB
Mandatory	HI	(3)	SSN (or credit card or bank account number) with first initial or first name and last name

c. Type of services provided

	N/A	(0)	No information regarding health services or care disclosed
	Lo	(1)	Identified as patient of an LHCQF customer or customer's provider
	Med	(2)	Reason for receiving care; diagnosis or treatment; or test results disclosed
Mandatory if any of 2 b applies	HI	(3)	"Sensitive" treatment revealed by location or a condition that might result in employment discrimination or reputational harm (e.g. HIV, Cancer, Substance Abuse, genetic disorders)

3. <u>What is the likelihood of unauthorized use or disclosure of the PHI?</u>

a. Lost or Stolen Device with ePHI

N/A	(0)	Not applicable
Lo	(1)	Device retrieved before it was accessed or device encrypted
Med	(2)	Device is known to be password protected but not encrypted
Hi	(3)	Device not known to be encrypted

b. Paper Media Breached (e.g. lost, stolen, faxed, or mailed)

N/A	(0)	Not applicable
Lo	(1)	Information is returned without seal on envelope being broken
Med	(2)	PHI is disclosed to someone who does not know the patient and who provides assurance the information has been returned and/or destroyed
HI	(3)	PHI is disclosed to someone who may know of the patient and who is reasonably believed to have accessed the information

LOUISIANA HEALTH CARE QUALITY FORUM

Risk Assessment Scoring Grid

Question	Score	Notes
1 a.		
1 b.		
2 a.		
2 b.		
2 c.		
3 a.		
3 b.		
TOTAL		
KEY:	0-7	Low Risk of Harm to the Individual (notification not required)
	8 – 9	Medium Risk of Harm to the Individual (notification may be required; determined by business leader and Privacy Office based upon facts of specific event)
	10 or more	High Risk of Significant Harm (notification will generally be required unless an exception is determined based upon specific facts of the event)
	2. b. HI	Automatically triggers notification requirements under Federal law (and possible State law)
	2. c. HI	Automatically triggers notification if any 2.b. direct identifiers are also disclosed

Completed by:

Date: