PROCEDURE # 3.5A		EFFECTIVE DATE	REVISED DATE
TITLE:	BREACH NOTIFICATION	8/20/2020	02/12/2024
ATTACHMENT TO		REVIEW DATES	
POLICY #:	3.5		
POLICY TITLE:	BREACH NOTIFICATION		
CHAPTER:	INFORMATION MANAGEMENT		

I. PURPOSE

To ensure Lakeshore Regional Entity (LRE) staff, member Community Mental Health Service Programs (CMHSPs), regional contracted providers and other Business Associates take required actions when a breach occurs.

II. PROCEDURE

A. Discovery of Breach

1. A breach shall be treated as discovered as of the first day on which such breach is known to LRE or, by exercising reasonable diligence, would have been known to LRE or any person, other than the person committing the breach, who is a workforce member or agent of LRE.
2. Workforce members who believe that patient information has been used or disclosed in any way that compromises the security or privacy of that information shall immediately notify the LRE Privacy Officer.
3. Following the discovery of a potential breach, LRE shall begin an investigation, conduct a risk assessment, and based on the results of the risk assessment, begin the process of notifying each individual whose PHI has been, or is reasonably believed by LRE to have been, accessed, acquired, used, or disclosed as a result of the breach. LRE shall also begin the process of determining what notifications are required or should be made, if any, to the Secretary of the Department of Health and Human Services {HHS), media outlets, or law enforcement officials.

B. Risk Assessment

For breach response and notification purposes, a breach is presumed to have occurred unless LRE can demonstrate that there is a low probability that the PHI has been compromised based on, at minimum, the following risk factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. Consider:
   a. Social security numbers, credit cards, financial data.
   b. Clinical detail, diagnosis, treatment, medications.
   c. Mental health, substance abuse, sexually transmitted diseases, pregnancy.
2. The unauthorized person who used the PHI or to whom the disclosure was made.

   a. Does the unauthorized person have obligations to protect the PHI's privacy and security?
   b. Does the unauthorized person have the ability to re-identify the PHI?
3. Whether the PHI was acquired or viewed.
   a. Does analysis of a stolen and recovered device show that PHI stored on the device was never accessed?
   b. The extent to which the risk to the PHI has been mitigated.
4. Can LRE obtain the unauthorized person's satisfactory assurances that the PHI will not be further used or disclosed or will be destroyed?

The evaluation should consider these factors, or more, in combination to determine the overall probability that PHI has been compromised. The risk assessment should be thorough and completed in good faith, and the conclusions should be reasonable. Based on the outcome of the risk assessment, LRE will determine the need to move forward with breach notification. The investigator must document the risk assessment and the outcome of the risk assessment process. All documentation related to the breach investigation, including the risk assessment, must be retained for a minimum of seven years.

C. Notification of Individuals Affected

If it is determined that breach notification must be sent to affected individuals, LRE's standard breach notification letter (as modified for the specific breach) will be sent out to all affected individuals. LRE also has the discretion to provide notification following an impermissible use or disclosure of PHI without performing a risk assessment, if LRE so chooses. Notice to affected individuals shall be written in plain language and must contain the following information:

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 types of unsecured protected health information that were involved in the 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).
3. Any steps the individuals should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what LRE is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, email address, website, or postal address.
6. This letter will be sent by first-class mail to the individual at the last known address of the individual. The notification shall be provided in one or more mailings as information is available.

- If LRE knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or personal representative shall be carried out.
- If there is insufficient or out-of-date contact information that precludes direct written notification, a substitute form of notice reasonably calculated to reach the individual shall be provided (such as electronically by email or via phone).
- If there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice or by telephone or by other means.
- If there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of LRE's website, or a conspicuous notice in major print or broadcast media in LRE's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free telephone number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

7. Notice to affected individuals shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. If LRE determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate, in addition to the methods noted above. It is the responsibility of LRE to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.
8. If the individual is a minor or legally incapacitated, notice to the parent or personal representative is acceptable.

D. Notification: HHS
In the event of a breach of unsecured PHI affecting 500 or more individuals, the Secretary of Health and Human Services (HHS) will be notified at the same time notice is made to the affected individuals, in the matter specified on the HHS website. If fewer than 500 individuals are affected, LRE will maintain a log of the breaches to be submitted annually to the Secretary of HHS no later than 60 days after the end of each calendar year, in the manner specified on the HHS website. The submission shall include all breaches discovered during the preceding calendar year.

E. Notification: Media
In the event of a breach of unsecured PHI affecting more than 500 residents of a state, prominent media outlets covering the area where the affected individuals live will be notified without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. The notice shall be provided in the form of a press release.

F. Business Associates of LRE

1. CMHSP Affiliates: Each CMHSP affiliate is also a covered entity and is bound by the same obligations under HIPAA and HITECH as LRE. The fidelity of each CMHSP to these rules and obligations are reviewed annually as part of the CMHSP Site Review process (Standard 17), and as guided by the contractual obligations in the PIHP/CMHSP contract.
2. Other Business Associates: Each Business Associate (**BA**) of LRE, as bound by the requirements of a signed Business Associate Agreement (**BAA**), shall fully comply with the privacy, confidentiality and breach reporting requirements of HIPAA and HITECH, as described within the BAA. If a BA discovers there has been a breach of PHI, it must notify LRE without unreasonable delay and within any time period prescribed by the BAA which shall in no event be later than 10 days after discovery. For this purpose, "discovery" means the first day on which the breach is known to the BA or, by exercising reasonable diligence, would have been known to BA or any person, other than the person committing the breach, who is a workforce member or agent of BA. BA shall also be obligated, under the BAA, to cooperate with LRE in the investigation of a security incident or breach including preparation and distribution of notices of the Breach to the affected individuals and providing notice to DHHS and media outlets as required by HIPAA.

G. Delay of Notification Authorized for Law Enforcement Purposes
If a law enforcement official states to LRE or a business associate that a notification, notice, or posting would impede a criminal investigation or cause damage to national security:
   1. If the statement is in writing and specifies the time for which a delay is required, LRE shall delay such notification, notice, or posting for the time period specified by the official; or
   2. If the statement is made orally, LRE shall 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.

   This applies to notices made to individuals, the media, HHS, and by business associates.

H. Maintenance of Breach Information
LRE shall maintain a process to record or log all breaches of unsecured PHI, regardless of the number of consumers affected. The following information should be collected for each breach:
   1. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
   2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, social security number, date of birth, home address, account number, other).
   3. A description of the action taken to notify patients regarding the breach.

4. Steps taken to mitigate the breach and prevent future occurrences.

I. Workforce Training
LRE shall train all members of its workforce on its policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within LRE.

J. Complaints
LRE provides a process for individuals to make complaints concerning LRE's privacy policies and procedures or its compliance with such policies and procedures. Individuals also have the right to complain about LRE's Breach Notification Processes.

K. Sanctions
Members of LRE's workforce who fail to comply with this policy shall be subject to disciplinary action, up to and including termination.

L. Retaliation/Waiver
LRE may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising his or her privacy rights. Individuals shall not be required to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

M. Burden of Proof
LRE has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach.

III. APPLICABILITY AND RESPONSIBILITY

LRE staff, Member CMHSPs, and LRE Business Associates

IV. MONITORING AND REVIEW

This policy will be reviewed by the LRE Chief Information Officer on an annual basis.

V. DEFINITIONS

Breach: The unauthorized acquisition, access, use or disclosure of unsecured PHI that compromises the privacy or security of the information. In order for a breach to occur, the acquisition, access, use or disclosure must be in violation of the Health Insurance and Portability Accountability Act (**HIPAA**) privacy rules.
Disclosure: The release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.
Protected Health Information (PHI): Protected health information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Unsecured Protected Health Information (Unsecured PHI): Unsecured PHI means all PHI except for ePHI secured through encryption, and ePHI or paper PHI that has been destroyed. HHS provides guidance prescribing acceptable encryption and destruction technologies and methodologies.

Notification: Contacting appropriate parties to notify them that there has been a breach of PHI. Depending on the breach situation, the following may need to be notified:

1. The individual(s) whose PHI has been breached
2. The media
3. HHS

Such notification must meet the minimum standards of both the HIPAA and HITECH Acts. The HIPAA breach notification rule can be found at 45 CFR 164.440-414.

Business Associate: A person or entity who performs functions or activities on behalf of, or certain services for, a covered entity that necessarily involve the use or disclosure of individually identifiable health information.

Covered Entity: A health plan, health care clearinghouse or health care provider that transmits any health information electronically in connection with a covered transaction. A covered entity may be a business associate of another covered entity. LRE is a covered entity.

Workforce: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for LRE or a business associate, is under the direct control of LRE or a business associate, whether or not they are paid by LRE or a business associate.

VI. RELATED POLICIES AND PROCEDURES

A. LRE Information Management Policies and Procedures
B. LRE Compliance Policies and Procedures
C. LRE Compliance Plan
D. LRE Human Resources Policy and Procedures

VII. REFERENCES/LEGAL AUTHORITY

A. Health Insurance Portability and Accountability Act of 1996
B. Health Information Technology for Economic and Clinical Health Act of 2009
C. Identity Theft Protection Act
D. MDHHS Medicaid Specialty Supports and Services Contract

VIII. CHANGE LOG

Date of Change	Description of Change	Responsible Party
12/16/21		CIO
02/12/24	Language update – changed CIO to LRE Privacy Officer.	CIO