


CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 35
SECTION Information Systems		DESCRIPTION Health Insurance Portability and Accountability Act Breach Notifications	
WRITTEN BY Sandy Koyl, BHSA IT, Billing and Data Management Supervisor	REVISED BY Lisa Ruddy, MPH, CHC Quality Improvement Supervisor & Sandy Koyl, BHSA, IT and Data Management Supervisor		AUTHORIZED BY  Brooke Sankiewicz, LMSW, CADC CEO

APPLICATION:

<input checked="" type="checkbox"/> CMH Staff	<input checked="" type="checkbox"/> Board Members	<input checked="" type="checkbox"/> Provider Network	<input checked="" type="checkbox"/> Employment Services Providers
<input checked="" type="checkbox"/> Employment Services Provider Agencies	<input checked="" type="checkbox"/> Independent Contractors	<input checked="" type="checkbox"/> Students	<input checked="" type="checkbox"/> Interns
<input checked="" type="checkbox"/> Volunteers	<input checked="" type="checkbox"/> Persons Served		

POLICY:

Lapeer County Community Mental Health (LCCMH) has established this policy to maximize safeguards against unauthorized access to Protected Health Information (PHI). In the event these safeguards are breached, LCCMH notifies all necessary parties, including persons served whose records have been compromised, up to and including necessary State and Federal offices and available media outlets.

STANDARDS:

- A. Breach Notification: LCCMH established processes for notifying appropriate persons or agencies of a breach of protected information as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH) Act of the American Recovery and Reinvestment Act of 2009 including subsequent regulatory amendments published at 78 FR 5565, and 42 CFR Part 2, and/or State of Michigan breach notification rules.

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 35
SECTION Information Systems		DESCRIPTION HIPAA Breach Notification	

- B. Sanctions: LCCMH has established standards for employee accountability and expectations regarding adherence to the provisions of Health Information Portability and Accountability Act (HIPAA) and Michigan law, and the relative corrective action(s) that may be imposed to address privacy and or security violations. REFERENCES: 45 CFR § 164.308(a)(1)
- C. Security Awareness Training: LCCMH provides ongoing security awareness training for all employees. The security awareness training shall provide employees with best practices to maintain the confidentiality, integrity and availability of the agency's protected health information. REFERENCES: 45 CFR § 164.308(a)(5)
- D. LCCMH complies with the standards as outlined in the Region 10 Prepaid Inpatient Health Plan (PIHP) HIPAA Breach Notification Policy 03.03.04

PROCEDURES:

- A. Breach Reporting (Internal)
 - 1. Any employee who becomes aware of a possible breach of the privacy or security of protected health information immediately informs their supervisor/manager, LCCMH CEO, Privacy Officer and the Security Officer.
 - 2. Notification must occur immediately upon discovery of a possible breach or before the end of the workday if other duties interfere. In no case must a notification occur later than twenty-four (24) hours after discovery.
 - 3. Upon reporting the possible breach, the employee is prepared to:
 - a. Provide as much detail as possible.
 - b. Be responsive to requests for additional information.
 - c. Be aware the Privacy Officer has an obligation to follow up on any reasonable belief private information has been compromised.
 - 4. Following the discovery of a potential breach, LCCMH begins an investigation and conducts a risk assessment.

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 35
SECTION Information Systems		DESCRIPTION HIPAA Breach Notification	

5. The CEO, in conjunction with the LCCMH Legal Counsel, determines whether or not to notify the appropriate persons or agencies taking into consideration the seriousness and scope of the breach as required by law.

B. Breach Reporting (PIHP)

1. LCCMH notifies the PIHP as soon as possible, but no later than 15 calendar days of becoming aware of any act, error or omission, negligence, misconduct or breach compromising or suspecting to compromise the security, confidentiality or integrity of PIHP Data.
2. LCCMH cooperates with the PIHP in investigating the occurrence, including making available all relevant records, logs, files, data reporting and other materials as required to comply with applicable law or otherwise required in the LCCMH Services Contract with the PIHP.

C. Containing a Breach

1. The Security Officer takes adequate and immediate steps to limit the scope and effect of the breach by:
 - a. Stopping the unauthorized practice that led to the breach.
 - b. Recovering the records, if possible.
 - c. Shutting down the breached system.
 - d. Correcting weaknesses in security practices.
2. The Privacy Officer notifies the appropriate authorities including the local Police Department if the breach involves, or may involve, any criminal activity.
3. Investigating & Evaluating the Risks Associated with a Breach
 - a. The Privacy Officer in collaboration with the LCCMH Legal Counsel investigates the circumstances of any breach. They review the results of the investigation to determine root causes, evaluate risks, and develop a resolution plan.

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 35
SECTION Information Systems		DESCRIPTION HIPAA Breach Notification	

- i. The Privacy Officer, in collaboration with the LCCMH Legal Counsel, conducts a risk assessment to determine whether a disclosure of protected health information constitutes a breach. Following the January 2013 HIPAA “Omnibus” rule, any “acquisition, access, use or disclosure in a manner not permitted is presumed to be a breach” unless a risk assessment determines there is a low probability the protected health information has been compromised. The risk assessment must include at least the following factors:
 - a) The nature and extent of the protected health information involved, including the likelihood of re-identification and types of identifiers.
 - b) The identity of the person to whom the unauthorized disclosure was made.
 - c) Whether the protected health information was actually acquired or viewed.
 - d) The extent to which the risk to the protected health information has been mitigated.

D. Breach Notification (External)

- 1. The Privacy Officer works with the LCCMH Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law.
- 2. The appropriate agencies of the government must be notified as required by law.
 - a. Information regarding breaches involving five-hundred (500) or more individuals, regardless of location, must be submitted to the Department of Health and Human Services at the same time notices to individuals are issued.
 - b. If a breach involves fewer than five-hundred (500) individuals, LCCMH is required to keep track of all breaches and to notify the U.S. Department of Health and Human Services within sixty (60) days after

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 35
SECTION Information Systems		DESCRIPTION HIPAA Breach Notification	

the end of the calendar year using LCCMH HIPAA Privacy Breach Report Log Form #F381.

3. If required by law, notification to individuals affected by the breach occurs as soon as possible following the breach.
 - a. Affected individuals must be notified without reasonable delay, unless instructed otherwise by law enforcement or other applicable state or local laws.
 - b. Notices must be in plain language and include basic information, including:
 - i. What happened
 - ii. Types of protected health information involved
 - iii. Steps individuals must take
 - iv. Steps covered entity is taking
 - v. Contact information
 - c. Notices are sent by first-class mail or if individual agrees electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.
4. If law enforcement authorities have been contacted, those authorities assist in determining whether notification may be delayed in order not to impede a criminal investigation.
5. Indirect notification such as website information, posted notices, and media generally occurs only where direct notification could cause further harm, or the contact information is lacking.
 - a. If a breach affects five-hundred (500) or more individuals, or the contact information is insufficient, the LCCMH Privacy Officer in the absence of the Chief Executive Officer notifies a prominent media outlet that is appropriate for the size of the location with affected individuals, and notice is provided in the form of a press release.

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 35
SECTION Information Systems		DESCRIPTION HIPAA Breach Notification	

6. Using multiple methods of notification in certain cases may be the most effective approach.

E. Breach Originating from a Business Associate

1. Business associates must notify LCCMH if they incur or discover a breach of unsecured PHI.
2. Notices must be provided without reasonable delay and in no case later than fifteen (15) days after discovery of the breach.
3. Business associates must cooperate with LCCMH in investigating and mitigating the breach.

F. Sanctions

1. All information related to a treatment for a person served is considered PHI. This information can only be accessed and shared with those who have a “need to know” while performing duties related to treatment, payment, and healthcare operations.
2. No information concerning the person served may be used, disclosed, or discussed outside of the agency unless specifically authorized by the person served, permitted and/or required by federal or Michigan law. The agency’s policies address these requirements and are adhered to by all persons working for LCCMH.
3. Employees who fail to comply with the policies of LCCMH or with the requirements of state and federal privacy regulations are subject to disciplinary action, up to and including termination.
4. All HIPAA and privacy related sanctions are documented in the employee’s personnel file.

G. HIPAA Security/Awareness Training

1. HIPAA Security training –LCCMH provides a security awareness training designed to educate both new and current employees on issues relating to safeguarding protected health information. New employees are provided with training during the orientation process. Existing employees are provided with ongoing training as needed but no less than once per year

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 35
SECTION Information Systems		DESCRIPTION HIPAA Breach Notification	

through the agency online training Learning Management Software. Security awareness training may vary based on an employee's job function; however, all employees are trained on HIPAA Privacy and Security measures relative to the agency.

DEFINITIONS:

Breach: A breach is the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Health Insurance Portability and Accountability Act (HIPAA), which compromises the security or privacy of the PHI. This excludes:

1. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under HIPAA.
2. Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.
3. A disclosure of protected health information where a covered entity or business associate has a good faith belief an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Business Associate: An individual, group or agency with whom LCCMH has a relationship and the Business Associate role is that of a non-covered entity and protected health information is shared as part of doing business.

Protected Health Information (PHI): PHI, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), with revisions from the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), includes 18

CHAPTER Information Management	CHAPTER 07	SECTION 001	SUBJECT 35
SECTION Information Systems		DESCRIPTION HIPAA Breach Notification	

identifiers that can be used to uniquely identify a person by their demographic information, health conditions, medical histories, assessment/laboratory/test results, services or insurance beneficiary information as i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. For PHI exclusions see 45 CFR §160.103. (See HIPAA Privacy Rules for more information.)

Unsecured PHI: Unsecured PHI means any PHI which is not unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology, such as encryption or destruction, as specified by the Secretary of the Department of Health and Human Services (HHS).

REFERENCES

45 CFR-Code of Federal Regulations

42 CFR-Code of Federal Regulations
78 Federal Registry 5565

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

LCCMH Form # F381 HIPAA Privacy Breach Report Log

Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)

Region 10 Prepaid Inpatient Health Plan (PIHP) HIPAA Breach Notification Policy
03.03.04

45 CFR § 164.308(a)(1)

45 CFR § 164.308(a)(5)

LR & SK