COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE POLICY AND PROCEDURES MANUAL				
Chapter **Program Quality**	**Section** **HIPAA**	**Chapter** **05**	**Section** **03**	**Subject** **19**
Subject **Breach Notification and Management**	**Authorization** Melissa Hall		**Approved: 08/30/16** **Replaces: None**	

Reviewed/No Updates: March 2022; October 2022

I. PURPOSE: To ensure compliance with regulatory standards regarding breaches of privacy and breach notification requirements.

II. APPLICATION: All individuals employed by Gogebic Community Mental Health Authority (CMHA), to include the members of the CMHA Board, all contract providers, and Business Associates (herein after referred to as "workforce").

III. DEFINITIONS:

1. **Breach**: An impermissible use or disclosure under the HIPAA Privacy Rule that compromises the security or privacy of protected health information. There are three exceptions to the definition of "breach" which are:
   - **a)** Any unintentional acquisition, access, or use of protected health information by an employee of CMHA or person acting under the authority of CMHA or a 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.
   - **b)** Any inadvertent disclosure by an employee who is authorized to access protected health information to a business associate or another employee authorized to access protected health information and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted.
   - **c)** A disclosure of protected health information where CMHA 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. **Unsecured protected health information**: Protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of the U. S. Department of Health and Human Services in the guidance issued under section13402(h)(2) of Public Law 111–5 (HITECH Act) on the Health and Human Services web site.
3. **Workforce**: Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for CMHA or a business associate, is under the direct control of CMHA or a business associate, whether or not they are paid by CMHA or a business associate.

IV. POLICY: CMHA, a HIPAA Covered Entity (CE), and other Covered Entities, and all Business Associates (BA) must provide notification following the discovery of a breach of unsecured protected health information (45 CFR §§ 164.400-414).

V. PROCEDURE:

A. Administrative Requirements and Burden of Proof:

1. An impermissible use or disclosure of protected health information (PHI) is presumed to be a breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:
   - **a)** The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
   - **b)** The unauthorized person who used the protected health information or to whom the disclosure was made;
   - **c)** Whether the PHI was actually acquired or viewed; and
   - **d)** The extent to which the risk to the PHI has been mitigated.
2. Policies, Training, and Enforcement: Covered Entities must have in place written policies and procedures regarding privacy of PHI and breach notification.
3. Training: Covered Entities' personnel must be trained on the policies and procedures with respect to protected health information, privacy and security practices, and breach notification as necessary and appropriate for personnel to carry out their duties.
4. Refraining from Intimidating or Retaliatory Acts: Covered Entities may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any right established, or for participation in any process provided for, by this procedure or any Privacy Practices, including the filing of a complaint under this section.
5. Waiver of Rights: CMHA will not require individuals to waive their rights under federal privacy laws as a condition of the provision of treatment, payment, enrollment, or eligibility for benefits.

B. Reporting and Documentation Requirements:

CMHA personnel who believe there has been a breach of protected health information shall notify their supervisor and/or CMHA's Privacy and Security Officers immediately. Upon receipt of a breach or suspected breach of PHI, CMHA will:

1. Record the date that the suspected breach was known, or should have reasonably been known, to CMHA;
2. Determine if an actual breach occurred; and
3. If a breach occurred:
   - **a)** Record the date the breach occurred.
   - **b)** To the extent practicable, mitigate the cause of the breach.
   - **c)** If the organization is acting as a business associate, notify the covered entity as soon as possible, but no later than the time frame stipulated in the applicable BAA, which cannot be more than 60 calendar days from the date of knowledge as required by federal law.
   - **d)** Provide notice, as required by federal law, to the individual affected by the breach outlined below.
   - **e)** Provide notice as required by federal law to the Department of Health and Human Services, as outlined below.
   - **f)** Conduct post-breach evaluation and remediation.

4. Ensure all required notifications have been provided or that a use or disclosure of unsecured PHI did not constitute a breach.
5. With respect to an impermissible use or disclosure, CMHA will maintain documentation that all required notifications were made, or alternatively, documentation to demonstrate that notification was not required, such as: (1) the risk assessment demonstrating a low probability that the PHI has been compromised by the impermissible use or disclosure, or (2) the application of any other exceptions to the definition of "breach."

C. Breach Notification Requirements: A breach shall be treated as discovered as of the first day on which such breach is known by the CE/BA, or, by exercising reasonable diligence would have been known to the CE/BA. CE/BA shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent.

Following the discovery of a breach of unsecured protected health information, CE/BA shall notify each individual whose unsecured protected health information has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach.

1. Individual Notice: CE/BA shall notify affected individuals in written form by first class mail to their last known address. Notice must be provided without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. The notification may be provided in one or more mailings as information is available. If the individual is deceased written notification by first class mail will be sent to the personal representative of the individual, if known. The notice shall include:
   - **a)** A brief description, in plain language, of what happened, including the date of the breach and the date of the discovery of the breach, if known.
   - **b)** 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).
   - **c)** Any steps individuals should take to protect themselves from potential harm resulting from the breach.
   - **d)** A brief description of what the CE/BA is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches.
   - **e)** Contact information for individuals to ask questions or learn additional information, including a toll-free number, and email address.
2. Substitute Notice – Insufficient or Out-of-Date Contact Information
   - **a)** If CE/BA has insufficient or out-of-date contact information for **fewer than 10** individuals, CE/BA may provide substitute notice by an alternative form of written notice, by telephone, or other means.
   - **b)** If CE/BA has insufficient or out-of-date information for **10 or more** individuals, CE/BA must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcast media where the affected individual likely

resides. A toll-free phone number that remains active for at least 90 days must be included.

c) These notices must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, the same information as noted in 1. a) – e), above.

3. Additional Notice in Urgent Situations: If CE/BA deems a breach to be a potential for imminent misuse of unsecured PHI, CE/BA may provide information to individuals by telephone or other means, as appropriate, in addition to the written notice.

4. Notification to the Media: For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, CE/BA shall notify prominent media outlets serving the State or jurisdiction. Media notification shall be provided without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. Media notification shall include the same information required for the individual notice.

5. Notification to the Secretary of Health and Human Services: In addition to notifying affected individuals and the media (where appropriate), CEs/BAs must notify the Secretary of breaches of unsecured PHI. Notification is made electronically at the HHS web site on the breach report form provided. If a breach affects 500 or more individuals, CE/BA must notify the Secretary without reasonable delay and in no case later than 60 days following the discovery of a breach. If, however, a breach affects fewer than 500 individuals, CE/BA may notify the Secretary of such breaches on an annual basis, no later than 60 days after the end of the calendar year in which the breaches are discovered.

6. Notification to a Covered Entity: If CMHA is a Business Associate of another Covered Entity, CMH will notify the covered entity immediately following the discovery of a potential breach of the covered entity's protected health information. The Covered Entity will file necessary notification to individuals, Secretary of HHS, and the media, as applicable, unless stated otherwise in the Business Associate Agreement.

7. Law Enforcement Delay: If a law enforcement official states that a notification, notice, or posting required under this procedure would impede a criminal investigation or cause damage to national security, CE/BA shall:

a) Delay such notification, notice, or posting for the time period specified by the official, if the statement is in writing and specifies the time for which a delay is required, or

b) 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, if the statement is made orally; or unless a written statement as described in paragraph (a) of this section is submitted during that time.

D. Notification by a Business Associate to CMHA as the Covered Entity: A Business Associate shall notify CMHA immediately following the discovery of a breach of unsecured protected health information as outlined in this policy. CMHA, as the CE, is responsible for breach notification to the individual, Secretary of Health and Human Services, and the media, as required, unless delegated to the Business Associate and stated in the Business Associate Agreement.

E. When is Breach Notification Not Required? Required notifications are only required if the breach involved unsecured protected health information. Encryption and destruction are technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals. Covered entities and business associates that secure information as specified by this guidance are not required to provide notifications following the breach of such information.

VI. REFERENCES AND LEGAL AUTHORITY: 45 CFR § 164 Privacy of Individually Identifiable Health Information; 45 CFR § 164.400-414 Breach Notification Rule; Public Law 111-5 Health Information Technology for Economic and Clinical Health Act (HITECH Act); NorthCare Network Breach Notification and Management Policy; URAC Accreditation Standards, as applicable

VII. EXHIBITS: None