


CHAPTER: 10	SECTION: 12	SUBJECT: MANAGEMENT OF INFORMATION
TITLE: BREACH NOTIFICATION		
EFFECTIVE DATE: 11/15/2019	REVISED/REVIEWED DATE: 09/16/2020, 9/24/21, 10/20/22, 12/12/23	
ISSUED AND APPROVED BY:  EXECUTIVE DIRECTOR		

I. PURPOSE:

The purpose of this Breach Notification Policy is to provide guidance to the staff of Community Mental Health of Ottawa County when there is a breach or disclosure of unsecured protected health information and protected identifiable information in a manner not permitted under the Health Insurance Portability and Accountability Act of 1996 and its implementing rules and regulations, which compromises the security or privacy of the Protected Health Information, and to ensure compliance with regulatory standards regarding breaches of privacy and breach notification requirements.

II. APPLICATION:

This policy applies to all staff employed by CMHOC, and contractual organizations as specified in their contracts.

III. DEFINITIONS:

Breach: The acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under HIPAA, which compromises the security or privacy of the protected health information.

Protected Health Information (PHI): PHI is individually identifiable health information that identifies the individual or that provides a basis for identifying the individual that is transmitted or maintained in any form or medium.

Protected Identifiable Information (PII): PII is information that identifies the individual or that provides information that, when used alone or with other relevant data, can identify an individual.

IV. POLICY:

It is the policy of CMHOC that all personnel must preserve the integrity and the confidentiality of Protected Health Information and Protected Identifiable Information pertaining to our consumers. HIPAA requires that covered entities notify individuals whose unsecured protected health information and protected identifiable information has been impermissibly accessed, acquired, used, or disclosed, compromising the security or privacy of the protected health information. CMHOC will develop, maintain, and regularly review procedures to be implemented in the event that there is a breach.

V. PROCEDURES:

- A. Discovery of Breach:** CMHOC receives notification from staff, contracted programs, and/or an external contact who believes that individual identifiable health information has been used or disclosed in any way that compromises the security or privacy of that information. The following

CMHOC staff will be immediately notified of the breach: Ottawa County Corporate Counsel (Privacy Officer), Ottawa County IT Security Officer, CMHOC Executive Director, CMHOC Recipient Rights Officer and Privacy Officer, CMHOC Security Officer, and CMHOC Compliance Manager.

- B. Breach Investigation:** Following the discovery of a potential breach, CMHOC 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/PII has been accessed, acquired, used, or disclosed as a result of the breach. CMHOC will 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), and media outlets.
- C. Risk Assessment:** The Risk Assessment shall assess the following components:
1. The nature and extent of the PHI/PII involved, including the following types of identifiers:
 - 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 type of media the PHI/PII was stored: paper, digital format sent via email, digital format on laptops, etc.
 3. The unauthorized person who used the PHI/PII or to whom the disclosure was made and if this person is obligated to protect the PHI/PII's privacy and security.
 4. Whether the PHI/PII was actually acquired or viewed.
 5. The extent to which the risk to the PHI/PII has been mitigated.

The evaluation should consider these factors, or more, in combination to determine the overall probability that PHI/PII 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, CMHOC will determine the need to move forward with breach notification. The risk assessment and the outcome of the risk assessment process must be documented. All documentation related to the breach investigation, including the risk assessment, must be retained for a minimum of six years.

- D. Notification: Individuals Affected:** If it is determined that breach notification must be sent to affected individuals, the CMHOC standard breach notification letter (as modified for the specific breach) will be sent out to all affected individuals. Notice to affected individuals shall be written in plain language and must contain the following information, which elements are included in the Practice's standard breach notification letter:
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 and/or protected identifiable information that were involved in the breach (such as full name, social security number, date of birth, home address, account number, other).
 3. Any steps the individuals should take to protect themselves from potential harm resulting from the breach.
 4. A brief description of what CMHOC 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 telephone number, email address, website, or postal address.
6. If the covered entity knows 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 either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.

This letter will be sent by first-class mail to the individual and/or individual representative or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail.

If there is insufficient or out-of-date contact information that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. 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, 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 the CMHOC website, or a conspicuous notice in major print or broadcast media in the CMHOC geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI/PII may be included in the breach.

Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.

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 CMHOC determines that notification requires urgency because of possible imminent misuse of unsecured PHI/PII, notification may be provided by telephone or other means, as appropriate, in addition to the methods noted above. It is the responsibility of CMHOC to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.

A copy of all correspondence shall be retained by CMHOC in accordance with state law record retention requirements.

- E. Notification of U.S. Department of Health and Human Services (HHS):** In the event a breach of unsecured PHI/PII affects 500 or more individuals, HHS will be notified at the same time notice is made to the affected individuals, in the manner specified on the HHS website. If fewer than 500 individuals are affected, CMHOC 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 specific on the HHS website. The submission shall include all breaches discovered during the preceding calendar year.
- F. Notification: Media:** In the event the breach affects more than 500 individuals, prominent media outlets serving the state and regional area 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.

- G. Delay of Notification Authorized for Law Enforcement Purposes:** If a law enforcement official states that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, CMHOC shall:
1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or
 2. If the statement is made orally, 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:** CMHOC shall maintain a process to record or log all breaches of unsecured PHI/PII, regardless of the number of individuals 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 individuals 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 with regard to notification of individuals regarding the breach.
 4. Steps taken to mitigate the breach and prevent future occurrences.

- I. Business Associate Responsibilities:** CMHOC's business associates shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach of unsecured PHI/PII, notify CMHOC of such breach. Such notice shall include the identification of each individual whose unsecured PHI/PII has been or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. The business associate shall provide CMHOC with any other available information that is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the business associate of discovery of a breach, CMHOC will be responsible for notifying affected individuals, unless otherwise agreed upon by the business associate to notify the affected individuals.

- J. Training:** CMHOC shall train all employees on the CMHOC policies and procedures with respect to PHI/PII as necessary and appropriate for employees to carry out their job responsibilities. Employees shall also be trained as to how to identify and report breaches no less than annually, which may include County of Ottawa Security Awareness Training.

- K. Sanctions:** CMHOC employees who fail to comply with this policy shall be subject to disciplinary action, up to and including termination.

- L. Retaliation/Waiver:** CMHOC 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: CMHOC 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.

VI. ATTACHMENT

VII. REFERENCES

U.S. Department of Health & Human Services, Health Information Privacy, Breach Notification Rule

Centers of Medicare & Medicaid Services. 2018, September). HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules

CMHOC Security Management Plan

CMHOC Policy, 10(08) Privacy and Security of Information

Ottawa County Policy, County Electronic Communication Policy

Ottawa County Policy, HIPAA Compliance

Ottawa County Policy, Information Security