SANILAC COUNTY COMMUNITY MENTAL HEALTH AUTHORITY

ADMINISTRATIVE POLICY

NUMBER: BA153

NAME: HIPAA BREACH NOTIFICATION

INITIAL APPROVAL DATE:	10/27/2020	BY: Sanilac CMH Board
STAKEHOLDER REVIEW:	09/07/2022	BY: Consumer Advisory Board
(LAST) REVISION DATE:	02/15/2023	BY: CIO
(LAST) REVIEW DATE:	01/16/2025	BY: Policy Committee
DISCONTINUED DATE:	N/A	REPLACED BY: N/A

I. PURPOSE

To ensure Sanilac County Community Mental Health Authority (Sanilac CMH) staff are in compliance with federal and state regulations.

II. APPLICATION

Populations: **NA**
Programs: **Direct - ALL**
Contracted - ALL

III. POLICY

It shall be the policy of Sanilac CMH to maximize safeguards against unauthorized access to protected health information (PHI). In the unlikely event that these safeguards are breached, it shall be the policy of Sanilac CMH to notify all necessary parties, including the individual(s) whose records have been compromised, up to and including the PIHP, the necessary State and Federal offices and available media outlets. The notification process is to be executed pursuant to the 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 CFR 5566, and handle SUD information as required in 42 CFR Part 2.

IV. 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:

i. 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.

ii. 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.

iii. A disclosure of protected health information 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.

Business Associate: An individual, group or agency with whom Sanilac CMH 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 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) in the guidance issued under section 13402(h)(2) of Public Law 111-5 (45 CFR § 164.402).

Workforce: Workforce means employees, volunteers, trainees, and other persons under the direct control of Sanilac CMH, whether or not they are paid by Sanilac CMH.

V. INTRODUCTION

In summary, HIPAA requires that covered entities notify individuals whose unsecured protected health information has been impermissibly accessed, acquired, used, or disclosed, compromising the security or privacy of the protected health information. The notification requirements only apply to breaches of unsecured PHI. In other words, if PHI is encrypted or destroyed in accordance with the HIPAA guidance, there is a "safe harbor", and notification is not required.

A. Discovery of Breach. A breach shall be treated as discovered as of the first day on which such breach is known to the CMH or, by exercising reasonable diligence, would have been known to the CMH or any person, other than the person committing the breach, who is a workforce member or agent of Sanilac CMH. Workforce members who believe that individual information has been used or disclosed in any way that compromises the security or privacy of that information shall immediately notify his/her supervisor, the Chief Executive Officer, and the Chief Information Officer, or the privacy officer. It is the responsibility of all Sanilac CMH personnel, including employees and Board members as well as Providers and Provider staff, to report to the Provider and/or Sanilac CMH his or her good faith belief of any violation of the CMH Corporate Compliance Program. (See Corporate Compliance Program Policy BA032.) Following the discovery of a potential breach, Sanilac CMH 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 the CMH to have been, accessed, acquired, used, or disclosed as a result of the breach. Sanilac CMH shall also begin the process of determining what notifications are required or should be made, if any, to the PIHP, to the Secretary of the HHS, media outlets, or law enforcement officials.

B. Breach Investigation. The Compliance and/or Privacy Officer of Sanilac CMH shall act as the investigator of the breach. The investigator shall be responsible for the management of the breach investigation, completion of the risk assessment, and coordinating with others at Sanilac CMH as appropriate (e.g., administration, information technology, human resources, risk management, legal counsel.) Sanilac CMH's entire workforce is expected to assist management in this investigation as requested. The investigator shall be the key facilitator for all breach notification processes.

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

i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. Consider:
   1. Social security numbers, credit cards, financial data
   2. Clinical detail, diagnosis, treatment, medications
   3. Mental health, substance abuse, sexually transmitted diseases, pregnancy

ii. The unauthorized person who used the PHI or to whom the disclosure was made.
   1. Does the unauthorized person have obligations to protect the PHI's privacy and security?
   2. Does the unauthorized person have the ability to re-identify the PHI?

iii. Whether the PHI was actually acquired or viewed: For example, does analysis of a stolen and recovered device show that PHI stored on the device was never accessed?

iv. The extent to which the risk to the PHI has been mitigated: Can the CMH 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, Sanilac CMH 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 ten years.

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

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

ii. 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).

iii. Any steps the individuals should take to protect themselves from potential harm resulting from the breach.

iv. A brief description of what the CMH is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

v. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, email address, website, or postal address.

This letter (written notification) will be sent by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If the CMH 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 or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. 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 of the individual. 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 CMH's website, or a conspicuous notice in major print or broadcast media in the CMH's 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 may be included in the breach.

Except as provided in 45 CFR 164.412 (law enforcement delay), CMH provides notification to individuals affected by a breach without unreasonable delay and in no case later than sixty (60) calendar days after the discovery of the breach. If CMH 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 the CMH to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay. A copy of all correspondence with the individual shall be retained by the CMH in accordance with state/federal law record retention requirements.

E. Notification: MDHHS. In the event of any suspected or confirmed unauthorized use or disclosure of protected health data and information that falls under the HIPAA requirements, of which the CMH becomes aware, the CMH will work with MDHHS to mitigate the breach, and will provide assurances to MDHHS of corrective actions to prevent further unauthorized uses or disclosures. Notification to MDHHS will occur immediately, but no later than one business day after the discovery of the unauthorized access, use or disclosure of confidential protected health information.

F. Notification: HHS. In the event a breach of unsecured PHI affects 500 or more of the CMH's individuals, 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 of the CMH's individuals are affected, the CMH 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.

G. Notification: Media. In the event the breach affects more than 500 residents of a state, 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.

H. Delay of Notification Authorized for Law Enforcement Purposes. If a law enforcement official states to the CMH or a business associate that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the CMH shall:

i. 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

ii. 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.

I. Maintenance of Breach Information. The CMH shall maintain a process to record or log all breaches of unsecured PHI, regardless of the number of individuals affected. The following information should be collected for each breach:

i. 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.

ii. 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).

iii. A description of the action taken with regard to notification of individuals regarding the breach.

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

J. Business Associate Responsibilities. The CMH's business associates shall, without unreasonable delay and in no case later than fifteen (15) calendar days after discovery of a breach of unsecured PHI, notify the CMH of such breach. Such notice shall include the identification of each individual whose unsecured PHI 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 the CMH with any other available information that the CMH 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, the CMH will be responsible for notifying affected individuals, unless otherwise agreed upon by the business associate to notify the affected individuals.

K. Workforce Training. The CMH shall train all members of its workforce on the CMH's 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 the CMH.

L. Complaints. The CMH provides a process for individuals to make complaints concerning the CMH's consumer privacy policies and procedures or its compliance with such policies and procedures. Individuals also have the right to complain about the CMH's breach notification processes.

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

N. Retaliation/Waiver. The CMH 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.

O. Burden of Proof. The CMH 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.