St. Clair County Community Mental Health
Providing Opportunities for Health, Wellness, & Connection

Administrative Policy

Policy Title:	**HIPAA Privacy Breach Notifications**
Policy #:	**08-002-0006**
Effective Date:	06/5/2025
Approved by:	Telly Delor, Chief Operating Officer
Functional Area:	Administration
Responsible Leader:	Telly Delor, Chief Operating Officer (and Privacy Officer)
Policy Owner:	Joy Vittone, Corporate Compliance Supervisor
Applies to:	SCCCMH Staff, Community Agency Contractor, Contracted Network Providers, Direct Operated Programs, Specialized Residential Providers, SCCCMH Board, all collectively referred to as "staff" in this policy

Purpose: To comply with HIPAA requirements to investigate all suspected and potential breaches, perform privacy breach risk analysis, and notify individuals, government and regulatory authorities, and media, when required.

I. Policy Statement

St. Clair County Community Mental Health (SCCCMH) shall ensure that all staff preserve the integrity and the confidentiality of the information of individuals served.

SCCCMH shall maximize safeguards against unauthorized access to *Protected Health Information (PHI)*. In the event these safeguards are breached, SCCCMH shall notify all necessary parties, including the individual(s) whose records have been breached, as well as appropriate state and federal offices and available media outlets, when required. The notification process will be executed pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act; the Confidentiality of Substance Use Disorder (SUD) Patient Records at 42 CFR part 2; the confidentiality provisions of section 3221 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act; the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy, Breach Notification, and Enforcement Rules; and any other applicable state and federal regulations.

II. Standards

A. In the case of a breach of *unsecured Protected Health Information (PHI)*, SCCCMH must notify the individual whose PHI was breached, or their guardian/personal

representative, without unreasonable delay and in no case later than 60 days after discovering the breach.

B. A breach is considered discovered as of the first day on which the breach is known by SCCCMH or the business associate. Business associates are required to report any breach to SCCCMH immediately upon discovery.

C. A breach is the impermissible acquisition, access, use, or disclosure of unsecured PHI which compromises the security or privacy of the PHI. The term breach does not include:

1. Any unintentional acquisition, access, or use of PHI by a staff member or person acting under the authority of SCCCMH or a business associate made in good faith and within the course and scope of the person's authority when the PHI is not further used or disclosed in a manner not permitted.
2. Any inadvertent disclosure of PHI by a person authorized to access the PHI at SCCCMH or an SCCCMH business associate to another person at SCCCMH or an SCCCMH business associate, or within an organized health care arrangement in which SCCCMH participates, when the information received as a result of the disclosure is not further used or disclosed in a manner not permitted.
3. SCCCMH or its business associate has a good faith belief that the unauthorized person to whom the PHI was disclosed would not reasonably have been able to retain the disclosed information.

D. SCCCMH designates the Chief Operating Officer as its Privacy Officer.

E. Following an Incident or the discovery of a potential breach, SCCCMH must immediately report the possibility of an impermissible use or disclosure to the PIHP (Exhibit D) and begin an investigation. A breach risk assessment must be conducted as needed, and based on the results of the risk assessment, SCCCMH must begin the process of notifying each individual whose PHI is reasonably believed by SCCCMH to have been accessed, acquired, used, or disclosed as a result of a breach. SCCCMH shall also begin the process of determining what notifications are required or should be made, if any, to the Secretary of the U.S. Department of Health and Human Services (HHS), the Michigan Department of Health and Human Services (MDHHS), media outlets, or law enforcement officials.

F. For breach response and notification purposes, a breach is presumed to have occurred unless SCCCMH 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 such as:
    - Social security numbers, credit cards, and financial data
    - Clinical detail, diagnosis, treatment, and medications

- Mental health, substance abuse, sexually transmitted diseases, and pregnancy

2. Regarding the unauthorized person who used the PHI or to whom the disclosure was made:
   - Does the unauthorized person have obligations to protect the PHI's privacy and security?
   - Does the unauthorized person have the ability to re-identify the PHI?
3. Was the PHI actually acquired or viewed? For example, does analysis of a stolen and recovered device show that PHI stored on the device was never accessed?
4. The extent to which the risk to the PHI has been mitigated: Can SCCCMH obtain the unauthorized person's satisfactory assurances that the PHI will not be further used or disclosed or will be destroyed?

G. Notice to affected individuals must 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 PHI 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 SCCCMH 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.

H. Notice to affected individuals must be made without unreasonable delay, and in no case later than 60 calendar days after the discovery of the breach. If SCCCMH 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 stated below. It is the responsibility of SCCCMH to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.

I. The notification letter must be sent to the individual’s last known address, or by electronic mail (if the individual has agreed to electronic notice and such agreement has not been withdrawn at time of breach notification). If SCCCMH is aware that the

individual is deceased and has the address of the next of kin or personal representative of the individual, written notification must be sent to the next of kin or personal representative.

J. If individuals' contact information is insufficient or out of date, not allowing for direct written or electronic notification, a substitute form of notice to reach individuals 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 SCCCMH's website, or a conspicuous notice in major print or broadcast media in SCCCMH'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 individuals can learn whether their PHI may have been included in the breach.

K. Notification to Michigan Department of Health and Human Services (MDHHS) Regarding Breach:

1. In the event of any confirmed unauthorized use or disclosure of PHI (as defined by HIPAA definition), SCCCMH will notify and collaborate with MDHHS to mitigate the breach and will provide to MDHHS a plan of corrective actions to prevent further unauthorized uses or disclosures of PHI (Exhibit B).

L. Notification to U.S. Department of Health and Human Services (HHS) Regarding Breach:

1. In the event a breach of unsecured PHI affects 500 or more of SCCCMH's individuals, HHS will be notified at the same time notice is made to the affected individuals, in the manner specified on the HHS website.
2. If fewer than 500 of SCCCMH's individuals are affected, SCCCMH 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.

M. Notification to Media Regarding Breach:

1. 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 new/press release (Exhibit C).

N. SCCCMH shall maintain a process to record or log all breaches of unsecured PHI, regardless of the number of individuals affected. The following information shall 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 PHI 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.

O. Violation of this policy is grounds for disciplinary action, up to and including termination of employment in accordance with Administrative Policy #06-001-0055, Personnel: Corrective/Disciplinary Action

III. Procedures, Definitions, and Other Resources

A. Procedures

Actions – Breaches

Action Number	Responsible Stakeholder	Details
1.0	Staff/Person Discovering Breach	1. Report all of the following occurrences to the SCCCMH Privacy Officer, using any of the methods communicated on Corporate Compliance flyers posted throughout SCCCMH facilities and set forth in Board Policy #01-002-0020, Corporate Compliance Complaint, Investigation & Reporting Process and Non-Retaliation: a. when they believe that individual information has been used or disclosed in any way that compromises the security or privacy of that information b. any improper disclosures of PHI c. any good faith belief of any violation of the SCCCMH Corporate Compliance Program

Actions – Breach Investigations

Action Number	Responsible Stakeholder	Details
1.0	SCCCMH Privacy Officer/ Designee	1. Act as the lead investigator of the breach with responsibility for managing the breach investigation, completing a risk assessment, and coordinating with other SCCCMH staff, as appropriate (e.g., administration, information technology, human resources, risk management, public relations, and legal counsel) 2. Immediately report to Region 10 PIHP the possibility of an impermissible use or disclosure to the PIHP (Exhibit D). 3. Act as the key facilitator for all breach notification processes 4. Count "day one" of a breach discovery as the first day that a breach is known, or would have been known to a SCCCMH staff, other than the person committing the breach 5. Perform a HIPAA Risk Assessment (RA) and document the outcome of the RA process. 6. Determine, based on the outcome of the Risk Assessment, the need to move forward with breach notifications 7. Retain all documentation related to the breach investigation, including the RA, for a minimum of ten years. 8. NOTE: SCCCMH also has the discretion to provide notification following an unauthorized use or disclosure of PHI without performing an RA.

Actions – Notification to Individuals Affected by Breach

Action Number	Responsible Stakeholder	Details
1.0	SCCCMH Privacy Officer	1. Send SCCCMH standard breach notification to all affected individuals (Exhibit A). 2. Maintain a copy of all individual's correspondences required by state and federal law record retention requirements.

Actions – Notification to Regulatory Agencies and Media

Action Number	Responsible Stakeholder	Details
1.0	SCCCMH Privacy Officer	1. Maintain a log tracking every reportable HIPAA breach. The log must include the date of each breach, the date of discovery of each breach, the number of individuals affected, the type of information that was breached, how the individuals were notified about the breach, and the steps taken to mitigate the breach and prevent future breaches. 2. Notify and collaborate with the Michigan Department of Health and Human Services (MDHHS) to mitigate the breach and provide a plan of correction to prevent further unauthorized use or disclosure of PHI (Exhibit B). 3. Notify the U.S. Department of Health and Human Services (HHS), Office of Civil Rights, no later than 60 days after discovery of a breach of unsecured PHI that affects 500 or more individuals served by SCCCMH. 4. Notify, within 60 calendar days, prominent media outlets via press release, when 500 or more residents of a state, are affected by a breach of PHI (Exhibit C).

Actions – Business Associates Responsibilities Regarding Breach

Action Number	Responsible Stakeholder	Details
1.0	Business Associate	1. Notify SCCCMH's Chief Executive Officer and/or Privacy Officer without unreasonable delay, within 15 calendar days, after discovery of a breach of unsecured PHI. Such notice shall include the identification of each individual whose unsecured PHI is believed to have been impermissibly accessed, acquired, used, or disclosed. 2. Provide SCCCMH with all available information required by SCCCMH for notification to the individual served. SCCCMH shall be responsible for notifying individuals affected by the breach unless it has been previously agreed (i.e., in Business Associates Agreement) that the business associate will perform necessary breach notifications.

B. Related Policies

Board Policy #01-002-0020, Corporate Compliance Complaint, Investigation & Reporting Process and Non-Retaliation

Administrative Policy 03-002-0025, Consent Forms

Administrative Policy 03-002-0030, Release of Case Record Information

Administrative Policy #05-002-0006, Informed Consent, Consent for Treatment, and Information Distribution

Administrative Policy #06-001-0055, Personnel: Corrective/Disciplinary Action

Administrative Policy 08-002-0005, Access, Use, and Disclosure of Confidential Information and Protected Health Information (PHI)

C. Definitions

1. *Breach*: The impermissible acquisition, access, use, or disclosure of *unsecured PHI* which compromises the security or privacy of the PHI.
2. *Business Associate*: A person or entity that performs or assists in the performance of a function or activity on behalf of SCCCMH that involved access, use, or disclosure of PHI by the Business Associate. SCCCMH must have a written business associate contract that establishes specifically what the Business Associate has been engaged to do.
3. *Covered Entity*: An individual, organization, or agency that must comply with HIPAA, including healthcare providers, health plans, and healthcare clearing houses. A covered entity may be a *business associate*. Region 10 PIHP and SCCCMH are both covered entities.
4. *Incident:* An event reported to the HIPAA Privacy Officer or Corporate Compliance Office that results in an investigation to determine the possibility of an impermissible use or disclosure of (PHI). An investigation will determine whether an Incident is a *Violation*, or a *Breach*, or neither of those.
5. *Individually Identifiable Health Information:* Information that is a subset of health information, including demographic information collected from an individual, that: (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; or the provision of health care to an individual; or the past, present, or future *payment* for the provision of health care to an individual; and (i) That identifies the individual; or (ii) that a person would reasonably believe can be used to identify the individual.
6. *Payment:* The various activities of health care providers to obtain payment or be reimbursed for services and of a health plan to obtain premiums, to fulfill coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

7. *Protected Health Information (PHI): Individually Identifiable Health Information* that a HIPAA *Covered Entity* transmits by electronic media, maintains in electronic media, or transmits or maintains in any other form or medium including paper.
8. *Unsecured Protected Health Information (PHI):* PHI that has not been secured through the use of a technology or methodology considered by the Department of Health and Human Services (HHS) as sufficient to render the information unusable, unreadable, or indecipherable to individuals by encryption and destruction methods identified in the HIPAA Security Rule and in accordance with the National Institute of Standards and Technology (NIST).
9. *Violation:* When unsecured PHI was acquired, used, or disclosed in a manner not permitted by the HIPAA Privacy or Security Rules. A violation is presumed to be a Breach unless it meets the definition of a Breach exception, or a completed risk assessment tool demonstrates low probability that the PHI has been compromised.
10. All other terms used in this policy have the same meaning as those terms in HIPAA, Public Law 104-191, the regulations at 45 CFR Parts 160, 162, and 164.

D. Forms

N/A

E. Other Resources (i.e., training, secondary contact information, exhibits, etc.)

Exhibit A: SCCCMH Breach Notification Individual Letter Template

Exhibit B: SCCCMH Breach Notification MDHHS Letter Template

Exhibit C: SCCCMH Breach Notification Media Release Template

Exhibit D: SCCCMH Notification to PIHP

F. References

1. Health Insurance Portability and Accountability Act of 1996 (HIPAA)
2. Privacy Standards 45 CFR Parts 160 & 164
3. HITECH Act of the American Recovery and Reinvestment Act (ARRA) of 2009
4. Confidentiality of Substance Use Disorder (SUD) Patient Records at 42 CFR part 2
5. Michigan Mental Health Code, Sections 330.1748 and 330.1749
6. Protected Health Information (PHI) Consent Tool

IV. History

- Initial Approval Date: 06/2002
- Last Revision Date: 04/2025 BY: Joy Vittone
- Last Reviewed Date: 09/2024 BY: Tommy Rankin and Joy Vittone
- Non-Substantive Revisions: N/A
- Key Words: breach, notification, disclosure, PHI, protected health information, report, notify, HIPAA, privacy, confidential,