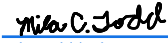




Section: Compliance	Procedure Name: Breach Oversight: Risk Assessment	Procedure #: P10.16.01
Overarching Policy: 10.16 Breach Team Program Oversight		
Owner: Chief Compliance Officer	Reviewed By: Mila C. Todd	Total Pages: 5
Required By: <input checked="" type="checkbox"/> BBA <input type="checkbox"/> MDHHS <input type="checkbox"/> NCQA <input checked="" type="checkbox"/> Other (please specify): <u>HIPAA/HITECH</u>	Final Approval By:  <u>Mila Todd (Jul 31, 2024 15:19 EDT)</u>	Date Approved: Jul 31, 2024
Application: <input checked="" type="checkbox"/> SWMBH Staff/Ops <input type="checkbox"/> Participant CMHSPs <input type="checkbox"/> SUD Providers <input type="checkbox"/> MH/IDD Providers <input type="checkbox"/> Other (please specify): _____	Line of Business: <input checked="" type="checkbox"/> Medicaid <input type="checkbox"/> Other (please specify): <input checked="" type="checkbox"/> Healthy Michigan _____ <input checked="" type="checkbox"/> SUD Block Grant <input checked="" type="checkbox"/> SUD Medicaid	Effective Date: 4/4/2019

Policy: Pursuant to 42 CFR 164.402(2), an impermissible use or disclosure of PHI is presumed to be a breach and therefore requires notification to the customer and the Office of Civil Rights (OCR) unless either of the following apply:

1. The use or disclosure satisfies one or more of three regulatory exceptions as prescribed by 42 CFR 164.402(1)(i)-(iii); or
2. Upon completion of a risk assessment, it is determined that there is a low probability that the PHI has been compromised.

A breach is treated as discovered as of the first day on which such breach is known to SWMBH or, by exercising reasonable diligence, would have been known to SWMBH or any person, other than the person committing the breach, who is a workforce member or agent of SWMBH. The Breach Notification Rules prescribe specific reporting time frames and thus, time is of the essence. As a result, all workforce members who believe that PHI may have been impermissibly used or disclosed are required to notify the SWMBH Chief Compliance Officer or his/her designee immediately. Workforce members will further cooperate in the Breach Risk Teams' fulfillment of its duties, including cooperating with reporting investigations, mitigation steps, and any required corrective action.

Purpose: SWMBH shall comply with Federal and State regulations concerning responding to impermissible uses and/or disclosures of Protected Health Information. The Procedure outlines



the steps that the Breach Risk Team (BRT) will take in performing a Breach Risk Assessment in order to determine SWMBH's obligations under HIPAA and HITECH.

Scope: All

Responsibilities: SWMBH's Program Integrity and Compliance Department shall investigate all reports of unauthorized uses and/or disclosures of PHI.

SWMBH's Breach Risk Team shall evaluate the investigation documents for reported impermissible uses and/or disclosures of PHI and complete a Breach Response Risk Assessment when indicated.

Definitions: See SWMBH Policy 10.16 Breach Team Program Oversight

Procedure:

- A. **Investigation:** The SWMBH Program Integrity & Compliance department will investigate all reports of impermissible use and/or disclosure of protected health information. The investigation may consist of interviews, documentation collection and review, and requiring mitigating action to prevent further impermissible uses or disclosures of PHI. All reports and documents will be reviewed by the BRT at its next regularly scheduled meeting.
- B. **Unauthorized Use or Disclosure:** After reviewing the investigation documentation, the BRT will determine if an impermissible use and/or disclosure of PHI occurred, and may consider the following, or other applicable factors:
 1. Whether the PHI was disclosed to only the correct recipient(s);
 2. If sent via email, whether it was encrypted via [ecrypt] and if not, if Transport Layer Security (TLS) encryption can be confirmed;
 3. Whether there is a Release of Information on file.
- C. **Exceptions:** If the BRT determines that an impermissible use and/or disclosure occurred, the BRT will then determine if an exception applies, such that the unauthorized use or disclosure would not amount to a breach. The three regulatory exceptions prescribed by 42 CFR §164.402(1)(i)-(iii) are as follows:
 1. Unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of SWMBH or its Business Associate (BA) if such acquisition, access or use was in good faith and in the scope of authority and does not result in further use or disclosure in a manner not permitted by the Privacy Rule.
 2. Inadvertent disclosure of PHI from a person who is authorized to access PHI at SWMBH or a BA to another person authorized to access PHI at the same entity.
 3. Good faith belief by SWMBH that the unauthorized person to whom disclosure was made would not reasonably have been able to retain such information.



If the BRT determines an exception applies, it will document why the impermissible use or disclosure falls within an exception and take any necessary corrective action.

If the BRT determines that the incident does not fit into an exception, then it will complete a Risk Assessment.

D. **Risk Assessment:** The BRT will complete the SWMBH Breach Response Risk Assessment Tool for all impermissible uses and/or disclosures that do not fall under an exception listed above. The BRT will use the Risk Assessment to assist in determining if a breach compromises the security or privacy of the subject PHI and poses a significant risk to the financial, reputational, or other harm to the customer or entity to the extent that it requires notification to the affected individual(s). The Risk Assessment Tool shall address the following factors:

1. Whether an unauthorized disclosure of PHI occurred;
2. The level of probability that the PHI in question was compromised, based on consideration 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 PHI 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.
3. Whether notification under the Breach Notification Rule is required; and
4. Whether corrective action is necessary to address business processes, employee behavior, or other elements that factored into the impermissible disclosure.

The BRT shall consider any additional factors based on the circumstances. A low score on the Risk Assessment Tool will not necessarily trigger notice obligations, but a high score near a 19 would likely indicate a need for notification. Based on the Risk Assessment and any additional factors, the BRT will determine whether the incident presents a low probability of compromise, or whether there is a need for notification.

E. **Reporting Obligations:** If the BRT determines, after completion of a Risk Assessment, that notification is required under the Breach Notification Rule, the Chief Compliance Officer or his/her designee will follow the procedures set out in SWMBH Operating Procedures 10.16.02 Breach Oversight: Breach Notification Procedures.

F. **Corrective Action:** The BRT shall review the circumstances and determine if Corrective Action is warranted to address business processes, employee behavior, or other elements that factored into the impermissible disclosure. Corrective Action recommendations shall be reported to the Compliance Oversight Committee for review at its next regulatory scheduled meeting.



G. **Compliance Oversight Committee Review:** The BRT's findings shall be reported to the SWMBH Compliance Oversight Committee for discussion at its next regularly scheduled meeting. The Compliance Oversight Committee may undertake a review and evaluation of any completed Risk Assessment. The Compliance Oversight Committee may review the factors required by the Risk Assessment and make a final determination as to whether there is a low probability of compromise to the subject PHI, or whether breach notification is required.

The Compliance Oversight Committee should make recommendations and propose policies that are necessary to take any corrective actions.

References:

42 CFR 164.402

SWMBH Operating Procedure 10.16.02 Breach Oversight: Breach Notification Procedures

Attachments: P10.16.01A Breach Response Risk Assessment Tool

P10.16.01 Breach Oversight - Risk Assessment

Final Audit Report

2024-07-31

Created:	2024-07-31
By:	Paige Pfaff (paige.pfaff@swmbh.org)
Status:	Signed
Transaction ID:	CBJCHBCAABAADf681zmM9idKeeVeb8ITNEloRoh87pqu

"P10.16.01 Breach Oversight - Risk Assessment" History

-  Document created by Paige Pfaff (paige.pfaff@swmbh.org)
2024-07-31 - 7:17:25 PM GMT- IP address: 104.159.231.26
-  Document emailed to Mila Todd (mila.todd@swmbh.org) for signature
2024-07-31 - 7:17:54 PM GMT
-  Email viewed by Mila Todd (mila.todd@swmbh.org)
2024-07-31 - 7:19:34 PM GMT- IP address: 104.47.51.126
-  Document e-signed by Mila Todd (mila.todd@swmbh.org)
Signature Date: 2024-07-31 - 7:19:47 PM GMT - Time Source: server- IP address: 50.124.35.84
-  Agreement completed.
2024-07-31 - 7:19:47 PM GMT