Section: **Compliance**	Procedure Name: **Breach Oversight: Breach Notification**	Procedure #: **P10.16.02**
Overarching Policy: **10.16 Breach Team Program Oversight**		
Owner: **Chief Compliance Officer**	Reviewed By: **Mila C. Todd**	Total Pages: **5**
Required By: ☒ **BBA** ☐ **MDHHS** ☐ **NCQA** ☒ **Other (please specify): HIPAA/HITECH**	Final Approval By: Mila C. Todd	Date Approved: **1/13/2022**
Application: ☒ **SWMBH Staff/Ops** ☐ **Participant CMHSPs** ☐ **SUD Providers** ☐ **MH/IDD Providers** ☐ **Other (please specify):** _____	Line of Business: ☒ **Medicaid** ☒ **Healthy Michigan** ☒ **SUD Block Grant** ☒ **SUD Medicaid** ☒ **MI Health Link** ☐ **Other (please specify):** _____	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. This Procedure outlines the steps that

SWMBH will take in the event that an impermissible use and/or disclosure is determined by the BRT to be a breach that requires reporting under the Breach Notification Rules at 42 CFR §§164.400-414. SWMBH's breach notification process will be carried out in compliance with applicable Breach Notification Rules, and all other applicable rules and regulations.

Scope: HIPAA requires notification to individuals whose unsecured PHI has been impermissibly accessed, acquired, used or disclosed when such impermissible access (etc.) compromises the security or privacy of the PHI. The breach notification requirements only apply to breaches of unsecured PHI (§164.404(a)). If PHI is encrypted or destroyed in accordance with the applicable regulatory guidance, there is a "safe harbor" and notification is not required.

Responsibilities: SWMBH's Breach Risk Team shall evaluate the investigation documents for reported unauthorized uses and/or disclosures of PHI and complete a Breach Response Risk Assessment when indicated, determining whether notification is required.

SWMBH's Program Integrity and Compliance Department shall ensure notification is accomplished and documented.

Definitions: See SWMBH Policy 10.16 Breach Team Program Oversight

Procedure:

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

This letter will be sent by first-class mail to the individual at the last known address of the individual. The notification shall be provided in one or more mailings as information is available. If SWMBH 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. 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 SWMBH's website, or a conspicuous notice in major print or broadcast media in SWMBH'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.

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 SWMBH 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 SWMBH to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.

B. **Notification: HHS:** In the event a breach of unsecured PHI affects 500 or more of SWMBH's consumers, the Secretary of Health and Human Services (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 SWMBH's consumers are affected, SWMBH 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.
C. **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.
D. **Delay of Notification Authorized for Law Enforcement Purposes:** If a law enforcement official states to SWMBH or a business associate that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, SWMBH 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.

References: SWMBH Operating Policy 10.16 Breach Team Program Oversight
42 CFR 164.400-414 (Breach Notification Rules)

Attachments: P10.16.02A SWMBH Breach Notification Letter

Southwest Michigan Behavioral Health

Revision History

Revision #	Revision Date	Revision Location	Revision Summary	Revisor
1	1/13/2022	Entire document	Moved to new template	Mila C. Todd

Principal Office: 5250 Lovers Lane, Suite 200, Portage, MI, 49002
P: 800-676-0423
F: 269-488-8270

BREACH NOTIFICATION

[Date]

[Customer Name/Address]

Dear [customer]:

On [date], Southwest Michigan Behavioral Health discovered that a breach of your protected health information occurred. Specifically, [describe facts specific to the incident]. The unsecured protected health information breached included [describe specific PHI breached].

SWMBH's Breach Response Team, in conjunction with the Program Integrity and Compliance Team, are working together to further investigate the breach, mitigate the harm to consumers, and ensure protection against future breaches of this nature. Specifically, [describe efforts being taken to mitigate/correct]. In an effort to be proactive, we recommend that you take additional steps to protect yourself from potential harm resulting from the breach. Those recommended steps include abstaining from giving out additional information over phone, not sending any personal information over email or through postal service to anyone you do not know personally, and call SWMBH if you feel that your information has been used by someone other than yourself.

We understand that you may have questions and concerns as a result of this letter, and we are ready and willing to do whatever is necessary to assist you. Please direct all of your questions and concerns to the contact information listed below.

Sincerely,

Mila C. Todd, Esq., CHC
SWMBH Chief Compliance & Privacy Officer
Southwest Michigan Behavioral Health
5250 Lovers Lane, Suite 200
Portage, Michigan 49002
mila.todd@swmbh.org
P: 800-676-0423