Southwest Michigan BEHAVIORAL HEALTH

Section: **Compliance**	Policy Name: **Breach Team Program Oversight**	Policy Number: **10.16**
Owner: **Chief Compliance & Privacy Officer**	Reviewed By: **Mila Todd**	Total Pages: **5**
Required By: ☐ **BBA** ☐ **MDHHS** ☐ **NCQA** ☒ **Other (please specify):** _____	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: **6/5/2020**

Policy:

A. **Regulatory Framework & Workforce Responsibilities:**

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

B. **Breach Risk Team:** SWMBH will maintain a Breach Risk Team (BRT) that will meet on a periodic basis, as defined by its members, to respond to suspected or confirmed breaches of PHI. The BRT will complete a risk assessment to assist in determining if an impermissible use or disclosure of PHI 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 it would require notification to the

affected individual(s). In fulfilling its duties, the BRT will adhere to relevant SWMBH procedures as set out below.

C. **Procedures:** SWMBH shall maintain Operating Procedures that address the following:
   1. Risk Assessment factors and process;
   2. Breach Notification requirements and processes; and
   3. Corrective Action standards and guidelines for consistent and tailored enforcement.

D. **Administrative Requirements:** SWMBH shall comply with the following requirements, as outlined by 42 CFR §164.530:
   1. **Workforce Training:** SWMBH shall train all members of its workforce on its 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 actual and suspected breaches within SWMBH consistent with SWMBH Operating Policy 10.6 Compliance Reporting Responsibilities.
   2. **Complaints:** SWMBH provides a process for individuals to make complaints concerning SWMBH's privacy policies and procedures or its compliance with such policies and procedures. Individuals also have the right to complain about SWMBH's breach notification processes.
   3. **Sanctions:** Members of SWMBH's workforce who fail to comply with this policy, and related procedures, and any other Compliance/privacy policies and/or procedures shall be subject to disciplinary action, up to and including termination.
   4. **Retaliation/Waiver**: SWMBH 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.
   5. **Burden of Proof:** SWMBH has the burden of proof for demonstrating that all notifications were made as required or that the impermissible use or disclosure of PHI did not constitute a breach.

E. **Maintenance of Breach Information:** SWMBH shall maintain a process to record or log all breaches of unsecured PHI, regardless of the number of consumers 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 patients 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 patients regarding the breach.
   4. Steps taken to mitigate the breach and prevent future occurrences.

F. **Document Retention:** All documentation related to breach investigations, Risk Assessments, required notifications, and corrective actions shall be retained in compliance with the SWMBH Compliance Documentation Retention Policy.

Purpose: Southwest Michigan Behavioral Health (SWMBH) will comply with Federal and State regulations concerning responding to unauthorized uses and/or disclosures of Protected Health Information (PHI). Specifically, SWMBH will have policies and procedures in place to comply with the Breach

Southwest Michigan
BEHAVIORAL HEALTH

Notification Rules of the Health Insurance Portability and Accountability Act (HIPAA), 45 CFR §164.400-414, and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act).

Scope: SWMBH and SWMBH Business Associates

Responsibilities: SWMBH Program Integrity & Compliance Department is responsible for investigating reported incidents, gathering supporting documentation, and providing it to the Breach Team.

SWMBH's Breach Team is responsible for meeting monthly, as needed, to review reported incidents and determine necessary action, if any.

SWMBH staff and Business Associates are responsible for reporting any actual or suspected unauthorized uses and or disclosures of Protected Health Information to SWMBH's Program Integrity & Compliance Department as soon as possible after learning of it.

Definitions:

Breach – The acquisition, access, use or disclosure of protected health information (PHI) in a manner not permitted under the Health Insurance Portability and Accountability Act and the Privacy Rule which compromises the security or privacy of PHI.

Protected Health Information (PHI) – has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations.

Risk Assessment- a Risk Assessment is to be completed after a Breach to determine whether there is a low probability that the PHI has been compromised, which will determine whether the breach notifications are applicable. A Risk Assessment consists of at least the following four factors: (1) the nature and extent of protected health information involved, (2) the identity of the unauthorized person that accessed the protected health information, (3) whether the protected health information was actually acquired or viewed, and (4) the extent to which the risk to the protected health information has been mitigated. In addition, given the circumstances of the impermissible use or disclosure, additional factors may need to be considered to appropriately assess the risk that PHI has been compromised.

Upon completion of the Risk Assessment, the Breach Risk Team must address each factor as well as additional factors and then evaluate the overall probability that the PHI has been compromised, considering all the factors in combination. The risk assessment must be thorough, competed in good faith, and the conclusions reached must be reasonable.

Unsecured Protected Health Information – PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance. Examples of methods to render PHI unusable, unreadable, or indecipherable include: valid

encryption processes consistent with NIST Publications for data at rest and for data in motion; destruction of media on which PHI is stored or recorded by either shredding/destroying such that the PHI cannot be read or otherwise reconstructed for paper, film, and other hard copy media; or clearing, purging, or otherwise destroying consistent with NIST Publications for electronic media.

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

References:

42 CFR §§164.400-414 (Breach Notification Rules)
42 CFR §164.530 (Administrative Requirements)
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)

Attachments:

A. 10.16A Breach Response Risk Assessment Tool
B. P10.16.02A Breach Notification Letter

Southwest Michigan
BEHAVIORAL HEALTH

Revision History

Revision #	Revision Date	Revision Location	Revision Summary	Revisor
Initial	6/5/2020	Throughout policy	New template	A. Wood
1	1/13/2022	N/A	Annual review	Mila C. Todd

Southwest Michigan Behavioral Health Breach Response Risk Assessment Tool

Breach Response Team Directives

Date:

Incident #:

Core Members	Absent	Reportable	Not Reportable
Ad hoc Members			

- ☐ Automatic Notification
- ☐ Notification not indicated
- ☐ Notification indicated-Initiate process
  - ☐ Affected Individuals
  - ☐ Attorney General
  - ☐ Credit Reporting Agencies
  - ☐ Media
  - ☐ Website
  - ☐ Dept. Of Health and Human Services
- ☐ File Police Report
- ☐ Initiate Credit Monitoring
- ☐ Other

Breach Risk Assessment Tool (BRAT)

Purpose: To assist in determining if a substantiated breach presents a compromise to the security and/or privacy of the PHI ***and*** poses a significant risk to the financial, reputational or other harm to the individual or entity, to the extent it would require notification to the affected individual(s).

Note: Any external disclosure to a non-covered entity containing a person's first name or first initial and last name in combination with the person's social security number are automatically considered as reportable security breaches.

Directions: To complete the blank field forms simply click on the gray area and enter the information. Justify the reasoning of your determination in the "Comments/Mitigation" section.

Incident #: Entity: Department: Date of Event: Date Reported: Date Investigation Completed: Number of individuals affected:	Completed By: Date Completed:
Brief Summary of the issue:	

Source of disclosure-Business Associate	**Yes**	**No**
Was a breach committed by us as a business associate? (yes/no)		
Was a breach committed by our Business Associate? (yes/no)		
Date Covered Entity made aware of the breach? (if applicable)		

Section One

Does incident qualify as an exception?	Y/N
Good faith, unintentional acquisition, access or use of PHI by employee/workforce member or a 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 unpermitted use or disclosure. Example: A billing employee receives and opens an email containing PHI about a patient which a nurse mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the nurse of the misdirected email, and then deletes it. (same employer)	
Inadvertent disclosure by a person who is authorized to access PHI at a covered entity or BA to another person authorized to access PHI at the same covered entity or BA and the inadvertent disclosure does not result in further unpermitted use or disclosure.	
A disclosure of PHI where there is a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.	

If "Yes" to one or more of the above, articulate reasoning below and do not proceed:

If "No" to all of the above, notice may be required under HIPAA. Proceed to Section 2.

45 CFR 164.402(2) – Except as provided in paragraph (1) of this definition (the exceptions listed above), an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the protected health information or to whom the disclosure was made;

(iii) Whether the protected health information was actually acquired or viewed; and

(iv) The extent to which the risk to the protected health information has been mitigated.

Section Two

Variable	Options	Level	Score
Method of disclosure	• Unauthorized *internal* acquisition, access and/or use without disclosure outside the organization	**0**	
	• Verbal Disclosure • View Only	**1**	
	• Paper	**2**	
	• Electronic (including faxes)	**3**	
Recipients(s)	• No Information Received	**0**	
	• Our Business Associate • Another Covered Entity • Internal Workforce	**1**	
	• Wrong payer (not the patients) • Unauthorized family member	**2**	
	• Unknown/Lost/Stolen • Non-Covered entity, member of the general public, media, etc.	**3**	
Circumstances of release	• Information accessible but not released	**0**	
	• Unintentional disclosure	**1**	
	• Intentional use/access w/o auth • Intentional disclosure w/o auth • Loss/Theft	**2**	
	• Using false pretense to obtain or disclose • Obtained for personal gain/malicious harm • Hacked/Targeted data theft	**3**	
Disposition	• Information accessible but not released	**0**	
	• Information returned complete • Information properly destroyed (attested) • Information could not reasonably be retained	**1**	

	• Information properly destroyed (unattested) • Electronically Deleted (unsure of back up status)	**2**	
	• Media • Unable to retrieve • Unsure of disposition or location • High (redisclosed or suspected redisclosure)	**3**	
Additional Controls	• Information accessible but not released	**0**	
	• Data Wiped • Encrypted/Destroyed • Physical/Policy Controls	**1**	
	• Password protected-not compromised • No Controls	**2**	
	• Password protected-compromised • No Controls or Unencrypted • Other (Explain in Comments)	**3**	

Total: Section One	Add highest score from each subsection	

Section Three (Choose one)

Below are general guidelines for ranking levels of risk for different types of information breached. **The circumstances surrounding each breach may impact how you will rank the risk level for the data breached.**			
Variable	**Level of Risk**	**Options**	**Assigned Score**
Type of information Breached	**1**	**Lowest Risk- Financial, Reputational & Other Harm** • Limited Data Set (evaluate possibility of re-identification if ZIP Code and/or DOB included **and** • Only identifier are breached that are **not** defined under the Michigan Identity Theft Protection Act and no other health information is breached. For example: name, address, city, state, telephone number, fax number, email address, admission/discharge dates, service dates, and/or date of death	

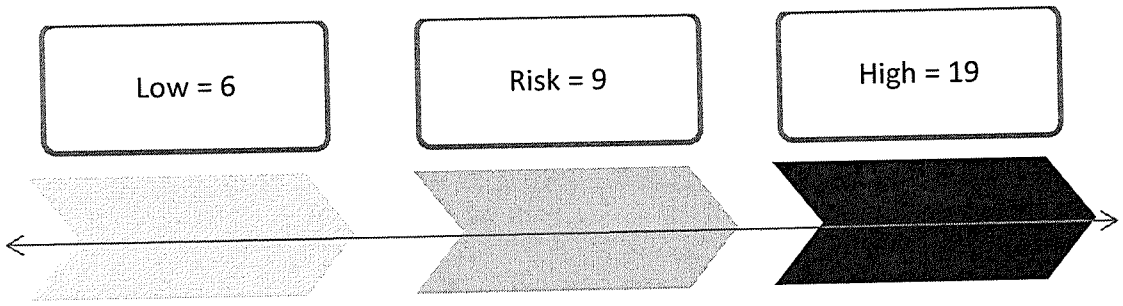
	2	**Medium Risk- Financial, Reputational & Other Harm** • Non-Sensitive Protected Health Information which may include information about treatment, diagnosis, service, medication, etc...(Evaluate closely the possibility of the information causing harm to the persons(s) impacted by the breach, because the information may not typically fall under our definition of sensitive information, but looking at the circumstances it may still cause harm.)	
	3	**High Risk** • The person's first name or first initial and last name in combination with **any one** of the following **(Score a 4 if in combination with more than one) ○ Social Security or employer taxpayer ID numbers ○ Driver's license, State ID care, or passport numbers ○ Checking/savings account numbers, credit card number, Debit card numbers ○ Personal Identification (PIN) Code ○ Electronic identification numbers, electronic mail names or addresses ○ Internet account numbers, or Internet identification names ○ Digital signatures, biometric data, fingerprints ○ Passwords ○ Any other numbers or information that can be used to access a person's financial resources ○ Parent's legal surname prior to marriage	
	4	**Highest Risk** • The person's first name or first initial and last name in combination with: ○ Sensitive Protected Health Information such as information about sensitive diagnosis such as HIV, Substance Abuse, and/or Mental Health. ○ More than one "high risk" combination	
Total: **Section Two**		Enter highest score from above	

Escalators and Minimizers

Escalator (+5)	• Believable threat of reporting to patient/regulatory body – asserted.	
Minimizer (-5)	• Self-reported, no indication of further reporting/ disclosure.	

The range of scoring is meant to serve as a guide in your decision making and is not designed to make the decision for you. There are a variety of factors and mitigations that may take place in your incident that this tool cannot foresee or predict.

The range of scoring is 6-19. A low score of 6 does not necessarily trigger notice obligations but a high score of or near 19 would likely indicate either a need to notify or a need to take other actions.



Enter Combine Risk Score: **Sections one and Two plus/minus Escalators and Minimizers**	

Comments/Mitigations- Additional information considered:

Section Four

Michigan Identity Theft Protection Act Assessment

"Personal Information"	Y/N
Did the information include a person's first name/initial and last name in combination with any of the following? (Yes/No) ○ Social Security or employer taxpayer ID numbers ○ Driver's license, State ID care, or passport numbers ○ Checking/savings account numbers, credit card number, Debit card numbers ○ Personal Identification (PIN) Code ○ Electronic identification numbers, electronic mail names or addresses ○ Internet account numbers, or Internet identification names ○ Digital signatures, biometric data, fingerprints ○ Passwords ○ Any other numbers or information that can be used to access a person's financial resources ○ Parent's legal surname prior to marriage	

If "NO" Stop Here

Was the information illegally used or is reasonably likely to be used illegally? (Yes/No)	
Is the disclosure reasonably likely to create a material risk of harm to a consumer to the extent it would require notification to the affected individual? (Yes/No) ****Note: Any unencrypted electronic data sent over the internet which contains a person's first name or first initial and last name combination with the person's social security number is automatically considered a reportable breach.**	

If "NO" to both of the above Stop Here

If "Yes" follow requirements of the Michigan Identity Theft Protection Act 452 of 2004, determined by the Breach Response Team.

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