Southwest Michigan BEHAVIORAL HEALTH

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: ☒ **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. 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 10.16.2 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. In determining appropriate corrective action, the BRT shall adhere to SWMBH Operating Procedures 10.16.3 Breach Oversight: Corrective Action Procedures

for its recommendations. Corrective Action recommendations shall be reported to the Compliance Oversight Committee for review and its next regulatory scheduled meeting.

G. **Compliance Oversight Committee Review:** The BRT's findings on completed Risk Assessments will be taken 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 10.16.2 Breach Oversight: Breach Notification Procedures
SWMBH Operating Procedure 10.16.3 Breach Oversight: Corrective Action Procedures

Attachments: P10.16.01A Breach Response Risk Assessment Tool

Southwest Michigan
BEHAVIORAL HEALTH

Revision History

Revision #	Revision Date	Revision Location	Revision Summary	Revisor
1	1/13/2022	Procedure, paragraph B Entire document.	Updated "encryptnow" to [ecrypt] for manual encryption method. Moved to new template.	Mila C. Todd

Southwest Michigan Behavioral Health Breach Response Risk Assessment Tool

Breach Response Team Directives

Date:

Incident #:

Core Members	Absent	Reportable	Not Reportable
Randy Paruch			
Petra Morey			
Beth Guisinger			
Courtney Juarez			
Tracy Dawson			
Mila Todd			
Ad hoc Members			

DISPOSITION

☐ Not an unauthorized use/disclosure:
- ☐ Exception applies
- ☐ OTHER: _____

_____

☐ Notification not indicated
- ☐ Low probability of compromise rationale: _____

_____

☐ Notification indicated – initiate process:
- ☐ Affected Individuals
- ☐ Attorney General
- ☐ Credit Reporting Agencies
- ☐ Media (more than 500 individuals effected)
- ☐ Website
- ☐ HHS Office for Civil Rights (OCR)
  - ☐ Within 60 days of discovery (500 or more individuals effected)
    DATE REPORTED: _____
  - ☐ Within 60 days of the end of the calendar year in which the breach was discovered
    DATE REPORTED: _____

☐ Additional Mitigation Steps Taken
- ☐ 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: SWMBH Department: Compliance Date of Event: Date Reported: Date Investigation Completed: Number of individuals affected:	Completed By: Date Completed:

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 payor (not the patients) • Unauthorized family member	2	
	• Unknown/Lost/Stolen • Non-Covered entity, member of the general public, media, etc.	3	
Circumstances of release/Intention of individual using or disclosing the information	• 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	3	

	• High (redisclosed or suspected redisclosure)		
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 Two	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	

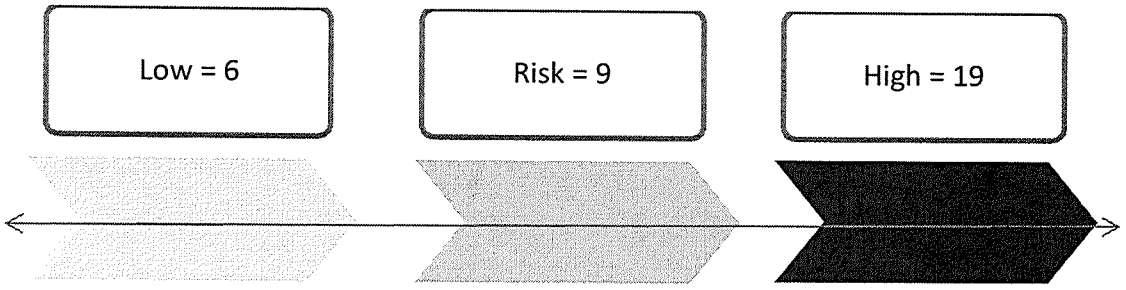
		definition of sensitive information, but looking at the circumstances it may still cause harm.)	
	3	**High Risk** • The person's first name or first initial <u>and</u> last name in combination with **<u>any one</u>** of the following **(Score a 4 if in combination with more than one) ○ Social Security 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 <u>or</u> first initial <u>and</u> 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 Three**		Enter highest score from above	

<u>Escalators and Minimizers</u>

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.