Subject: Breach Team Program Oversight	Accountability: Compliance	Effective Date: 8/27/2014	Pages: 3
REQUIRED BY: BBA Section _____ PIHP Contract Section _____ NCQA/URAC Standard _____ Other _____		Last Reviewed Date: 10/4/18	Past Reviewed Dates: 8/27/15 11/21/16 5/17/17
LINE OF BUSINESS: ☒ Specialty Waiver (B/C) ☒ 1115 Waiver ☒ Healthy Michigan ☒ SUD Medicaid ☒ SUD Block Grant ☒ MI Health Link ☐ OTHER: _____	APPLICATION: ☒ SWMBH Staff and Ops ☐ Participant CMHSPs ☐ SUD Providers ☐ MH / DD providers ☐ Other:_____	Last Revised Date: 10/4/18	Past Revised Dates: 11/21/16 5/17/17
Approved : Mila C. Todd Date: 10-11-18		Required Reviewer: Chief Compliance & Privacy Officer	

I. 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 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).

II. Policy

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

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);
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.

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.

III. 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.

IV. 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)

V. Attachments

A. SWMBH Operating Procedure 10.16.1 Breach Oversight: Risk Assessment Procedures
    1. 10.16.1A SWMBH Breach Risk Assessment Tool
B. SWMBH Operating Procedure 10.16.2 Breach Oversight: Breach Notification Procedures
    2. 10.16.2A SWMBH Breach Notification Letter
C. SWMBH Operating Procedure 10.16.3 Breach Oversight: Corrective Action Procedures