VAN BUREN COMMUNITY MENTAL HEALTH AUTHORITY
POLICIES & PROCEDURES

Title: Breach Team Program Oversight
Originated: 2/13/25
Number: I.06.16
Approved By: Executive Team

DIRECTIVE:

This procedure shall serve as a guideline to ensure that VBCMH will comply with Federal and State regulations concerning responding to unauthorized uses and/or disclosures of Protected Health Information (PHI). VBCMH 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).

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 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, completed 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 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 VBCMH, whether or not they are paid by VBCMH.

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);
        - 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.
    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 VBCMH or, by exercising reasonable diligence, would have been known to VBCMH or any person, other than the person committing the breach, who is a workforce member of VBCMH. 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 VBCMH Compliance Officer or their 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:

VBCMH 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 Breach Risk Team (BRT) will adhere to relevant VBCMH procedures as set out below.

The VBCMH Risk Response Team will utilize the Breach Notification Assessment Tool 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). VBCMH Breach Risk Team is responsible for meeting monthly, as needed, to review reported incidents and determine necessary action, if applicable.

C. Operating Procedures:

VBCMH shall maintain Operating Procedures that address the following:

1. Risk Assessment factors and process
2. Breach Notification factors and process

D. Administrative Requirements:

VBCMH shall comply with the following requirements, as outlined by 42 CFR §164.530:

1. **Workforce Training**: VBCMH 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 the VBCMH consistent with VBCMH Reporting of Potential Compliance Violations Policy 1.06.05.
2. **Complaints**: VBCMH provides a process for individuals to make complaints concerning VBCMH's privacy policies and procedures or its compliance with such policies and procedures, as well as the Breach notification processes.
3. **Sanctions**: Members of VBCMH 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.

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 Insurance Technology for Economic and Clinical Health Act of 2009 (HITECH)
Breach Notification Risk Assessment Tool
Breach Notification Letter