VAN BUREN COMMUNITY MENTAL HEALTH AUTHORITY
POLICIES & PROCEDURES

Title: Breach Assessment and Notification
Number: I.06.15
Originated: 01/24/19, 2/13/25
Approved By: Executive Team

PURPOSE: VBCMH shall comply with Federal and State regulations concerning responding to impermissible uses, and/or disclosures of Protected Health Information (PHI). This procedure outlines the steps that VBCMH will take to assess risk in the event that impermissible use and/or disclosure occurs. A Breach Risk Team as appointed by the CEO determines if a breach requires reporting under the Breach Notification Rules at 42 CFR §§164.400-414. VBCMH's breach notification process and reporting will be carried out in compliance with applicable Breach Notification Rules and all other applicable rules and regulations.

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 the 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 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 VBCMH or be 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.

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. Corrective action may be necessary to address business processes, staff behavior, or other elements that factored into, or otherwise contributed to, an impermissible use and/or disclosure of PHI.

Responsibilities: VBCMH's Breach Risk Team shall evaluate the investigation documents for reported unauthorized uses and/or disclosures of PHI and complete a Breach Notification Risk

Assessment when indicated, determining whether notification is required. VBCMH's Compliance Department shall ensure notification is accomplished and documented.

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 (HIPAA) and the Privacy Rule which compromises the security of privacy or PHI.

Protected Health Information (PHI): Individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or medium, whether electronic, on paper, or oral, as defined in section 160-103 of Title 45, Code of Federal Regulations.

Risk Assessment: A Risk Assessment consists of at least the following four factors: (1) the nature and extent of PHI involved, (2) the identity of the unauthorized person(s) who may have accessed the PHI, (3) whether the PHI was actually acquired or viewed, and (4) the extent to which the risk to the PHI 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. A Risk Assessment will be completed after an actual or suspected breach to determine the probability that PHI has been compromised in order to determine whether Breach notifications are applicable.

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 a technology or methodology specified by the Secretary of HHS. 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 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.

PROCEDURE:

A. **Notification: Affected Individuals**

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

Notifications will be sent by first-class mail to individuals at their last known address. Multiple notifications may be sent, based on availability of information. If VBCMH knows that an affected individual is deceased, written notification by first-class mail will be sent to the next of kin or personal representative, if such address is on file.

If there is insufficient or out-of-date contact information that precludes direct written 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 VBCMH's website, or a conspicuous notice in major print or broadcast media in VBCMH'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 their 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 VBCMH 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 VBCMH 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 VBCMH's customers, 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 VBCMH's customers are affected, VBCMH 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 VBCMH or a business associate that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, VBCMH 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

VBCMH Policy I.06.14 Compliance Monitoring/Staff Access
42 CFR §§164.400-414 (Breach Notification Rules)
VBCMH Policy 1.06.16 Breach Team Program Oversight
Breach Notification Risk Assessment Tool