BAY-ARENAC BEHAVIORAL HEALTH AUTHORITY
POLICIES AND PROCEDURES MANUAL

Chapter: 13	**Corporate Compliance**		
Section: 1	**HIPAA**		
Topic: 13	**Breach Notification**		
Page: 1 of 10	**Supersedes Date:** **Pol:** **Proc: 10-23-15, 2-20-14**	**Approval Date:** **Pol: 2-20-14** **Proc: 10-4-2021**	_____ ***Board Chairperson Signature*** _____ ***Chief Executive Officer Signature***
Note: Unless this document has an original signature, this copy is uncontrolled and valid on this date only: 2/13/2025. For controlled copy, view Agency Manuals - Medworxx on the BABHA Intranet site.			

DO NOT WRITE IN SHADED AREA ABOVE

Policy

It is the policy of Bay-Arenac Behavioral Health Authority (BABHA) to adhere to the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) as modified via the 2013 Omnibus Final Rule and issue breach notifications as required by the federal law and any applicable state law(s).

Purpose

This policy and procedure is established to provide clear guidelines to BABHA employees, contracted service providers, and business associates regarding compliance requirements and procedures for breach notifications.

Education Applies to:

☒ All BABHA Staff
☐ Selected BABHA Staff, as follows:
☒ All Contracted Providers: ☐ Policy Only ☒ Policy and Procedure
☐ Selected Contracted Providers, as follows:
☐ Policy Only ☐ Policy and Procedure
☐ Other: BABHA Business Associates and their Subcontractors
☐ Policy Only ☐ Policy and Procedure

Definitions

Breach: Acquisition, use or disclosure of protected health information (PHI) in a manner not permitted under the HIPAA Privacy Rule that compromises the security or privacy of PHI.

Business Associate: A person (other than a BABHA staff), or entity who creates, receives, maintains, or transmits PHI on behalf of BABHA or who provides services to or for BABHA involving the disclosure of PHI. See BABHA Policy and Procedure, C13-S01-T18 – Business Associates for more information.

Discovery Date: The first date on which a BABHA staff, contract service provider or business associate of BABHA becomes aware, or with the exercise of reasonable diligence would have become aware, that a potential Breach occurred.

Limited Data Set: PHI data that does not contain any direct identifiers, dates of birth, and/or zip codes.

Protected Health Information (PHI): Individually identifiable health information transmitted by

or maintained in an electronic media format (EPHI), or transmitted or maintained in any other form or medium, including paper.

Risk Assessment: A determination of the probability an impermissible acquisition, access, use, or disclosure compromised the PHI, based on at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.
- The unauthorized person who used the PHI or to whom the disclosure was made.
- Whether the PHI was actually acquired or viewed.
- The extent to which the risk to the PHI has been mitigated.

Secured PHI: PHI that is encrypted or has been destroyed in such a way that the PHI is unusable, unreadable, or indecipherable.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system used or maintained by BABHA.

Unsecured PHI: PHI not secured through the use of technology or a methodology that renders the information unusable, unreadable, or indecipherable to unauthorized individuals.

Procedure

1. Duty to Report a Breach

   a. Business associates are required (at 45 CFR 164.410) to notify BABHA no later than 60 days, and the BABHA Business Associate Agreement calls for notification within five (5) calendar days of discovery any breach of unsecured PHI that is accessed, maintained, retained, modified, recorded, stored, or otherwise held by them on behalf of BABHA. (see C13-S01-T18 Business Associates for more information).

   b. BABHA staff are required to notify BABHA's Privacy Officer, or if not available, the Security Officer, as well as their supervisor, of any privacy or security violation, including potential breaches, within two (2) business days of discovery of the incident.

   c. BABHA contracted service providers are required to notify BABHA's Privacy Officer, or if not available, the Security Officer, of any privacy or security violation, including potential breaches, within five (5) business days of discovery of the incident.

   d. As soon as feasible after discovery, BABHA will take reasonable action to cure the

breach and/or prevent further violation. If a breach is discovered by a business associate, it is the responsibility of the BA to take such action.

2. Breach Notification Requirements

   a. The Privacy Officer, or if so designated, the Security Officer, determines whether an impermissible use or disclosure of PHI constituted a breach. Determining whether breach notification is required under federal law involves a four-step process as listed below (see Attachment 1 – Breach Determination Decision Tree).

      i. Step 1: Determine whether the use or disclosure of the PHI violated the HIPAA Privacy Rule. If it did not violate the Privacy Rule, then no breach notification is required. If the use or disclosure did violate the Privacy Rule, continue to Step 2.

      ii. Step 2: Determine whether the PHI was unsecured or "limited." If the PHI was secured by a method or technology such as encryption or destruction, then no breach notification is required. If the PHI was unsecured, but was limited to a Limited Data Set, then no breach notification is required. If the PHI was unsecured and contained any direct identifiers, such as, names, dates of birth, city, zip codes, social security numbers, etc. then continue to Step 3. (See BABHA Policy and Procedure, C13-S01-T15 – De-identification of PHI for a list of direct identifiers).

      iii. Step 3: Determine whether one of the breach notification exclusions applies:

         1) The unintentional acquisition, access, or use of PHI by a BABHA staff, contracted service provider, or Business Associate, performing his/her duties, if made in good faith and within the scope of authority, and such situation does not result in a further impermissible use or disclosure.

         2) The inadvertent disclosure of PHI by a person authorized to access the PHI at BABHA, a contracted service provider's, or a Business Associate's location, to another person authorized to access the PHI at BABHA, the contracted service provider, or the same Business Associate, or an organized health care arrangement in which BABHA participates, and such situation does not result in a further impermissible use or disclosure.

         3) PHI was disclosed to a person who, in the good faith judgment of BABHA, contracted service provider, or a Business Associate, reasonably would not have been able to retain the information. If one of the above exceptions applies, then no breach notification is required. If none of these exceptions apply, continue to

Step 4.

iv. Step 4: Conduct a risk assessment following the criteria defined by the Federal government to determine whether the violation compromised the security or privacy of the PHI and whether there is a low probability or high probability that the PHI has been compromised. In determining low or high probability, BABHA should take into consideration the following (see attachment - Corporate Compliance Privacy-Security Record):

1) Who impermissibly used the PHI or to whom the PHI was impermissibly disclosed.
2) What immediate steps were taken to mitigate the impermissible use or disclosure.
3) Whether the PHI was returned before it was accessed for an improper use.
4) The type and amount of PHI.
5) The sensitivity of the information contained in the PHI.

b. In addition to the risk assessment, if a data breach was involved, a Security Incident Worksheet will also be completed by the BABHA Security Officer to evaluate relevant security concerns. (see Attachment – Security Incident Worksheet)

c. If based on the risk assessment, it is determined that the violation demonstrates a:

i. Low probability that the PHI has been compromised, then no breach notification is required.

ii. High probability that the PHI has been compromised, then breach notification is required, and notification will be issued as set forth below (see Attachment – Flowchart for Breach Notification).

3. Breach Notification to Individuals and or Other Entities

a. The Privacy Officer, or if so designated, the Security Officer, will notify the BABHA Chief Executive Officer (CEO) and the Recipient Rights Office immediately upon determination that a breach has occurred.

b. The Privacy Officer will notify the Mid-State Health Network (MSHN) PIHP within five business days of breaches involving Medicaid beneficiaries, as required by MSHN policies and procedures. The PIHP will notify the MI Department of Health and Human

Services (MDHHS). BABHA will directly notify MDHHS of breaches involving non-Medicaid beneficiaries.

c. BABHA will complete the breach notifications for breaches discovered by BABHA as required by federal law and any applicable state law. For breaches discovered by a business associate, the BA will complete the notifications. The BA will communicate with BABHA regarding the notifications as required by the terms of the Business Associate Agreement.

d. The following HIPAA-mandated breach notices will be sent:

   i. Individual Notice: As required at 45 CFR 164.404, BABHA must notify each individual without unreasonable delay and in no case later than 60 calendar days following discovery of the breach. BABHA must also provide written notification by first-class mail at the last known address of the individual or, if the individual agrees to electronic notice, by email. If BABHA knows the individual is deceased and has the address of the next of kin, or personal representative, then written notification must be provided to the next of kin or personal representative. Additional mailings may be utilized as information becomes available.

   ii. Substitute Notice: If there is insufficient or out-of-date contact information for ten (10) or more individuals, BABHA must provide substitute notice in the form of either a conspicuous posting for 90 days on the home page of its Web site or conspicuous notice in major print or broadcast media in geographic areas where the affected individuals likely reside, and include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's information may be included in the breach. In cases in which BABHA has insufficient or out-of-date contact information for fewer than ten (10) individuals, BABHA may provide substitute notice by an alternative form of written notice, telephone, or other means.

   iii. Additional Notice: If BABHA determines that the breach requires urgency because of the possible imminent misuse of unsecured PHI, BABHA may, in addition to the written notice, provide notice to individuals by telephone, or other means, as appropriate.

   iv. Media Notice: If the breach involves more than 500 individuals, BABHA will provide notice in prominent media outlets in the State or jurisdiction where those

individuals reside without unreasonable delay and in no case later than 60 days following the discovery of a breach, as well as include the same information as that required for the individual notice.

v. Pre-Paid Inpatient Health Plan Notice: BABHA must notify the payor Mid-State Health Network without unreasonable delay and in no case later than 10 business days following discovery of the breach.

vi. HHS Notice:

1) If the breach affects fewer than 500 individuals, BABHA must notify HHS with an annual notice to be submitted within 60 days of the end of the calendar year in which the breach was discovered. Notices must be submitted electronically, and a separate form must be completed for every breach that was discovered within the calendar year.

2) If the breach affects 500 or more individuals, BABHA must provide notice of the breach to HHS without unreasonable delay and in no case later than 60 days from discovery of the breach, unless BABHA grants an exception based on a law enforcement request as defined below. Notifications must be submitted electronically as required by HHS and if it is unclear exactly how many individuals are affected, an estimated number of individuals should be provided.

3) If additional information is discovered and needs to be reported after a notification has been submitted to HHS, BABHA may submit an additional form and note that it is an updated submission.

4. Delay of Notification for Law Enforcement Purposes

a. BABHA may delay a required notification if a law enforcement official determines that such notice or notification would impede a criminal investigation or cause damage to national security.

i. BABHA will document all requests by law enforcement agencies whether made orally or in writing, including the agency name, the official's name, and the date of the request.

ii. If the request is in writing and specifies the time for which a delay is required, BABHA will delay the notification for the time period specified.

iii. If the request is made orally, the statement will be documented including the

identity of the official making the statement, and BABHA will delay the notification no longer than thirty (30) days from the date of the oral statement, unless a written statement as described in ii. above is submitted during the thirty (30) day period.

5. Content of Notice

   a. BABHA will, to the extent possible, include the following information in the notice in plain language:

      i. Description of the incident(s).
      ii. Date(s) of the breach.
      iii. Date the breach was discovered.
      iv. Description of the types of unsecured PHI involved (e.g., name, social security number, etc.).
      v. Steps the individual should take to protect himself/herself against potential harm.
      vi. Description of the investigation, mitigation efforts, and prevention of future breaches.
      vii. Toll-free contact information for BABHA.

6. Mitigation/Remediation

   a. BABHA will mitigate, to the extent practicable, any harmful effects that are known and that result from a use or disclosure of PHI in violation of its privacy policies and procedures or the Privacy Rule, including violations by its business associates and contracted providers.

   b. Appropriate steps to mitigate/remediate harm will vary based on a totality of the circumstances, however, the Privacy Officer, or designee, in consultation with the Security Officer (as warranted), the CEO, and the Corporate Compliance Officer (CCO), will determine the appropriate actions which may include, but are not limited to, the following:

      i. Contacting the network administrator, as well as other potentially affected entities, to try to retrieve or otherwise limit the further distribution of improperly disclosed information.

      ii. Identifying the cause of the violation and amending policies and procedures to ensure it does not recur.

      iii. Providing free credit monitoring to individuals who are possibly at risk for identity

theft as a result of the violation.

iv. Training or retraining BABHA staff who handle PHI.

v. Imposing sanctions on BABHA staff primarily in response to serious employee errors such as, violating policies and procedures, unauthorized access, etc.

vi. Performing a new risk assessment.

vii. Revising business associate contracts to more require additional protection for confidential information

7. Monitoring

a. PHI is maintained in the BABH electronic health record, Phoenix. Legacy PHI is maintained in a record imaging system, Gallery. Both record systems are monitored for security breaches quarterly.

b. Individuals are granted access to the records for persons served based upon BABHA functional permissions. Users accessing records to which they are not assigned must activate a 'break the glass' feature in each system and enter a reason for doing so.

c. *The Medical Records Associate reviews the user access exception log in the Gallery Clinical Forms Reports and the Unauthorized Consumer Access Report in Phoenix,* under the direction of the Privacy Officer.

d. The Security Officer is responsible for monitoring breaches of the Information Systems (see BABHA Policy and Procedure, C09-S03-T04 – Security Management Process – Information Systems Activity Review).

e. Any findings from monitoring functions will be reviewed with the Corporate Compliance Officer who in turn will work with the supervisor of the program and/or the employee. If necessary, the Compliance Officer will forward findings to the CEO and the Human Resources Director for further action and take further investigative steps as outlined in C13-S02-T22 Complaint Investigations.

8. Training

a. All BABHA employees receive training on breach notification requirements at new employee orientation and during annual Staff Development Days training.

b. BABHA business associates and contracted providers are responsible for training their

own employees and subcontractors on breach notification requirements.

c. BABHA will inform its business associates and contracted providers of its policies and procedures with which they must comply through the BABHA Provider website and communications from the BABHA Contract Manager.

9. Documentation

a. The Privacy Officer will maintain all documentation related to breach reports, determinations, notifications, and resolutions for six years from the date of creation or the date when it last was in effect, whichever is later.

Attachments

- Breach Notification Decision Tree
- Flowchart for Breach Notification
- Corporate Compliance Privacy/Breach Record
- Security Incident Worksheet

Related Forms

N/A

Related Materials

- C09-S03-T04 – Security Management Process – Information Systems Activity Review
- C13-S01-T15 – De-Identification of PHI
- C13-S01-T18 – Business Associates

References/Legal Authority

- 45 CFR 164.400-164.414 Notification in the Case of Breach of Unsecured PHI
- 45 CFR 164.500-164.534 Privacy of Individual Identifiable Health Information
- HITECH Act of 2009
- OMNIBUS Rule of 2013

SUBMISSION FORM				
AUTHOR/ REVIEWER	APPROVING BODY/ COMMITTEE/ SUPERVISOR	APPROVAL/ REVIEW DATE	ACTION (Deletion, New, No Changes, Replacement or Revision)	REASON FOR ACTION If replacement, list policy to be replaced
M. Wolber	J. Pinter CCO	12/13/13	NEW	New policy to reflect compliance with HITECH breach notification procedures.

BAY-ARENAC BEHAVIORAL HEALTH AUTHORITY
POLICIES AND PROCEDURES MANUAL

Chapter: 13	**Corporate Compliance**		
Section: 1	**HIPAA**		
Topic: 13	**Breach Notification**		
Page: 10 of 10	**Supersedes Date:** **Pol:** **Proc: 10-23-15, 2-20-14**	**Approval Date:** **Pol: 2-20-14** **Proc: 10-4-2021**	_____ ***Board Chairperson Signature*** _____ ***Chief Executive Officer Signature***
Note: Unless this document has an original signature, this copy is uncontrolled and valid on this date only: 2/13/2025. For controlled copy, view Agency Manuals - Medworxx on the BABHA Intranet site.			

DO NOT WRITE IN SHADED AREA ABOVE

B. Kish	J. Pinter CCO	07/24/15	Revision	Revisions reflect changes in EHR consumer record monitoring and includes notification of PIHP in case of breach
B. Kish	J. Pinter CCO	10/23/15	Revision	Revisions reflect transition to Security Officer taking primary role in HITECH breach notification procedures
J. Pinter	Corporate Compliance Committee	10/4/2021	Revision	Triennial review. Update language to reflect guidance from legal counsel; update to match current practices
K. Amon	Corporate Compliance Committee	1/30/25	No Changes	Triennial Review.