BAY-ARENAC BEHAVIORAL HEALTH AUTHORITY
POLICIES AND PROCEDURES MANUAL

Chapter: 9	**Information Management**		
Section: 3	**Administrative Safeguards**		
Topic: 1	**Security Management Process – Risk Analysis, Management and Evaluation**		
Page: 1 of 7	**Supersedes Date:** **Pol: 4-21-05** **Proc: 4-21-05**	**Approval Date:** **Pol: 3-20-14** **Proc: 1-21-14**	_____ ***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: 9/6/2024. 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 (BABHA) to conduct periodic risk analyses in order to protect BABHA's information technology systems from potential risks and vulnerabilities and to identify, assess, manage and evaluate such security risks.

Purpose

This policy and procedure is established to proactively identify potential risks to BABHA in regards to how it operationalizes information system technologies, and/or to determine potential risks for the varying types of technology that are utilized for day-to-day operations. Targeted evaluations of BABHA's security program will be used to make recommendations for improvement and close gaps in the program as needed.

Education Applies to:

☐ All BABHA Staff
☒ Selected BABHA Staff, as follows: Information Systems, Management, Privacy and Security Officers
☐ All Contracted Providers: ☐ Policy Only ☐ Policy and Procedure
☒ Selected Contracted Providers, as follows: IS Operations Support Contract Providers
☐ Policy Only ☒ Policy and Procedure
☐ Other:

Definitions

Availability: Refers to the data or information that is accessible and useable upon demand by an authorized person.

Electronic Equipment: Electronic devices, such as desktops, laptops, tablets, smartphones, facsimile machines, copiers, and any other electronic device, that can potentially store PHI data.

Electronic Media: (1) Electronic storage media includes memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; video tapes; audio tapes; and removable storage devices such as USB drives; or (2) transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Health Information: Any information, whether oral or recorded in any form, that is created or received by BABHA and relates to an individual's past, present, or future physical or mental health, or to the payment for such health care.

Individually Identifiable Health Information: Health information, including demographic information that identifies an individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Information System: For purposes of this policy and procedure, information system refers to an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, and applications.

Integrity: Refers to the property that data or information has not been altered or destroyed in an unauthorized manner.

Protected Health Information (PHI): Individually identifiable health information transmitted by or maintained in an electronic media format (e-PHI), or transmitted or maintained in any other form or medium, including oral and/or paper.

Chapter: 9	**Information Management**		
Section: 3	**Administrative Safeguards**		
Topic: 1	**Security Management Process – Risk Analysis, Management and Evaluation**		
Page: 3 of 7	**Supersedes Date:** **Pol: 4-21-05** **Proc: 4-21-05**	**Approval Date:** **Pol: 3-20-14** **Proc: 1-21-14**	_____ ***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: 9/6/2024. For controlled copy, view Agency Manuals - Medworxx on the BABHA Intranet site.			

DO NOT WRITE IN SHADED AREA ABOVE

Risk: The likelihood of a given threat exercising (exploiting) a particular vulnerability and the resulting impact of that event.

Threat: Something or someone that can intentionally or accidentally exploit a vulnerability.

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls which can be exploited by a threat and result in unauthorized use and/or disclosures of PHI.

Workforce Member: Employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, students, volunteers, and staff from third party entities who provide service to the covered entity.

Procedure

I. Risk Analysis

1. BABHA will regularly identify, define, and prioritize risks to the confidentiality, integrity, and availability of its information systems containing e-PHI and will do so based on a formal and documented risk analysis process.

2. BABHA's Security Officer, or designee, is responsible for setting up and conducting periodic assessments of potential risks and vulnerabilities to the information systems and executing a risk analysis under the direction of the Corporate Compliance Officer (CCO).

3. The risk analysis process will include an analysis of the e-PHI flow throughout the information systems including external sources of e-PHI, such as vendors and consultants handling e-PHI for BABHA, as well as the e-PHI created, received, maintained, or transmitted by BABHA itself.

4. New electronic equipment, and/or forms of technology, that handle e-PHI will be assessed to identify potential risks and vulnerabilities.

5. The Security Officer, or designee, will share the results of the risk assessments and analyses with the CCO. BABHA will use the information to guide its decisions related to the protection of e-PHI.

II. Risk Management

1. BABHA's Security Officer, or designee, is responsible for implementing risk management processes under the direction of the CCO.

2. BABHA will reduce risks and vulnerabilities to a reasonable level by the application of the following interventions:
   a. All workforce member technology network accounts must be established on the BABHA technology network domain and will be added and terminated only by Information Systems (IS) staff authorized for this function at the direction of BABHA management.
   b. Computing environments and user workstations will be managed securely such that all access to applications and information systems will be centrally controlled.
   c. IS staff will be responsible for ensuring intrusion monitoring of BABHA's technology network.
   d. IS staff will be responsible for applying reasonable safeguards to protect BABHA servers and its network from malicious code and unauthorized access.
   e. IS staff will apply industry standard back-up and restore/recovery procedures in its operations.
   f. BABHA servers and technology network components will be contained in a secure and monitored facility utilizing reasonable access control procedures.

III. Evaluation

1. BABHA's Security Officer, or designee, will conduct a periodic evaluation of the processes and systems within BABHA, including review of the technical controls,

amendments to regulations and standards, and procedural review of the security program.

2. Evaluations will be done at a minimum, annually, or after one of the following conditions occurs:
   i. A security incident
   ii. When new technologies and/or systems are deployed
   iii. When environmental or operational changes occur which have the potential to significantly impact information systems containing E-PHI.

3. The Security Officer will review and analyze the evaluations for gaps in the security program and make recommendations for remediation. This information will be shared with the BABHA Corporate Compliance Officer, or designee.

IV. Additional Information

1. The CCO, or designee, will have direct oversight over all risk analysis, risk management and evaluation processes.

2. Risk analysis, risk management and evaluation processes will be modeled upon an objective, industry standard method similar to those recommended by the National Institute for Standards and Technology (NIST).

3. The Security Officer, or designee, will fully document all activities and efforts related to risk assessments, risk analyses, risk management and evaluations of BABHA's security program and maintain such documentation for six years from the date of creation or the date when it last was in effect, whichever is later.

Attachments

N/A

Chapter: 9	**Information Management**		
Section: 3	**Administrative Safeguards**		
Topic: 1	**Security Management Process – Risk Analysis, Management and Evaluation**		
Page: 6 of 7	**Supersedes Date:** **Pol: 4-21-05** **Proc: 4-21-05**	**Approval Date:** **Pol: 3-20-14** **Proc: 1-21-14**	_____ ***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: 9/6/2024. For controlled copy, view Agency Manuals - Medworxx on the BABHA Intranet site.			

DO NOT WRITE IN SHADED AREA ABOVE

Related Forms

N/A

Related Materials

NIST SP 800-30 (http://csrc.nist.gov/publications) - This is related material only. It cannot be inferred that all or any items detailed in NIST document are included in this policy. It is for reference purposes only.

References/Legal Authority

Administrative Safeguards - HIPAA Section 164.308(a)(1), (a)(8)

BAY-ARENAC BEHAVIORAL HEALTH AUTHORITY
POLICIES AND PROCEDURES MANUAL

Chapter: 9	**Information Management**		
Section: 3	**Administrative Safeguards**		
Topic: 1	**Security Management Process – Risk Analysis, Management and Evaluation**		
Page: 7 of 7	**Supersedes Date:** **Pol: 4-21-05** **Proc: 4-21-05**	**Approval Date:** **Pol: 3-20-14** **Proc: 1-21-14**	_____ ***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: 9/6/2024. For controlled copy, view Agency Manuals - Medworxx on the BABHA Intranet site.			

DO NOT WRITE IN SHADED AREA ABOVE

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/T. Piorkowski	Janis Pinter, CCO	01/21/14	Replacement & Revision	Revised to reflect HIPAA compliance and updated to current practices. Replaces C09-S03-T02 which is being deleted.
B. Kish	Janis Pinter, CCO	2/10/17	No Changes	Triennial Review
B. Kish	Janis Pinter, CCO	2/12/20	No Changes	Triennial Review
J. Bellinger	Karen Amon, CCO	03/10/2023	No Changes	Triennial Review