BAY-ARENAC BEHAVIORAL HEALTH AUTHORITY
POLICIES AND PROCEDURES MANUAL

Chapter: 9	**Information Management**		
Section: 5	**Technology Safeguards**		
Topic: 1	**Access Controls – Unique User Identification and Logoff**		
Page: 1 of 6	**Supersedes Date:** **Pol: 4-21-05** **Proc: 2-10-17,6-27-13, 4-21-05**	**Approval Date:** **Pol: 8-15-13** **Proc: 9-13-19**	_____ ***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: 9/30/2019. 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 safeguard information systems by implementing controls that identify and track the access and usage of information systems by workforce members.

Purpose

This policy and procedure is established to identify and implement the safeguards that store confidential data, documents, or protected health information (PHI), from unauthorized access or usage.

Education Applies to:

☒ All BABHA Staff
☐ Selected BABHA Staff, as follows:
☒ All Contracted Providers: ☐ Policy Only ☒ Policy and Procedure
☒ Selected Contracted Providers, as follows: Primary Information Technology Vendor
☐ Policy Only ☒ Policy and Procedure
☐ BABHA's Affiliates: ☐ Policy Only ☐ Policy and Procedure
☐ Other:

Definitions

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.

Generic or Group Identifier: A user identification (ID) that is typically shared by more than one user and does not uniquely identify an individual, non-standard in its naming convention (making tracing the individual in the system impossible), and used often by temporary staff.

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, an 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.

Mobile Devices: A generic term used to refer to a variety of hand-held or plug-in devices that allow people to access and/or download data and information just as if they were using a conventional computer. This includes such devices as cell phones, smart phones, tablets, USB drives, flash drives, etc.

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 oral and/or paper.

Chapter: 9	**Information Management**		
Section: 5	**Technology Safeguards**		
Topic: 1	**Access Controls – Unique User Identification and Logoff**		
Page: 3 of 6	**Supersedes Date:** **Pol: 4-21-05** **Proc: 2-10-17,6-27-13, 4-21-05**	**Approval Date:** **Pol: 8-15-13** **Proc: 9-13-19**	_____ ***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: 9/30/2019. For controlled copy, view Agency Manuals - Medworxx on the BABHA Intranet site.			

DO NOT WRITE IN SHADED AREA ABOVE

Virtual Desktop: A common name given to software applications that are deployed on BABHA's information system. These applications utilize VMware® Virtual Machine Services for deploying desktop.

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. Access Controls – User Identification

1. Access to BABHA's information systems requires approval of a workforce member's immediate supervisor. For auditors, consultants, and vendors, access requires approval of the relevant director. Relevant supervisors and directors need to send an email to the Information Systems Help Desk to have the access request processed.

2. Once the email request is processed, BABHA's Help Desk will create a unique user identification name for workforce members following a standard naming practice and will grant them access via unique IDs that:
   a. Individually identify workforce members, and
   b. Allows activities performed on information systems to be traced back to them through the tracking of their unique IDs, provided the technical capabilities of the information system allows such tracing.

3. Workforce members are not to share their user ID to prevent unauthorized access to information systems and to prevent being held liable for someone else's actions.

Chapter: 9	**Information Management**		
Section: 5	**Technology Safeguards**		
Topic: 1	**Access Controls – Unique User Identification and Logoff**		
Page: 4 of 6	**Supersedes Date:** **Pol: 4-21-05** **Proc: 2-10-17,6-27-13, 4-21-05**	**Approval Date:** **Pol: 8-15-13** **Proc: 9-13-19**	_____ ***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: 9/30/2019. For controlled copy, view Agency Manuals - Medworxx on the BABHA Intranet site.			

DO NOT WRITE IN SHADED AREA ABOVE

4. Generic or group user identifiers must not be used to gain access to BABHA information systems or sensitive media that contains PHI. The only exception for using generic or group user IDs is to gain access to those systems, files or databases not containing PHI or in individual access situations that are determined impractical, as determined by the BABHA Security Officer and approved by the BABHA Corporate Compliance Officer. Such exceptions are expected to occur rarely or not at all; and if made, must be time limited and risk mitigated through the application of comprehensive auditing/monitoring controls, including checks for security breach

5. Nothing in this policy shall limit the use of additional security measures, including login and access measures, which may further enhance the security and protection provided for PHI.

6. BABHA will ensure that audit activity on a per-user ID basis will occur regularly.

7. The BABHA Security Officer, or designee, is responsible for managing and tracking the user IDs of new, existing, and terminated workforce members (see BABHA Policy and Procedure, C09-S03-T07 – Workforce Security – Access Clearance and Termination).

II. <u>Access Controls – User Logoff</u>

1. BABHA's Information Systems Department will provide for automated screen lock (thin client and personal computer [PC]) devices through the following action:
    - After fifteen (15) minutes of a Virtual Desktop session being left idle, the password protected screen lock will turn on (local device automated screen lock activation time is set by the workforce member).

2. Personal computers and laptops that access, transmit, receive, or store PHI and are located in open, common, or otherwise insecure areas must employ the use of inactivity timers or automatic logoff mechanisms. Workforce members must activate their screen lock option and also turn on the password protection option.

3. All other types of mobile devices, including but not limited to cell phones, smart phones, tablets, etc., which have PHI stored directly on them, or have the potential to store PHI, must also employ the use of inactivity timers or automatic logoff mechanisms. Inactivity timers on those devices must be set according to the functions available within those devices.

4. All sessions and devices which require the use of inactivity timers or automatic logoff mechanisms must terminate at a maximum of fifteen (15) minutes of inactivity. Inactivity intervals may be set to a lower amount at the user's discretion.

5. If a system requires the use of an inactivity timer or automatic logoff mechanism, as detailed in the above procedures, but does not support an inactivity timer or automatic logoff mechanism, one of the following procedures must be implemented:
    - The system must be upgraded or moved to support the minimum automatic logoff procedures.
    - The system must be moved into a secure environment.
    - All PHI must be removed and relocated to a system which supports the minimum automatic logoff procedures.

6. Workforce members are required to log-off of servers, workstations, applications, database systems, or other computer systems when they are leaving their offices for the day, are on ETO, or are on any other type of leave from employment.

Attachments

N/A

Related Forms

N/A

BAY-ARENAC BEHAVIORAL HEALTH AUTHORITY
POLICIES AND PROCEDURES MANUAL

Chapter: 9	**Information Management**		
Section: 5	**Technology Safeguards**		
Topic: 1	**Access Controls – Unique User Identification and Logoff**		
Page: 6 of 6	**Supersedes Date:** **Pol: 4-21-05** **Proc: 2-10-17,6-27-13, 4-21-05**	**Approval Date:** **Pol: 8-15-13** **Proc: 9-13-19**	_____ ***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: 9/30/2019. For controlled copy, view Agency Manuals - Medworxx on the BABHA Intranet site.			

DO NOT WRITE IN SHADED AREA ABOVE

Related Materials

N/A

References/Legal Authority

Technology Safeguards - HIPAA Section 164.312(a)(1)

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	CCP/SLT	06/27/13	Revision	Revised to reflect HIPAA compliance and updated to current practices.
B. Kish	J. Pinter, CCO	02/10/17	Revision	Triennial Review-Revised to reflect change to 15 minutes of inactivity before screen lock. Also changed language to reflect VDI not Secure Desktop
B. Kish	J. Pinter, CCO	9/13/19	Revision	Small revision to include unique ID when accessing electronic media