BAY-ARENAC BEHAVIORAL HEALTH AUTHORITY
POLICIES AND PROCEDURES MANUAL

Chapter: 9	**Information Management**		
Section: 3	**Administrative Safeguards**		
Topic: 15	**Security Awareness – Password Management**		
Page: 1 of 4	**Supersedes Date:** **Pol: 4-21-05** **Proc: 6-27-13, 4-21-05**	**Approval Date:** **Pol: 8-15-13** **Proc: 2/10/17**	***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: 5/31/2017. 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 have processes in place that establish, maintain, and monitor information systems passwords to ensure information systems security.

Purpose

This policy and procedure is established to govern password management, including creating, changing, and safeguarding passwords for BABHA.

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
☐ BABHA's Affiliates: ☐ Policy Only ☐ Policy and Procedure
☐ Other:

Definitions

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.

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.

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.

Workstation: An electronic computing device. For example, laptops or desktop computers, dumb terminals, thin clients, Personal Digital Assistants (PDAs), wireless devices, or any other device that performs similar functions and has electronic media stored in its immediate environment. This includes any personal electronic computing devices when they are used to access any BABHA information system for work-related purposes.

Procedure

1. Supervisors and/or directors will request system access for workforce members by submitting an email to the BABHA Information Systems Help Desk. The Help Desk will follow up on the request using their ticketing system. (See BABHA Policy and Procedure, C09-S03-T07 - Workforce Security – Access Clearance and Termination).

2. The Help Desk is responsible for creating the workforce member's initial password and confidentially communicating that password back to him/her. Upon receiving the new password, workforce members must immediately change the password to their own unique one.

3. Workforce members should keep their password confidential at all times. Under no circumstances should passwords ever be shared or written down and kept at or near computers and workstations where they may be found by others. (See BABHA Policy and Procedure, C09-S05-T01 – Access Controls-Unique User Identification and Logoff).

4. Workforce members must log onto any system only with their own password.

5. Workforce members must change their VDI and EHR passwords every 90 days when the system automatically prompts them to do so, however, they are free to change it before then if they desire.

    a. To change the VDI password before being automatically prompted, workforce members should click on the "Control-Alt-Delete" buttons simultaneously. The system will then allow a password change. If the password is not changed at the 90 day automatic prompt, the system will deny access.
    b. To change the EHR password before being automatically prompted, workforce members should click on the "Change Password" option at the bottom of the main EHR navigation bar.

6. Workforce members who lose, misplace, forget or experience any compromise to their password must immediately notify the Help Desk and change their password.

Attachments

N/A

Related Forms

N/A

Related Materials

BABHA Policies and Procedures:
1. C09-S03-T07 – Workforce Security-Access Clearance and Termination
2. C09-S05-T01 – Access Controls-Unique User Identification

References/Legal Authority

Administrative Safeguards - HIPAA Section 164.308(a)(5)

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-Updated language to change password manually for the VDI and EHR