BAY/ARENAC BEHAVIORAL HEALTH AUTHORITY
POLICIES AND PROCEDURES MANUAL

Chapter: 9	**Information Management**		
Section: 5	**Technology Safeguards**		
Topic: 5	**Transmission Security – Encryption and Decryption**		
Page: 1 of 7	**Supersedes Date:** **Pol: 4-21-05** **Proc: 6-4-15, 4-21-05**	**Approval Date:** **Pol: 4-21-05** **Proc: 2-21-2020**	_____ ***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: 10/23/2020. 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 appropriately use encryption to protect the confidentiality, integrity, and availability of data and protected health information (PHI) transmitted over the electronic computer network and communication systems.

Purpose

This policy and procedure is established to provide guidance on the use of encryption when data and/or PHI are transmitted outside of the BABHA computer network and communication systems thereby ensuring that sensitive information and/or PHI are not accessed by unauthorized persons and/or programs.

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 Business Associates: ☐ Policy Only ☒ Policy and Procedure
☐ Other:

Definitions

Encryption: A mechanism that converts an original message or text into a format that is unreadable but eventually becomes readable through the use of a deciphering key in the hands of the intended receiver of the message or text.

Chapter: 9	**Information Management**		
Section: 5	**Technology Safeguards**		
Topic: 5	**Transmission Security – Encryption and Decryption**		
Page: 2 of 7	**Supersedes Date:** **Pol: 4-21-05** **Proc: 6-4-15, 4-21-05**	**Approval Date:** **Pol: 4-21-05** **Proc: 2-21-2020**	_____ ***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: 10/23/2020. For controlled copy, view Agency Manuals - Medworxx on the BABHA Intranet site.			

DO NOT WRITE IN SHADED AREA ABOVE

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.

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.

Procedure

I. Workforce Member Responsibilities

1. Workforce members who send PHI in email messages **must** encrypt the email messages (see Attachment 1 – How to Send an Encrypted Email Message.pdf). This includes email sent to BABH staff email accounts (babha.org). Applying encryption to all emails messages containing PHI prevents the accidental or inadvertent transmission of PHI to external recipients by the sender or subsequent recipient of the encrypted email.

2. Use of the secure messaging feature within the electronic health record (EHR) is the preferred method of communicating PHI electronically. The use of encryption can be avoided, because primary providers have direct access to the secure messaging system within the EHR.

3. Workforce members should contact the Help Desk for assistance for email handling recommendations or for emailing an encrypted attachment (see Attachment – How to Send an Encrypted Email Message).

4. PHI faxed through BABHA email fax accounts is considered secure and does not need encryption.

5. Workforce members who receive encrypted PHI in email messages should follow the sender's instructions for decrypting the messages.

6. If workforce members have any concerns regarding sending confidential information or PHI either within or outside of the BABHA computer network, and/or storing such information, they should contact the BABHA Corporate Compliance Officer, Security Officer, or Privacy Officer for assistance.

7. Workforce members using their own equipment cannot download confidential information or PHI data onto their own equipment unless an exception is made by the Security Officer.

8. Workforce members should never attempt to subvert or hack the BABHA network system and will be subject to disciplinary action if they do so.

II. <u>Mobile Devices</u>

Agency mobile devices and personal mobile devices, along with other portable devices, are a specific category of devices that present a particularly high risk for incidents involving unauthorized exposure of confidential data and/or PHI, most often as a result of being stolen or lost.

1. BABHA's Policy and Procedure, C09-S05-T08 – Mobile Device Use and Security, identifies the acceptable use of mobile devices used to conduct agency business.

III. Other Portable Devices

1. BABHA agency staff are not allowed to use portable or remote memory devices that can store PHI unless an exception is made by the Security Officer. If an exception is made, any portable device used must have the ability to encrypt the PHI and the encryption capability on the device must be activated. (See BABHA Policy and Procedure, C09-S04-T07 – Electronic Devices and Media Controls).

2. Portable devices must have the proper protection mechanisms installed, including approved anti-malware software and firewall, with unneeded services and ports turned off and properly configured needed applications.

3. Portable devices should not be used for the long-term storage of any confidential information or PHI.

4. Hard drives of portable devices must be encrypted using products and/or methods approved by IS. Unless otherwise approved by IS and BABHA management, such devices shall have full disk encryption with pre-boot authentication.

5. Removable media including CD's, DVD's, USB flash drives, etc. that contain confidential information or PHI must be encrypted and stored in a secure locked location and transported in a secure manner.

6. Portable or removable media that contain confidential data must be in the possession of the authorized user at all times (e.g., must not be checked as luggage while in transit).

IV. Information Systems (IS) Responsibilities

1. IS is responsible for recommending, testing, implementing, and training key workforce members in automated encryption protocols and services.

2. Healthcare software operating within the BABHA internal network that contains PHI, and which users are required to authenticate, must operate in the virtual desktop infrastructure environment.

3. Externally hosted systems containing PHI, such as electronic health record, must employ Hypertext Transfer Protocol Secure (HTTPS) to achieve adequate encryption for all client connections.

4. Transfer files containing PHI must use Secure File Transfer Protocol (SFTP) or File Transfer Protocol (FTP) using Secure Shell (SSH) or Secure Copy (SCP).

V. Data-at-Rest

1. PHI or confidential data-at-rest on computer systems owned by and located within BABHA controlled spaces and networks should be protected by one or more of the following:
   a) Firewalls with strict access controls that authenticate the identity of individuals accessing the data (see Policies and Procedures C09-S03-T13 Security Awareness-Protection from Malicious Software and C09-S03-T14 Security Awareness-Log-in Monitoring);
   b) Other compensating controls, including complex passwords, physical isolation/access, etc (see Policies and Procedures C09-S03-T15 Security Awareness – Password Management and C09-S04-T02 Facility and Physical Access Security).

2. Password protection should be used in combination with all controls, including encryption, since password protection alone is not an acceptable alternative to protecting confidential information or PHI.

3. BABHA secures its stored data on file systems, disks, and tape drives in servers and a storage area network environment. Back up data must be protected using AES 256-bit algorithm encryption methodologies, whenever technologically feasible.

4. Policy and Procedure, C09-S04-T07 – Electronic Devices and Media Controls – Movement, Re-use, Data Back-up and Disposal, identifies how data storage devices will be sanitized, disposed of, or prepared for re-use.

Attachments

How to Send an Encrypted Email Message

Related Forms

N/A

Related Materials

BABHA Policy and Procedure, C04-S06-T04 Electronic Communication with Persons Served Data-In-Transit

References/Legal Authority

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

BAY/ARENAC BEHAVIORAL HEALTH AUTHORITY
POLICIES AND PROCEDURES MANUAL

Chapter: 9	**Information Management**		
Section: 5	**Technology Safeguards**		
Topic: 5	**Transmission Security – Encryption and Decryption**		
Page: 7 of 7	**Supersedes Date:** **Pol: 4-21-05** **Proc: 6-4-15, 4-21-05**	**Approval Date:** **Pol: 4-21-05** **Proc: 2-21-2020**	_____ ***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: 10/23/2020. 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**
J. Pinter M. Bartlett M. Wolber	J. Pinter	04/21/05	Revision & Replacement	Revised to reflect HIPAA compliance and updated to current practices. Revised to add restrictions to agency-issued and personal cellphones for security purposes related to PHI access. This also replaces P/P C09-S05-T04
B. Kish	J. Pinter	06/04/15	Revision	Revised to reflect new encryption method, and remove redundant language that existed on other P/P's.
B. Kish	J. Pinter, CCO	02/10/17	Revision	Corrections were missed related to the new email encryption method used
B. Kish	J. Pinter, CCO	02/21/20	Revision	Triennial Review-added language regarding emailing PHI and apply encryption