Salish Behavioral Health
Administrative Services Organization

Policy Name: PROTECTED HEALTH INFORMATION E-MAIL AND INTERNET SECURITY POLICY

Policy Number: PS909

Effective Date: 1/1/2020

Revision Dates: 1/14/2021

Reviewed Date: 4/5/2023

Executive Board Approval Dates: 7/30/2021

PURPOSE

The Salish Behavioral Health Administrative Services Organization (SBH-ASO) uses this and other policies to set limits on the use of email, PCs, cell phones, and telecommunications by workforce member. The requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2 require that these policies be established, enforced, and audited.

POLICY

This policy provides specific instructions on the ways to secure electronic mail (e-mail) on computers (desktop, laptop, and/or mobile devices) and servers.

The policies apply to SBH-ASO workforce members, and covers e-mail located on SBH-ASO computers if these systems are under the jurisdiction and/or ownership of SBH-ASO.

PROCEDURE

1. SBH-ASO Property

   As a productivity enhancement tool, SBH-ASO encourages the business use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by SBH-ASO electronic communications systems, including back-up copies, are considered to be the property of SBH-ASO and are not the property of users of the electronic communications services.

2. User Separation

   These policies must be implemented where electronic communications systems provide the ability to separate the activities of different users. For example, electronic mail systems must employ user IDs and associated passwords to isolate the communications of different users. However, fax machines that do not have separate mailboxes for different recipients need not support such user separation. All SBH-ASO staff and authorized business associates have unique usernames and passwords to access the e-mail system.

3. User Accountability

   a. Individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions the other party takes with the password, and it exposes SBH-ASO to considerable risk.

   b. If users need to share computer resident data, they should utilize message-forwarding facilities, public directories on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic communications, users must choose passwords that are difficult to guess - not a dictionary word, not a personal detail, and not a reflection of work activities.

4. No Default Protection

   Employees are reminded that outgoing SBH-ASO electronic communications systems are not encrypted by default. If Protected Health Information (PHI) must be sent by electronic communications systems outside of the Kitsap County network, an electronic encryption that meets National Institute of Standards and Technology standards or similar technologies to protect the data must be employed.

5. Respecting Privacy Rights

   a. Except as otherwise specifically provided, employees and business associates may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. SBH-ASO is committed to respecting the rights of its employees and business associates, including their reasonable expectation of privacy. However, SBH-ASO also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

   b. It is the policy of the SBH-ASO that no e-mail message shall be sent or received that contain PHI unless it is sent with electronic encryption that meets National Institute of Standards and Technology standards, as specified in the HIPAA security rule, and sent to a verified email address. If at any time either an SBH-ASO workforce member use e-mail to transmit PHI as part of an unencrypted e-mail message, the SBH-ASO employee

shall notify the sending party that the e-mail has been sent in violation of our HIPAA Security Policy; delete the message from their mailbox empty their e-mail trash and notify the SBH-ASO Privacy Officer.

c. All electronic communications containing PHI shall be protected and secured as defined by this policy and may be accomplished by accessing the shared network drive through the system Virtual Private Network/Secure Socket Layer system.

6. No Guaranteed Message Privacy

   SBH-ASO cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

7. Regular Message Monitoring

   It is the policy of SBH-ASO **not** to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored to support operational, maintenance, auditing, security, and investigative activities. SBH-ASO retains the right to monitor messages to ensure compliance with HIPAA AND 42 CFR Part 2 regulations concerning security and client privacy. Users should structure their electronic communications in recognition of the fact that SBH-ASO will from time to time examine the content of electronic communications.

8. Message Forwarding

   Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. SBH-ASO sensitive information and PHI must not be forwarded to any party outside SBH-ASO without the prior approval of their manager.

<u>Responsibilities</u>

As defined below, Kitsap County and SBH-ASO staff responsible for electronic mail security has been designated in order to establish a clear line of authority and responsibility.

- Kitsap County Information Systems (IS) must establish e-mail security policies and standards and provide technical guidance on e-mail security to all SBH-ASO staff.
- The SBH-ASO Privacy Officer must review all such policies and procedures to ensure compliance with the applicable HIPAA and 42 CFR Part 2 regulations.

- Kitsap County IS staff must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Managers must ensure that their staff are in compliance with the personal computer security policy established in this document. Kitsap County IS staff must also provide administrative support and technical guidance to management on matters related to e-mail security.
- SBH-ASO managers must ensure that employees under their supervision implement e-mail security measures as defined in this document.

Contact point

Questions about this policy may be directed to the SBH-ASO Privacy Officer.

Enforcement

All managers are responsible for enforcing this procedure. The SBH-ASO Privacy Officer is notified of any violations. Employees who violate this procedure are subject to personnel action.