SALISH BHO

HIPAA, 42 CFR PART 2, AND MEDICAID COMPLIANCE STANDARDS POLICIES AND PROCEDURES

Policy Name: PROTECTED HEALTH INFORMATION DATA, E-MAIL, AND INTERNET SECURITY POLICY **Policy Number:** 5.12

Reference: 45 CFR Parts 160, 162 and 164; 42 CFR Part 2; Kitsap County Electronic Communication Policy

Effective Date: 5/2005

Revision Date(s): 10/2012; 5/2016; 5/2018

Reviewed Date: 5/2016; 5/2017; 5/2018

Approved by: SBHO Executive Board

CROSS REFERENCES

- Policy: Password Protection Procedure
- Policy: Corrective Action Plan

PURPOSE

Introduction

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. SBHO uses these and other policies to set limits on the use of email, PCs, cell phones, and telecommunications by employees.

This policy statement provides specific instructions on the ways to secure electronic mail (e-mail) on personal computers and servers.

Scope

The policies apply to SBHO employees and business associates, and covers e-mail located on SBHO computers if these systems are under the jurisdiction and/or ownership of SBHO. The policies apply to stand-alone personal computers with dial-up modems as well as those attached to networks.

PROCEDURE

1. Company Property

   As a productivity enhancement tool, SBHO encourages the business use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of SBHO 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. But, fax machines that do not have separate mailboxes for different recipients need not support such user separation. All SBHO staff and authorized business associates have unique usernames and passwords to access the e-mail system.

3. User Accountability

   a. Regardless of the circumstances, 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 SBHO 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. (Please reference the Password Protection procedure.)

4. No Default Protection

   Employees are reminded that outgoing SBHO electronic communications systems are not encrypted by default. If PHI must be sent by electronic communications systems outside of the 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 may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. SBHO is committed to respecting the rights of its employees, including their reasonable expectation of privacy. However, SBHO 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 SBHO that no e-mail message shall be sent or received that contain protected health information (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 a SBHO employee or contractor use e-mail to transmit PHI as part of an unencrypted e-mail message, the SBHO 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 SBHO 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

   SBHO 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 SBHO **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. SBHO 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 SBHO 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. SBHO sensitive information must not be forwarded to any party outside SBHO without the prior approval of their manager.

<u>Responsibilities</u>

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

- Information Systems must establish e-mail security policies and standards and provide technical guidance on e-mail security to all SBHO staff.
- The Privacy Officer must review all such policies and procedures to ensure compliance with the agency's overall Privacy and Security Plan and to ensure compliance with applicable HIPAA and 42 CFR Part 2 regulations.

- IS staff must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Managers must ensure that their staffs are in compliance with the personal computer security policy established in this document. IS staff must also provide administrative support and technical guidance to management on matters related to e-mail security.
- SBHO 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 Privacy Officer.

Enforcement

Violation of these policies may subject employees or business associates to disciplinary procedures in accordance with Kitsap County's personnel policies.

MONITORING

This policy is mandated by contract or statute.

1. This policy will be monitored through use of SBHO:
   - Annual SBHO Provider and Subcontractor Administrative Review

2. If a provider performs below expected standards during the review listed above, a Corrective Action will be required for SBHO approval. Reference SBHO Corrective Action Plan Policy.