



SALISH BHO

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

Policy Name: WORKSTATION AND PORTABLE
COMPUTER USE PROCEDURE

Policy Number: 5.11

Reference: 45 CFR Parts 160, 162 and 164; 42 CFR Part 2

Effective Date: 10/2005

Revision Date(s): 5/2016

Reviewed Date: 5/2016; 6/2017

Approved by: SBHO Executive Board

CROSS REFERENCES

- Policy: Confidentiality, Use and Disclosure of Protected Health Information
- Policy: Password Protection Procedure
- Policy: Corrective Action Plan

PURPOSE

All staff of Salish Behavioral Health Organization (SBHO) and provider network agencies who use computer terminals, laptop, notebook, or other portable computers must be familiar with the procedure. Demonstrated competence in the requirements of the procedure is an important part of every SBHO employee's responsibilities.

POLICY

SBHO staff must monitor the computer's operating environment and report potential threats to the computer and to the integrity and confidentiality of data contained in the computer system. SBHO staff will take appropriate measures to protect computers and data from loss or destruction.

PROCEDURE

Workstation Use

- Personnel using computers will not smoke, eat, or drink at the terminal to prevent damage due to spills and so forth.
- Personnel logging onto the system will ensure that no one observes the entry of their password.

- Personnel will neither log onto the system using another's password nor permit another to log on with their password. Nor will personnel enter data under another person's password. Please refer to the Password Protection Procedure.
- Each person using SBHO computers is responsible for the content of any data he or she inputs into the computer or transmits through or outside the SBHO system. No person may hide his or her identity as the author of the entry or represent that someone else entered the data or sent the message. All personnel will familiarize themselves with and comply with County e-mail policy.
- No employees may access any confidential or other information that they do not have a need to know. No employee may disclose confidential or other information unless properly authorized (SBHO Confidentiality Policy and the Disclosure Policy).
- Employees must not leave printers unattended when they are printing confidential information. This rule is especially important when two or more computers share a common printer or when the printer is in an area where unauthorized personnel have access to the printer.
- Personnel using the computer system will not write down their password and place it at or near the terminal, such as putting their password on a yellow "sticky" note on the screen or on a piece of tape under the keyboard.
- Each computer will be programmed to generate a screen saver when the computer receives no input for a specified period
- Users must log off the system if he or she leaves the computer terminal for more than thirty (30) minutes or if he/she is leaving the premises.
- No personnel may download protected health information (PHI) from SBHO system onto diskette, CD, hard drive, fax, scanner, any network drive or any other hardware, software, or paper without the express permission of their manager with written notice to the Privacy Officer.
- No personnel shall download any software without express written permission of the IS Manager. The IS Manager must approve any software than an employee wishes to download in order to protect against the transmission of computer viruses into the system.

File Naming Procedures

Any documents or files that contain PHI and are retained by SBHO must include "PHI" in the file name and saved to the secure and confidential drive.

Portable Computer

Officers, agents, employees, contractors, and others using portable computers (users) must read, understand, and comply with this policy.

No user may, for any purpose, download, maintain, or transmit, confidential or other PHI on a computer without the written authorization of the Privacy Officer upon the recommendation of their manager.

SBHO strongly discourages the storage of PHI on portable devices by network providers.

Any provider that utilizes portable electronic devices (including but not limited to laptops, thumb drives, removable drives, etc.) to store PHI must have a current encryption strategy policy.

Any portable equipment and all related components, and data are the property of SBHO and must be safeguarded and be returned upon request and upon termination of your employment. You are responsible for the equipment SBHO issues you during your employment.

The user agrees to use the equipment solely for SBHO business purposes. The user further understands:

- Dial in functions are restricted to dialing into SBHO. User is not permitted to dial into any other unauthorized services, Internet service providers, or any other Internet access or to use the dial-up capabilities in any other manner than as instructed.
The user understands that the hardware has been disabled from performing any functions other than those intended for business use and that the user may not attempt to enable such other functions.
- Computers, associated equipment, and software are for business use only, not for the personal use of the user or any other person or entity.
- Users will not download any software onto the computer except as loaded by authorized staff of the Information Services department.
- Users must use only batteries and power cables provided by SBHO and may not, for example, use their car's adaptor power sources.
- Users will not connect any non-SBHO peripherals (keyboards, printers, modems, etc.) without the express authorization of the Information Services department.
- Users are responsible for securing the unit, all associated equipment, and all data, within their homes, cars, and other locations.
- Users may not leave mobile computer units unattended unless they are in a secured location.
- Users should not leave mobile computer units in cars or car trunks for an extended period in extreme weather (heat or cold) or leave them exposed to direct sunlight.
- Users must place portable computers and associated equipment in their proper carrying cases when transporting them.
- Users must not alter the serial numbers and asset numbers of the equipment in any way.
- Users will not permit anyone else to use the computer for any purpose, including, but not limited to, the user's family and/or associates, clients, client families, or unauthorized officers, employees, and agents of SBHO.
- Users must not share their passwords with any other person and must safeguard their passwords and may not write them down so that an unauthorized person can obtain them. (See the Password Protection procedure)
- Users must report in writing any breach of password security immediately to the Privacy Officer.

- Users must maintain confidentiality when using the computers. The screen must be protected from viewing by unauthorized personnel, and users must properly log out and turn off the computer when it is not in use.
- Users must immediately report in writing any lost, damaged, malfunctioning, or stolen equipment or any breach of security or confidentiality to the Privacy Officer.

Enforcement

All managers are responsible for enforcing this procedure. Employees who violate this procedure are subject to discipline.

MONITORING

1. This policy is mandated by contract and statute.
 - This policy will be monitored through 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 Policy.