SALISH BHO

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

Policy Name: PASSWORD PROTECTION PROCEDURE **Policy Number:** 5.10

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

Effective Date: 5/2005

Revision Date(s): 5/2016

Reviewed Date: 5/2016; 6/2017; 5/2018

Approved by: SBHO Executive Board

CROSS REFERENCES

- Agreement: Business Associate Addendum
- Policy: Corrective Action Plan

PURPOSE

The Salish Behavioral Health Organization's (SBHO) mission and guiding ethical principal places great value on the privacy and confidentiality information. Beyond these principles, this privacy and security are mandated by state and federal laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and 42 CFR Part 2.

These regulations require that SBHO deploy and maintain a set of policies, practices, and technologies to safeguard confidential information and ensure that such information is not disclosed to anyone without the proper authorization to view or possess such information.

PROCEDURE

<u>Access Codes and Passwords</u>

The confidentiality and integrity of data stored on company computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties. The Information Services department will institute a system of access controls consisting first of a unique identification code and password requirement for each employee with a need to use SBHO computer systems and networks. The characteristics of the password requirement will be established by the Kitsap County Information Services department.

Information Services Responsibilities

- The Information Services department shall be responsible for the administration of access controls to all company computer systems.
- The Information Services department will deploy and maintain a set of system/network access and password procedures that require unique user identification codes and passwords that conform to standardized characteristics.
- The Information Services department will maintain a list of administrative access codes and passwords and keep this list in a secure area.
- The Information Services department will assign responsibility for maintenance of the access code and password assignment to a qualified individual in the Information Services department. Additionally, a back-up staff person of the department will also be assigned these duties as a backup to the primary staff person.
- No less than annually, the Information Services department will conduct an audit of the access code and password policy and practice. The results of this audit will be forwarded to the Privacy Officer.

Employee Responsibilities

Each employee:

- Shall be responsible for all computer transactions that are made with his/her User ID and password.
- Shall not disclose passwords to others. This should be strictly interpreted by all staff. If a password is requested from an employee, the employee should verify the identity of that person with the Information Services department staff member responsible for maintenance of the access codes and passwords. If the responsible staff are not available, the employee is instructed not to disclose his/her password.
- Passwords must be changed immediately if it is suspected that they may have become known to others. In the event that an employee suspects or knows that his/her password has become known to an unauthorized person, the employee should immediately report this event to the following agency staff:
    a. The designated staff person in the Information Services department responsible for maintenance of access codes and passwords
    b. The Privacy Officer
- Passwords should not be recorded where they may be easily obtained. Employees shall not display passwords in any area that can be viewed by others. This means practically that passwords should not be written on “sticky” notes on the monitor, placed on paper and taped to the bottom of the keyboard, etc.
- Will change passwords at least every 60 days.
- Should use passwords that will not be easily guessed by others.
- Should log out when leaving a workstation for more than 30 minutes or when leaving the premises for any length of time.

Managers' Responsibility

Managers should notify the Information Services department promptly whenever an employee leaves the company so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

Enforcement

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

MONITORING

This policy is a mandate by contract and 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.