



SALISH BHO

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

Policy Name: REMOVAL OF PHI FROM OFFICE

Policy Number: 5.22

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

Effective Date: 5/2016

Revision Date(s):

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

Approved by: SBHO Executive Board

CROSS REFERENCES

- Plan: Compliance Plan
- Policy: Corrective Action Plan

PURPOSE

The Salish Behavioral Health Organization (SBHO), in an effort to be compliant with the federal and state statutes, all requirements of the Health Insurance Portability and Accountability Act (HIPAA) confidentiality and use/ disclosure of protected health information, and in accordance with 42 CFR Part 2, optimizes the security regarding the removal of PHI from office.

DEFINITIONS

Protected Health Information (PHI) - individually identifiable information relating to past, present or future physical, substance use, mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.

Workforce Members- employees, volunteers, trainees, and other persons whose conduct, in the performance of work for SBHO, its offices, programs or facilities, is under the direct control of SBHO, office, program or facility, regardless of whether they are paid by SBHO.

POLICY

In general, all PHI (Protected Health Information) must remain at the office. In certain circumstances, with the approval of the Director or Privacy Officer, PHI may be taken out of the office. This may take the form of traveling employees or employees working from home.

PROCEDURE

Originals are not taken off site. Copies are made for transport. Paper copies are shredded when no longer needed. Electronic copies are deleted.

All PHI taken off site is locked in a suitable container such as a locking file box or briefcase. When not in use, PHI removed from the office is protected from access by unauthorized persons using locking containers or software encryption if PHI is stored on removable storage media.

The above items apply to PHI in paper files, laptops, and electronic removable storage media such as computer disks, tape back-up media, and USB jump drives.

All PHI on electronic removable storage media and laptops are encrypted and password protected.

Penalties for violation.

MONITORING

This Policy is mandated by contract and statute.

1. This Policy will be monitored through use of SBHO:
 - Quality Management Plan activities, such as review targeted issues for trends and recommendations
2. If a provider performs below expected standards during any of the reviews listed above a Corrective Action will be required for SBHO approval. Reference SBHO Corrective Action Plan Policy.
3. Additional disciplinary actions and sanctions, per the Kitsap County policy, may also be enforced for failure to comply with this policy.