SALISH BHO

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

Policy Name: HIPAA and PRIVACY AGENCY STAFF TRAINING **Policy Number:** 5.05

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

Effective Date: 8/2005

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

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

Approved by: SBHO Executive Board

CROSS REFERENCES

- Policy: Corrective Action Plan

PURPOSE

The Salish Behavioral Health Organization (SBHO), in an effort to be ensure staff are knowledgeable with the Privacy Rules of Health Insurance Portability and Accountability Act's (HIPAA) Administrative Simplification provisions and 42 CFR Part 2, sets out in this policy, to define requirements for training of the Privacy and Security Regulations of the law.

POLICY

1. SBHO stores protected health information electronically and bills for services electronically so are considered a "covered entity" under HIPAA.
2. SBHO trains agency staff at least annually on the requirements of the Privacy and Security Regulations of the law. The training curriculum is reviewed and modified as required annually through the efforts of the Privacy Officer of the agency.

PROCEDURE

1. HIPAA recommends that agency staff is trained every year on the requirements of the Privacy and Security Regulations of the law.
2. The training outline includes the following:

   An Overview of the Law

   - Technology
   - Policy
   - Practice

     - Purpose of the Privacy Regulations

- Purpose of the Security Regulations
- Purpose of the Breach Notification Regulations
- Purpose of the Standardization of the Transaction and Code Sets

Privacy Regulations

- Definition of Protected Health Information
  - Individual Rights to Notice, Access, Accounting and Modification.
  - Business Relationships
  - Policies and Procedures of the Agency
  - Need to Know “Minimal Necessary Disclosure”

Security Regulations

- Administrative Safeguards
  - Contingency Plan
  - Chain of Trust Agreements
  - Access procedures
  - Incident Response Procedures
  - Virus Protection and Backup requirements
  - Media Controls (use and storage of disks).
- Technological
  - Authorization Controls
  - Data Authentication
  - Unique User ID
  - Passwords/PIN/Tokens (Password Management)
  - Automatic Log off
- Physical Safeguards
  - Assigned Security Responsibility
  - Physical Access Control
  - Controls over physical media
  - Secure Workstation Location
  - Policy over Workstation Use
  - Security Awareness Training
  - Work Station Use

Breach Notification Regulations

- Definition of a Breach
  -Description of Unsecured Protected Health Information
  -Disclosures excluded from Breach definition
  -Identifiers that compromise the security or privacy of the PHI
- Agency Process for breach identification
  -Procedure for informing appropriate agency staff
  -Method for determining whether incident was a breach or not

- Notification Requirements
  -Timeliness of Notification
  -Content of Notification
  -Methods of notification
  -Requirement to inform the HHS Secretary
- Documentation Requirements
  -Agency procedure for documenting potential breach incidents

MONITORING

This policy is mandated by 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 Policy.