SALISH BHO

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

Policy Name: BUSINESS ASSOCIATES **Policy Number:** 5.21

Reference: 45 CFR 164.308, 42 CFR Part 2, State Contract

Effective Date: 5/2016

Revision Date(s):

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

Approved by: SBHO Executive Board

CROSS REFERENCES:

- Plan: Compliance Plan, FY 2018
- Policy: 5.03 Privacy Administrative Requirements
- Policy: 5.07 Confidentiality, Use, and Disclosure of Protected Health Information
- Policy: 5.21a Business Associate Addendum
- Table: SBHO Compliance Plan Checklist

PURPOSE

To identify Business Associates and their unique requirements, to ensure regular review of Business Associates' policies and procedures for HIPAA compliance, and to ensure compliance with contractually required oversight.

DEFINITIONS

Health Insurance Portability and Accountability Act of 1996 (HIPAA) - This Act requires, among other things, under the Administrative Simplification subtitle, the adoption of standards, including standards for protecting the privacy of individually identifiable health information, comprehensively including the closely-related Health Information Technology for Economic and Clinical Health (HITECH) Act.

42 CFR Part 2 - Federal regulations, enacted in 1987, governing the confidentiality of drug and alcohol abuse treatment and prevention records. The regulations set forth requirements applicable to certain federally assisted substance abuse treatment programs limiting the use and disclosure of substance abuse patient records and identifying information.

Business Associate - A person or entity who, on behalf of a covered entity, performs or assists in performance of a function or activity involving the use or disclosure of individually identifiable health information, such as data analysis, claims processing or administration, utilization review, and quality assurance reviews, or any other function or

activity regulated by the HIPAA Administrative Simplification Rules, including the Privacy Rule. Business associates are also persons or entities performing legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity where performing those services involves disclosure of individually identifiable health information by the covered entity or another business associate of the covered entity to that person or entity. A member of a covered entity's workforce is not one of its business associates. A covered entity may be a business associate of another covered entity.

Business Associate Agreement - A document of the Covered Entity between the Covered Entity and the Business Associate that, at a minimum, addresses the following: 1) the legal requirement to follow HIPAA and HITECH for security and privacy protections, 2) the responsibility for use and management of information, 3) the express use of PHI for Covered Entity-approved purposes only, 4) information accessibility obligations, 5) breach reporting requirements, and 6) data handling requirements on termination of services.

Covered Entity - A health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with a transaction for which HHS has adopted a standard.

Covered Function – Functions that make an entity a health plan, a health care provider, or a health care clearinghouse. See the definition for Business Associate for additional information regarding the determination of a Business Associate.

Individually Identifiable Health Information - Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) relates to the past, present, or future physical, substance use, mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Protected Health Information (PHI) - PHI is individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

Workforce - Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of the covered entity, whether or not they are paid by the covered entity.

POLICY

Every entity or individual providing a service, function, or product to the Covered Entity shall be evaluated according to the procedure herein to determine whether it is a Business Associate prior to the entity or individual being granted access to PHI.

Every Business Associate of the Covered Entity shall sign a Business Associate Agreement that has been approved by the Covered Entity's Privacy Officer prior to the entity or individual being granted access to PHI.

- Business Associate Agreement must include a provision for the complete destruction of all copies of data received as a result of the Business Associate's service provided for the Covered Entity upon termination of services; or, in the event that it is not possible or feasible to completely destroy all copies of the data, the Business Associate shall agree to continue to provide the data the protections afforded by HIPAA as long as it shall retain the data.
- Business Associates must be audited for compliance with the signed Business Associate Agreement at minimum biennially, beginning no later than six(6) months following the beginning of service.
- Organizations within the SBHO with a common Business Associate may conduct a single biennial audit of the common Business Associate. This final combined audit must contain a list of all Covered Entities that participated in the audit of the Business Associate.
- SBHO and its network providers have 90 days from the date of approval of this policy by the SBHO Board of Directors to implement this policy in their respective organizations.

PROCEDURE

Every contracted entity or individual must be evaluated against three criteria to determine whether it is a Business Associate. The failure to have a signed Business Associate Agreement for a contracted entity or individual that is a Business Associate is a violation of HIPAA (164.308)(8)(b)(1). If the answers to questions below, specifically one (1) and three (3) are "yes" and question two (2) is "no", the entity or individual is a Business Associate.

1. Are they performing a covered function for us on our behalf?
2. Are they a member of our workforce?
3. Do they use PHI to do their job?

The biennial audit must include a review of the Business Associate's policies and procedures that demonstrate compliance with the Business Associate Agreement and by extension HIPAA. Contractual requirements with the State and/or the SBHO require a review of the Business Associate's processes specifically regarding the access, storage, transportation and deletion (upon termination of the contract) of data.

POLICY MONITORING

This Policy is a mandated by contract and statute.

1. This Policy will be monitored through use of SBHO:
    - SBHO Compliance Committee review, at least annually
    - Annual SBHO Provider and Subcontractor Administrative Review
    - Annual Encounter Validation Study
    - Monthly Excluded Provider Attestation Tracking
    - Annual SBHO Provider Fiscal Review
    - Annual Provider Chart Reviews

- Grievance Tracking Reports
- Biennial Provider Quality Review Team On-site Review
- Semi-annual Provider Revenue and Expense Report
- Quality Management Plan activities, such as review targeted issues for trends and recommendations
- Review of previous Provider Corrective Action Plans related to policy, including provider profiles related to performance on targeted indicators

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 SBHO Compliance Plan and SBHO contract, may also be enforced for failure to comply with this policy.