Effective Date: 7/17/2013; 4/14/2003, Motion #03-013
Revised Date: 2/27/2018
Review Date: 2/27/2018

North Sound Behavioral Health Organization

Section 2500 – Privacy: Business Associates/Qualified Service Organizations

Authorizing Source: 45 CFR 164 (HIPAA); 42 CFR Part 2 (Part 2); RCW 70.02
Cancels:
See Also:
Responsible Staff: Privacy Officer
Executive Director's Signature:

Approved by: Board of Directors
Motion #: 03-013 Date: 4/14/2003

Date: 3/6/2018

POLICY #2507.00

SUBJECT: BUSINESS ASSOCIATES AND QUALIFIED SERVICE ORGANIZATIONS

PURPOSE

In compliance with Health Insurance Portability and Accountability Act (HIPAA), Part 2 and Washington law, this policy sets out the nature of third-party relationships with Business Associates and Qualified Service Organizations (QSO) as well as other contractors and the requirements for contracting with these entities with the Business Associates/QSOs.

Capitalized terms have specific meanings. Defined terms in this policy include Business Associate, Business Associate Agreement (BAA), Part 2 Information, Protected Health Information (PHI), QSO, Qualified Service Organizations Agreement (QSOA), Required by Law, and Subcontractor. See Policy 2502.00: Definitions for Policies Governing PHI.

POLICY

North Sound Behavioral Health Organization (North Sound BHO) will determine whether any vendor, independent contractor, or Subcontractor is a Business Associate and/or a QSO. North Sound BHO shall not permit a Business Associate/QSO to create, receive, maintain, or transmit any PHI, including Part 2 Information, unless the Business Associate/QSO first provides written assurances, usually in the form of a BAA/QSOA.

Additionally, North Sound BHO, from time to time, may be acting as a Business Associate, a contractor to a lawful holder of Part 2 Information, or a QSO and will comply with its obligations under a BAA, QSOA, or agreement with the lawful holder of Part 2 Information and with federal and state law, including HIPAA, Part 2 and Washington Law.

PROCEDURES

1. **Identification of Business Associates**. North Sound BHO will consider any third-party, who is not a member of the Workforce, to be a Business Associate when the person or entity creates, receives, maintains, or transmits PHI on North Sound BHO's behalf or when providing certain services to North Sound BHO. This includes claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, repricing, legal, actuarial, accounting, consulting, data aggregation, management,

administrative, accreditation, or financial services if those functions or services involve the creation, receipt, maintenance, or transmission of PHI. The determination of whether a Subcontractor is a Business Associate depends not on what it is, but on the basis of the services or functions it provides to North Sound BHO and whether it creates, receives, maintains, or transmits of PHI, including Part 2 Information, in the course of performing its services for North Sound BHO.

1.1 **Business Associate Definition.** A Business Associate, with respect to a Covered Entity, is any person or entity (other than in the capacity of Workforce) who:

1.1.1 Activities on Behalf of a Covered Entity Involving PHI. On behalf of a Covered Entity (or Organized Health Care Arrangement in which the Covered Entity participates) creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing, or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management and repricing;

1.1.2 Services Involving PHI. Provides to a Covered Entity (or Organized Health Care Arrangement in which the Covered Entity participates) legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services involving the disclosure of PHI from the Covered Entity or organization; and/or

1.1.3 Specified Entity. Is: (a) a health information organization, e-prescribing gateway, or other person that provides data transmission services with respect to PHI and requires access on a routine basis to the PHI; (b) a person who offers a personal health record to Individuals on behalf of a Covered Entity; and/or (c) a Subcontractor that creates, receives, maintains, or transmits PHI on behalf of a Business Associate.

1.2 **Excluded as a Business Associate**. A Business Associate is NOT:

1.2.1 A Health Care Provider receiving PHI for Treatment purposes, even if doing so under contract with and on behalf of North Sound BHO;

1.2.2 A financial institution (or entity acting on behalf of a financial institution) engaging in financial transactions;

1.2.3 A sponsor of a Health Plan (for Health Plan activities);

1.2.4 A government agency for determining eligibility for or enrollment in a government health plan;

1.2.5 A Subcontractor that receives or accesses only De-Identified Data (but would be a Business Associate if it were De-Identifying PHI) See Policy 2503.00: De-Identification and Limited Data Sets;

1.2.6 A Covered Entity performing services on behalf of an Organized Health Care Arrangement in which it participates; or

1.2.7 Workforce of North Sound BHO.

2 **Identification of QSOs.** North Sound BHO will consider any third-party to be a QSO when the person or entity provides any of the following services to a Part 2 Program involving Part 2 Information: data processing, bill collecting, dosage preparation, laboratory analyses, or legal, medical, accounting, other professional services, population health management, or services to prevent or treat child abuse or neglect, including training on nutrition and child care and individual and group therapy.

3 **Contractual Obligations**

3.1 **Written Assurances**. North Sound BHO, through its Privacy Officer, requires any Business Associate of North Sound BHO to sign a BAA or another document that meets HIPAA requirements. Because North Sound BHO regularly receives Part 2 Information through the authorization by or on behalf of an Individual and, therefore, acts as a lawful holder of Part 2 Information, North Sound BHO, through its Privacy Officer, will require additional contractual obligations on any of its Business Associates that are to create, receive, maintain, or transmit Part 2 Information.

3.2 **When Acting as a Business Associate or QSO.** In the event the North Sound BHO qualifies as a Business Associate, it will enter into a BAA with the Covered Entity or Business Associate as a Business Associate. If the Covered Entity has a Part 2 Program and North Sound BHO will handle Part 2 Information on the Covered Entity's behalf, then the BAA or other written assurances will include QSOA provisions.

3.3 **Content of BAA—HIPAA Requirements.** North Sound BHO prefers to use one of its template agreements, which includes the expanded obligations for Part 2 Information. Not all relationships will require the expanded BAA requirements, and some Business Associates will insist on using their template agreements. For these reasons, before executing any BAA that modifies the template or that is not a North Sound BHO template, the responsible Workforce member must obtain approval of the Privacy Officer, who may consult with legal counsel. A BAA, at a minimum, shall contain the following provisions:

3.3.1 Establish the permitted and required uses and disclosures of PHI by the Business Associate;

3.3.2 Not authorize the Business Associate to use or further disclose the PHI in a manner that would not be permissible under the HIPAA Privacy Rule, if done by the Covered Entity, except for data aggregation or management/administration/legal obligations of the Business Associate, if permitted by the Covered Entity;

3.3.3 Not use or further disclose the PHI other than as permitted or required by the BAA or as Required by Law;

3.3.4 Use appropriate safeguards to protect the PHI;

3.3.5 Comply with the HIPAA Security Rule with respect to electronic PHI;

3.3.6 Report to the Covered Entity any use or disclosure of PHI not provided for by the BAA of which it becomes aware;

3.3.7 Report to the Covered Entity any Breach of Unsecured PHI;
3.3.8 Report to the Covered Entity any Security Incident, which may include certain proactive notification (with no further notification required) for Security Incidents that do not represent risk to PHI such as pings on a firewall;
3.3.9 Ensure any Subcontractor that creates, receives, maintains, or transmits PHI on the Business Associate's behalf agrees to the same restrictions and conditions that apply to the Business Associate with respect to PHI, including complying with the Security Rule;
3.3.10 Make available PHI to facilitate access to PHI;
3.3.11 Make available PHI for amendment and incorporate any amendments to PHI maintained;
3.3.12 Provide an accounting of disclosures;
3.3.13 Make its internal practices, books and records relating to the use and disclosure of PHI received from, or created, or received by the Business Associate on behalf of, the Covered Entity available to the Secretary of the Department of Health and Human Services (DHHS) for purposes of determining compliance with HIPAA;
3.3.14 To the extent the Business Associate is to carry out an obligation of the Covered Entity under the Privacy Rule, comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of the obligation; and
3.3.15 Upon termination of the BAA, if feasible, return or destroy all PHI received from, or created, or received by the Business Associate on behalf of, the Covered Entity the Business Associate still maintains in any form and retain no copies of the PHI or if return or destruction is not feasible, extend the protections of the BAA to the PHI and limit further uses and disclosures of the PHI to those purposes that make the return or destruction of the PHI infeasible.

3.4 **Expanded Part 2 Content Requirements.** When a Business Associate, which is providing Payment or Health Care Operations services to North Sound BHO, will create, receive, maintain, or transmit Part 2 Information, the BAA also must provide the Business Associate:

3.4.1 Is fully bound by the provisions of Part 2 upon receipt of Part 2 Information; and
3.4.2 Receives from North Sound BHO one (1) of the two (2) following notices:

(a) This information has been disclosed to you from records protected by federal confidentiality rules (42 CFR part 2). The federal rules prohibit you from making any further disclosure of information in this record that identifies a patient as having or

having had a substance use disorder (SUD) either directly, by reference to publicly available information or through verification of such identification by another person unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose (see § 2.31). The federal rules restrict any use of the information to investigate or prosecute with regard to a crime any patient with SUD, except as provided at §§ 2.12(c)(5) and 2.65;

or

(b) 42 CFR Part 2 prohibits unauthorized disclosure of these records.

3.4.3 Implements appropriate safeguards to prevent unauthorized uses and disclosures of Part 2 Information;

3.4.4 Report any unauthorized uses, disclosures, or breaches of Part 2 Information to North Sound BHO; and

3.4.5 Not re-disclose Part 2 Information to a third-party unless the third-party is a contract agent of the Business Associate helping the Business Associate provide services described in the services agreement and only if the agent only further discloses the Part 2 Information back to the Business Associate or to North Sound BHO.

3.5 **Content of QSOA.** Part 2 Programs must enter into QSOAs with their QSOs. It is possible, although unlikely, that North Sound BHO would be deemed a QSO. A QSOA which may be combined with a BAA, shall contain the following additional provisions:

3.5.1 To the extent in performing services for or on behalf of a Part 2 Program, the QSO uses, discloses, maintains, or transmits Part 2 Information, which governs SUD records from a federally assisted alcohol or drug abuse program, the QSO acknowledges and agrees that:

(a) In receiving, storing, processing, or otherwise dealing with any Part 2 Information, it is fully bound by Part 2; and

(b) If necessary, will resist in judicial proceedings any efforts to obtain access to Part 2 Information except as permitted by Part 2.

The QSO shall acknowledge and agree any Part 2 Information it receives is subject to protections that prohibit the QSO from disclosing Part 2 Information to agents or Subcontractors without the specific written consent of the Individual.

3.6 **Additional Provisions.** North Sound BHO may negotiate additional provisions in its agreements to further protect North Sound BHO and the Individuals who receive services through North Sound BHO. These provisions include requiring insurance/cyber (data privacy/network security) insurance, indemnification, more restrictive Breach notification timeframes, or documentation requirements and removal of limitations of liability. Workforce responsible for negotiating agreements, including BAAs, should consult legal counsel when appropriate.

3.7 **Amendments.** Amendments to a template or existing BAA or QSOA may not be made without the Privacy Officer and/or the prior advice and recommendation of North Sound BHO's legal counsel.

3.8 **Monitoring of Business Associates.** Because the protection of PHI is of crucial importance to North Sound BHO, Workforce should be cognizant of the behavior of Business Associates and report any conduct that is inconsistent with the BAA to North Sound BHO's Privacy Officer.

3.9 **Documentation.** All BAAs and QSOAs along with any accompanying documentation shall be retained for at least six (6) years. Documentation retention requirements include:

3.9.1 **Policies and procedures for Business Associates/QSOs**;
3.9.2 **BAA/QSOA templates; and**
3.9.3 **Executed Business Associate Agreements/QSOAs.**

3.10 **Other Policies.** Other policies and procedures to review that are related to this policy:

3.10.1 Policy 2500.00: Privacy and Confidentiality;
3.10.2 Policy 2502.00: Definitions for Policies Governing PHI;
3.10.3 Policy 2503.00: De-Identification & Limited Data Sets; and
3.10.4 Policy 2522: Uses and Disclosures of PHI.

FORMS

Template Business Associate Agreement