Effective Date: 7/1/2019
Review Date: 7/30/2019
Revised Date:

North Sound Behavioral Health Administrative Services Organization, LLC

Section 2500 – Privacy: Breach Notification and Reporting to Upstream Covered Entities Under HIPAA

Authorizing Source: 45 CFR 164 (HIPAA); 42 CFR Part 2 (Part 2); RCW 70.02
Approved by: Executive Director Date: 7/30/2019 Signature:

POLICY # 2525.00

SUBJECT: BREACH NOTIFICATION AND REPORTING TO UPSTREAM COVERED ENTITIES UNDER HIPAA

PURPOSE

In compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Part 2, Washington law and any applicable Business Associate Agreements (BAAs) with Upstream Covered Entities, this policy establishes the process by which North Sound Behavioral Health Administrative Services Organization (North Sound BH-ASO), in North Sound BH-ASO's role as a Business Associate for certain Upstream Covered Entity and in its role as a former Covered Entity with respect to Pre-Transition PHI, shall provide notification of a Breach of Unsecured PHI and other events that require notification.

Capitalized terms have specific meanings. Defined terms in this policy include Breach, Business Associate Agreement (BAA), Disclosure or Disclose, Protected Health Information (PHI), Security Incident, Upstream Covered Entity, Use and Workforce. See Policy 2502.00: Definitions for Policies Governing PHI.

POLICY

North Sound BH-ASO will provide appropriate notifications with respect to PHI, create a culture of compliance and comply with applicable federal law and State Law this policy, other relevant North Sound BH-ASO policies, procedures and practices and applicable BAAs.

To the extent that North Sound BH-ASO creates, receives, maintains or transmits PHI from or on behalf of an Upstream Covered Entity in its role as the Business Associate of the Upstream Covered Entity, North Sound BH-ASO will notify the Upstream Covered Entity and make other notifications that are required or determined to be appropriate in the event of: (a) a Breach of Unsecured PHI; (b) an impermissible Use or Disclosure of PHI; or (c) a reportable Security Incident.

To the extent that North Sound BH-ASO discovers any Breach of Unsecured Pre-Transition PHI, in its role as a former Covered Entity, North Sound BH-ASO will provide required or appropriate notifications to affected Individuals, the Department of Health and Human Services and, if required, the media.

North Sound BH-ASO Workforce must report **immediately** to the Privacy Officer or Security Officer any actual or suspected unauthorized (or otherwise impermissible) acquisition, access, Use, Disclosure, modification or destruction of PHI or other identifiable information and any interference with systems operations of its information systems. North Sound BH-ASO will not retaliate against anyone for making good faith reports under this policy.

PROCEDURE

1. **Notification Obligations.** North Sound BH-ASO has certain notification obligations: (a) in its role as a Business Associate of Upstream Covered Entities; and (b) with respect to Pre-Transition PHI, in its role as a former Covered Entity.

2. **Internal Reporting of Actual or Suspected Breaches and Other Events.** Workforce members of North Sound BH-ASO will report immediately, to the Privacy Officer or Security Officer, actual or suspected unauthorized (or otherwise impermissible) acquisition, access, Use, Disclosure, modification or destruction of PHI and interference with the systems operations of the information systems.

3. **Response to Notifications Reports, Complaints and Concerns.** The Privacy Officer or Security Officer, without unreasonable delay, will conduct or coordinate an appropriate investigation of any notifications, reports, complaints or concerns, which may include from Workforce, Subcontractor Business Associates, Individuals, Upstream Covered Entities and others, relating to actual or suspected unauthorized (or otherwise impermissible) acquisition, access, Use, Disclosure, modification or destruction of PHI and/or Security Incidents.

4. **Determination of Notification Obligations as a Business Associate.** Based on the information obtained during the investigation, the Privacy Officer, which may be in consultation with legal counsel or the Security Officer, will determine whether North Sound BH-ASO needs to provide notification to an Upstream Covered Entity or to take any further actions under this policy. Workforce members should not attempt to make these determinations themselves.
   - 4.1 **Reporting Impermissible Use or Disclosure.** If it is determined that a Use or Disclosure of PHI was impermissible under its BAA, then North Sound BH-ASO will report to the applicable Upstream Covered Entity the impermissible Use or Disclosure, as required under its BAA, even if the Use or Disclosure does not constitute a Breach of Unsecured PHI that requires notification under the Breach Notification Rule.
   - 4.2 **Reporting of a Security Incident.** If it is determined that a Security Incident occurred, then North Sound BH-ASO will report the Security Incident to the affected Upstream Covered Entity to the extent reporting is required by its BAA. BAAs may not require reporting of every type of Security Incident, such as for unsuccessful Security Incidents.
   - 4.3 **Breach Notification.** If it is determined that a Breach of Unsecured PHI occurred, then North Sound BH-ASO will notify the applicable Upstream Covered Entity, as required by the Breach Notification Rule and its BAA. The Privacy Officer will make the determinations as described in Section 6 to determine whether North Sound BH-ASO must provide notification of a Breach of Unsecured PHI.
   - 4.4 **Other Notification.** North Sound BH-ASO will provide notifications that are required under State Law. See also Section 11.

5. **Determination of Notification Obligations with respect to Pre-Transition PHI.** Based on the information obtained during the investigation, the Privacy Officer, which may be in consultation with legal counsel or the Security Officer, will determine whether North Sound BH-ASO needs to provide notification of a Breach of Unsecured Pre-Transition PHI and to take other actions under this policy. Notification of a Breach of Unsecured Pre-Transition PHI would be to: (a) Individuals; (b) the Department of Health and Human Services; and (c) media, if more than 500 Individuals have been affected. The Privacy Officer will make the determinations as described in Section 6 to determine

whether North Sound BH-ASO must provide notification of a Breach of Unsecured PHI. Additionally, North Sound BH-ASO will provide notifications that are required under State Law. See Section 11.

6. **Breach of Unsecured PHI.** The Privacy Officer, which may be in consultation with legal counsel or the Security Officer, will make the determinations described below to determine whether a reportable Breach of Unsecured PHI occurred. To assist in determining whether notification for a Breach of Unsecured PHI is required, see Exhibit A for a decision tree and see the definition for "Breach" under Policy 2502.00: Definitions for Policies Governing PHI.

6.1 **Whether PHI was Involved.** PHI, in any medium, must be involved to trigger HIPAA's notification requirements. For example, De-Identified Data is not PHI and would not trigger Breach notification obligations.

6.2 **Whether the PHI was "Unsecured."** This generally means that the PHI was encrypted or shredded. "Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in guidance issued by the Secretary of the Department of Health and Human Services. For more information in what constitutes Unsecured PHI, see http://www.hhs.gov/ocr/privacy. Generally, PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals if one or more of the following applies:

6.2.1 Electronic PHI has been encrypted, which requires: (a) the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key; (b) the confidential process or key that might enable decryption has not been breached; and (c) decryption tools be stored on a device or at a location separate from the data that were used to encrypt or decrypt. Mere access controls, such as firewalls and passwords, will not suffice. Information is not considered encrypted if the encryption keys are kept on the same storage device as the encrypted data.

6.2.2 The media on which the information is stored or recorded has been properly destroyed. For paper, film or other had copy media, the media have been shredded or destroyed so that the PHI cannot be read or otherwise cannot be reconstructed. Redaction specifically is excluded as a means of data destruction.

6.2.3 Electronic media has been cleared, purged or destroyed consistent with the standards established by the National Institute of Standards and Technology.

6.3 **Whether PHI was Acquired, Accessed, Used, or Disclosed in an Unauthorized Manner.** To constitute a Breach, there must be an unauthorized acquisition, access, Use or Disclosure of PHI.

6.4 **Whether there was a Use or Disclosure that was not Permissible under the Privacy Rule.** To require notification, the unauthorized acquisition, access, Use or Disclosure must constitute an impermissible Use or Disclosure under the Privacy Rule. For example, incidental disclosures that are permissible under the Privacy Rule would not trigger notification under the Breach Notification Rule.

6.5 **Whether an Exception to the Notification Requirement Applies.** Exceptions to the definition of Breach are:

6.5.1 Any unintentional acquisition, access or Use of PHI, that is not further Disclosed, by a North Sound BH-ASO Workforce member (or person authorized by a Covered Entity or Business Associate) if the acquisition, access or Use was made in good faith and within the scope of authority and does not result in further Use or Disclosure in a manner not permitted by the Privacy Rule.

6.5.2 Any inadvertent Disclosure of PHI from one authorized person to another within North Sound BH-ASO without further Disclosure that would not be permitted by the Privacy Rule.

6.5.3 A Disclosure of PHI where North Sound BH-ASO has a reasonable belief that the unauthorized person who received the PHI would not reasonably have been able to retain the PHI.

6.6 **Presumption.** An unauthorized acquisition, access, Use or Disclosure of Unsecured PHI in a manner that is impermissible under the Privacy Rule and that does not fall within an exception as described in Section 6.5 of this policy is presumed to be a Breach that requires notification.

6.7 **Whether the Presumption Can Be Overcome.** The presumption that a reportable Breach occurred may be overcome if North Sound BH-ASO demonstrates there is a low probability that the PHI has been compromised based on a risk assessment. The risk assessment must be thorough, completed in good faith, and have reasonable conclusions. The risk assessment shall evaluate the overall probability that the PHI has been compromised and shall evaluate at least the following four (4) factors:

6.7.1 The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification.

6.7.2 The unauthorized person who Used the PHI or to whom the Disclosure of PHI was made.

6.7.3 Whether the PHI actually was acquired or viewed.

6.7.4 The extent to which the risk to the PHI has been mitigated.

7. Timing of Notification.

7.1 **Notice of Upstream Covered Entities.** Unless otherwise specified in Section 7 or unless a shorter time period is required in the applicable BAA, North Sound BH-ASO will provide notification of a Breach of Unsecured PHI without unreasonable delay and in no case later than sixty (60) calendar days after the discovery of a Breach. For purposes of this policy, a Breach will be treated as discovered by North Sound BH-ASO as of the first day on which the Breach is known to North Sound BH-ASO or, by exercising reasonable diligence, would have been known to any person, other than the person committing the Breach, who is an agent or a Workforce member of North Sound BH-ASO. The Privacy Officer also will determine whether North Sound BH-ASO is required to provide notice sooner than required above, such as if so required in the applicable BAA, in an urgent situation as described in Section 9.1.2 of this policy or as provided in Section 4.4, 8 or 11.

7.2 **Notice Relating to Pre-Transaction PHI.**

7.2.1 Notice to Individuals. Unless otherwise specified in Section 7, North Sound BH-ASO will provide notification of a Breach of Unsecured PHI to Individuals without unreasonable delay and in no case later than sixty (60) calendar days after the discovery of a Breach. A Breach will be treated as discovered by North Sound BH-ASO as of the first day on which the Breach is known to North Sound BH-ASO or, by exercising Reasonable Diligence, would have been known to any person, other than the person committing the Breach, who is an agent or a Workforce member of North Sound BH-ASO. The North Sound BH-ASO Privacy Officer also will determine whether North Sound BH-ASO is required to provide notice sooner than required above, such as in an urgent situation as described in Section 9.1.2 or as provided in Section 5, 8 or 11 of this policy.

7.2.2 Notification to the Department of Health and Human Services. Following the discovery of a Breach of Unsecured PHI, North Sound BH-ASO shall notify the Department of Health and Human Services as provided below.

(a) Large Breach. If a distinct Breach Involved five hundred (500) or more Individuals, then notification to the Department of Health and Human Services must be provided contemporaneously with the notification to the Individuals.

(b) Small Breach. If a distinct Breach involved fewer than 500 Individuals, then North Sound BH-ASO may maintain a log or other documentation of any Breach that occurs and not later than sixty (60) days after the end of each calendar year, submit the notification concerning the Breaches discovered during the preceding calendar year to the Department of Health and Human Services.

7.2.3 Media. If a distinct Breach involved more than 500 residents of a single state, then North Sound BH-ASO will provide notification to the media without unreasonable delay and in no case later than sixty (60) calendar days after discovery of the Breach.

8. **Delay of Notification.** If a Law Enforcement Official informs North Sound BH-ASO that a notification, notice or posting required under this Policy would impede a criminal investigation or cause damage to national security, then North Sound BH-ASO will delay notification as provided below.

8.1 **Written Law Enforcement Statement.** If the statement is in writing and specifies the time for which the delay is required, then North Sound BH-ASO will delay the notification, notice or posting for the time period specified by the Law Enforcement Official.

8.2 **Verbal Law Enforcement Statement.** If the statement is made verbally, then North Sound BH-ASO will document the statement, including the identity of the Law Enforcement Official making the statement, and delay the notification, notice or posting temporarily, but no longer than thirty (30) days from the date of the verbal statement, unless a written statement, as described in Section 8.1 above, is submitted during that time.

9. **Methods of Breach Notification.**

9.1 **Notification as a Business Associate.** Notification of a Breach of Unsecured PHI will be provided to the applicable Upstream Covered Entity. North Sound BH-ASO, which may maintain PHI from multiple Upstream Covered Entities, needs to provide notification to only the Upstream Covered Entities to whom the Breach relates. If, however, a Breach involves the Unsecured PHI of multiple Upstream Covered Entity and it is unclear to whom the Breached PHI relates, then it may be necessary to notify all potentially affected Upstream Covered Entity. Notification will meet the following requirements:

9.1.1 Notice. The notice will be written and delivered to the applicable Upstream Covered Entity addressed to the Upstream Covered Entity to the address as directed in BAA or to the Upstream Covered Entity's last known address.

9.1.2 In Urgent Situations. If North Sound BH-ASO determines that prompt action is required because of possible imminent misuse of Unsecured PHI or other urgent situation, then North Sound BH-ASO may provide information to the applicable Upstream Covered Entity by telephone or other means, as appropriate, in addition to the written notification required. Notice pursuant to Section 9.1.1 still must be provided.

9.1.3 Multiple Notifications. The notification may be provided in one or more submissions as information becomes available.

9.2 **Notification Concerning Pre-Transition PHI.**

9.2.1 HIPAA Breach Notification to Individuals. Notification of a Breach of Unsecured PHI to an Individual under HIPAA must have all the required content described in Section 10 and must meet the following requirements:

(a) Written Notice. The notice must be written and delivered to the Individual by first-class mail addressed to the Individual (or to the next-of-kin or Authorized Representative of the Individual if the Individual is deceased) at the Individual's (or next-of-kin's or Authorized Representative's) last known address, unless Section (b) or (c) applies.

(b) Electronic Notice. When the Individual (or next-of-kin or Authorized Representative) has agreed to electronic notice (and this agreement has not been withdrawn), the notification may be delivered by electronic mail.

(c) Substitute Notice. When there is insufficient or out-of-date contact information that precludes direct written (or, as appropriate, electronic) notification (under Section (a) or (b)), North Sound BH-ASO will provide substitute form of notice reasonably calculated to reach the Individual. When North Sound BH-ASO has insufficient or out-of-date contact information for fewer than ten (10) Individuals, substitute notice may be provided by an alternate form of written notice, telephone or other means. When there are ten (10) or more Individuals for which there is insufficient or out-of-date contact information, substitute notice will: (i) be in the form of either a conspicuous posting for a period of ninety (90) days on the home page of the North Sound BH-ASO website or conspicuous notice in major print or broadcast media in geographic areas where the Individuals affected by the Breach likely reside; and (ii) include a toll-free telephone number where an Individual can learn whether or not the Individual's Unsecured PHI was involved in the Breach. No substitute notice is required when the insufficient or out-of-date contact information is for the next-of-kin or personal representative of the Individual.

(d) Urgent Notice. If North Sound BH-ASO determines that prompt action is required because of possible imminent misuse of Unsecured PHI or other urgent situation, then North Sound BH-ASO may provide information to the applicable Individual by telephone or other means, in addition to the written notification required. Notice pursuant to Section 9.2.1(a), (b) or (c) still must be provided.

9.2.2 Department of Health and Human Services. North Sound BH-ASO shall provide notification to the Department of Health and Human Services through its website at http://www.hhs.gov/ocr/privacy.

9.2.3 Notification to Media. For a Breach of Unsecured PHI of more than five hundred (500) Individuals who are residents of a single state, North Sound BH-ASO shall notify prominent media outlets serving the applicable state. The press release or other media notification shall have all of the required elements of notice to Individuals, as described in Section 10.

10. **Content of Notification.** Notice of a Breach shall include, to the extent possible, the information set forth below.

10.1 **Affected Individuals.** For notification to an Upstream Covered Entity, the identification of each Individual about whom Unsecured PHI has been, or is reasonably believed by North Sound BH-ASO to have been, acquired, accessed, Used or Disclosed during the Breach.

10.2 **Content Required for Covered Entities (including Upstream Covered Entities and North Sound BH-ASO as a Former Covered Entity).** Other available information that the Upstream Covered Entity is required to include in its notification to an Individual, which may include:

10.2.1 A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.

10.2.2 A description of the types of Unsecured PHI that were involved in the Breach (such as full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information). The actual Unsecured PHI should not be included in the notice.

10.2.3 Any steps affected Individuals should take to protect themselves from potential harm resulting from the Breach.

10.2.4 A brief description of what North Sound BH-ASO is doing to: (a) investigate the Breach; (b) mitigate harm to affected Individuals; and (c) protect against any further Breaches.

10.3 **Other Information.** Other information that is required under the BAA or that is determined by North Sound BH-ASO to be appropriate based on the situation.

11. **Other Notification or Reporting Requirements.** The Privacy Officer will determine whether additional notification or reporting is required, based on, for example, the identity of the affected Individuals, the residence of the affected Individuals, the type of information involved, the location of the information required and other facts surrounding the situation. These additional notification requirements may be based on federal or state law or contractual obligations. For example, a Breach of Unsecured PHI also may require notification under State Law.

12. **Mitigation.** North Sound BH-ASO, to the extent practicable, shall mitigate known harmful effects resulting from Breach of Unsecured PHI (as well as a Security Incident or a Use or Disclosure of PHI in a manner not permitted by HIPAA).

13. **Documentation.** The Privacy Officer will develop and maintain documentation sufficient to meet North Sound BH-ASO's burden of proof that all notifications were made in accordance with this policy and HIPAA. The documentation will be maintained for at least six (6) years. Document retention requirements include:

13.1 **Policies and procedures for Security Incidents, incident response and breach and other notifications.**

13.2 **Analysis determining whether or not a Breach occurred and associated risk assessments.**

13.3 **Determinations that no notice would be required.**

13.4 **Notifications.**

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

14.1 **Policy 2501.00: Privacy and Confidentiality of PHI.**

14.2 **Policy 2502.00: Definitions for Policies Governing PHI.**

14.3 **Policy 2502.00: De-Identified Data and Limited Data Sets.**

14.4 **Policy 2520.00: Training of Workforce.**

14.5 **Policy 2522.00: Uses and Disclosures of PHI.**

14.6 **Policy 2524.00: Verification of Identity and Authority.**

Exhibit A

Decision Tree for Breach Notification under HIPAA