



SALISH BHO

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

Policy Name: BREACH NOTIFICATION REQUIREMENTS **Policy Number:** 5.16

Reference: 45 CFR Parts 164

Effective Date: 03/2016

Revision Date(s):

Reviewed Date: 6/2017; 5/2018

Approved by: SBHO Executive Board

PURPOSE

Breach notification regulations, issued in August 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act by requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. The Salish Behavioral Health Organization (SBHO) in an effort to be compliant with the Privacy Rules of Health Insurance Portability and Accountability Act's (HIPAA) Administrative Simplification provisions, sets out in this policy, rules regarding notification in the case of a breach.

PROCEDURE

Following a discovery of any potential breach, SBHO shall notify state and begin a thorough investigation. If the PHI is determined to have been compromised to the extent of a breach SBHO will notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

A breach shall be treated as discovered the first day on which it is known, or if by exercising reasonable diligence it would have been known to any staff person of SBHO.

1. **Timeliness of notification:** Except when there is a law enforcement delay as described in **6. Law Enforcement Delay** of this procedure, SBHO shall provide the notification without unreasonable delay, and in no case later than 60 calendar days after discovery of the breach. SBHO shall also notify state of a compromise or potential compromise within 1 business day.

2. **Content of the Notification:** All notifications shall include to the extent possible the following:
- a. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
 - b. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
 - c. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
 - d. A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
 - e. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

3. **Methods of notification:** Written notification shall be provided by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail.

The notification may be provided in one or more mailings as information is available.

- a. In the case in which there is insufficient or out of date contact information that precludes written notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided:
 - i. If there are fewer than 10 individuals for whom there is insufficient or out of date contact information the substitute notice may be provided by an alternative form of written notice, telephone, or other means. ii. If there are 10 or more individuals for whom there is insufficient or out of date contact information for 10 or more individuals the substitute notice shall:
 - Be in the form of either a conspicuous posting for a period of 90 days on the home page of the SBHO Web site, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and
 - Include a toll-free phone number that remains active for at least 90 days where an individual can learn whether the individual's unsecured protected health information may be included in the breach.
- b. If SBHO determines that imminent misuse of unsecured protected health information is present and that disclosure to affected individuals is urgent, then SBHO may provide information to individuals by telephone or other means, as appropriate, in addition to all other requirements in this policy.

- c. If the individual is deceased, the written notification shall be made to either the next of kin or personal representative if SBHO has the address of the next of kin or personal representative, unless there is insufficient or out of date contact information for the next of kin or personal representative.
 - d. When a breach of unsecured protected health information involves more than 500 individuals as long as the 500 affected individuals are all residents of the Washington State, SBHO shall notify prominent media outlets serving affected residents, such as local newspapers, in addition to the individual notification as described in this policy.
4. **Notification to the Secretary:** Following the discovery of a breach of unsecured protected health information, SBHO shall notify the Secretary.
- a. If the breach involves 500 or more individuals, SBHO shall provide notice to the Secretary at the same time as notice is provided to the affected individuals, and in the manner specified on the HHS Web site.
 - b. If the breach involves less than 500 individuals, SBHO shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, notify the Secretary of the breaches occurring during the preceding calendar year, in the manner specified on the HHS Web site.
 - c. The HHS Web site address for Instructions to notify the Secretary is:
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html>
5. **Notification by a business associate:** Unless there is a law enforcement delay as described in this policy, SBHO requires that all network Contractors and Subcontractors notify the SBHO HIPAA Officer immediately following the discovery of a breach of unsecured protected health information.
- a. Notification shall include identification of each affected individual, as well as all information described in **2. Content of Notification**.
 - b. Network Contractors and Subcontractors who are covered entities, shall comply with all specifications described in this policy.
6. **Law Enforcement Delay:** If a law enforcement official states to SBHO that a notification, notice or posting required under this policy would impede a criminal investigation or cause damage to national security, SBHO shall:
- a. Delay such notification, notice, or posting for the time period specified by the official, as long as there is a written statement that specifies the time for which a delay is required.
 - b. If the official's communication regarding the criminal investigation or national security threat is made orally, SBHO shall document the statement, include the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the

oral statement, unless a written statement as described above is submitted during that time.

MONITORING

This policy is mandated by contract or 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 Plan Policy.