Salish Behavioral Health
Administrative Services Organization

Policy Name: HIPAA BREACH NOTIFICATION REQUIREMENTS

Policy Number: PS906

Effective Date: 1/1/2020

Revision Dates:

Reviewed Date: 10/15/2020; 3/15/2023

Executive Board Approval Dates: 11/20/2020

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 Administrative Services Organization (SBH-ASO) 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.

POLICY

The SBH-ASO adheres to and requires its Business Associates to comply with HIPAA notice requirements to individuals whose unsecured PHI has been impermissibly accessed, acquired, used, or disclosed as well as the notification requirements to the U.S. Department of Health and Human Services. Additionally, the SBH-ASO complies with the HCA BH-ASO breach notification requirements.

DEFINITIONS

Breach: Any unauthorized acquisition, access, use, or disclosure of protected health information will be considered a breach unless the Covered Entity (CE) or Business Associate (BA) can show the chance of protected health information being compromised is low. The SBH-ASO will use the four factor aids listed to determine whether Protected Health Information (PHI) has been compromised to the extent necessary to be considered and reported as a breach.

1. the identity of the person to whom the PHI was disclosed to

2. if the PHI was acquired or viewed
3. the actual content of the PHI e.g. identifying factors
4. how the risk of disclosure of PHI has been mitigated

For the purposes of this definition “compromises the security or privacy of the protected health information” means that it poses a risk of financial, reputational, or other harm to the individual. A use or disclosure of protected health information that does not include the following identifiers does not compromise the security or privacy of the protected health information:

- Names
- Date of Birth
- Zip Code
- Postal address information, other than town or city, and State
- Telephone numbers
- Fax numbers
- Electronic mail addressee
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account number
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images

Breach excludes:

- Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of SBH-ASO, if such 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 under SBH-ASO HIPAA Privacy and Security policies.

- Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under SBH-ASO HIPAA Privacy and Security policies.

- A disclosure of protected health information where SBH-ASO has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Unsecured protected health information: means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5 on the HHS Web site, which is updated annually. The HHS Web site address for this guidance is: https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html.

PROCEDURE

1. **Discovery of a Breach**: Workforce members who believe an individual's PHI has used or disclosed in any way that compromises the security or privacy of that information will immediately notify the SBH-ASO Privacy Officer, verbally or in writing.

   Following a discovery of any potential breach, the SBH-ASO Privacy Officer shall begin a thorough investigation. If the PHI is determined to have been compromised to the extent of a breach, the SBH-ASO 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 the SBH-ASO.

2. **Breach Investigation**: SBH-ASO Privacy Officer is responsible for the management of the HIPAA breach investigation and coordinating with SBH-ASO and Business Associate staff, as necessary. All SBH-ASO and Business Associate staff who were directly involved in the potential breach are expected to complete the SBH-ASO risk assessment, with the assistance of the SBH-ASO Privacy Officer as needed. As the principal investigator, the SBH-ASO Privacy Officer will be the facilitator of all breach notification processes.

3. **Risk Assessment**: For breach response and notification purposes, a breach is presumed to have occurred unless the SBH-ASO can demonstrate there is a low probability that the PHI has been compromised on, at a minimum , the following risk factors:

   a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. Consider:
      i. Social security or Provider One numbers
      ii. Identifying clinical details, diagnosis, treatment, and medications
      iii. Demographic information
   b. The unauthorized person who used the PHI or to whom the disclosure was made.

i. Does the unauthorized person have obligations to protect the PHI's privacy and security?
ii. Does the unauthorized person have the ability to re-identify the PHI?

c. Whether the PHI was actually acquired or viewed.
   i. Does analysis of a stolen and recovered device show that PHI stored on the device was never accessed?
d. The extent to which the risk to the PHI has been mitigated.
   i. Can the SBH-ASO obtain the unauthorized person's satisfactory assurances that the PHI will not be further used or disclosed and will be destroyed?

The evaluation should consider these factors, or more, in combination to determine the overall probability that PHI has been compromised. The risk assessment should be thorough and completed in good faith, and the conclusions should be reasonable.

Based on the outcome of the risk assessment, SBH-ASO Privacy Officer will determine the need to move forward with breach notification. The Privacy Officer must document the risk assessment and the outcome of the risk assessment process.

4. **Notification – Health Care Authority**: SBH-ASO shall notify the HCA of a compromise within five (5) business days of discovery. At HCA's request SBH-ASO will coordinate its investigation and notifications with HCA and the Office of the State of Washington Chief Information Officer (OCIO), as applicable. SBH-ASO shall notify HCA in writing within two (2) business days of determining notification must be sent to non-Medicaid individuals. At HCA's request SBH-ASO will provide draft Individual notification to HCA at least five (5) business days prior to notification and allow HCA an opportunity to review and comment on the notifications. If the SBH-ASO does not have full details regarding the potential breach, it will report what is available, and then provided full details within fifteen (15) business days of discovery.

5. **Notification to Affected Individual(s):** If it is determined that breach notification must be sent to affected individuals, a standard breach notification letter (as modified for the specific breach) will be sent to all affected individuals. The SBH-ASO also has the discretion to provide notification following an impermissible use or disclosure of PHI without performing a risk assessment, if deemed appropriate.
   a. **Content of Notification**: Notice to affected individuals shall be written in plain language and must contain the following information:
      i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

ii. 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);
iii. Any steps individuals should take to protect themselves from potential harm resulting from the breach;
iv. 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
v. 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.

b. **Timeliness of notification:** Except when there is a law enforcement delay as described in section 8 below, Law Enforcement Delay, SBH-ASO shall provide the notification to the affected individual(s) without unreasonable delay, and in no case later than 60 calendar days after discovery of the breach.
c. **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.
    i. 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:
        1. 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.
        2. 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 SBH-ASO 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.
    ii. If SBH-ASO determines that imminent misuse of unsecured protected health information is present and that disclosure to affected individuals is urgent, then SBH-ASO may provide information to individuals by telephone or other means, as

appropriate, in addition to all other requirements in this policy.

iii. If the individual is deceased, the written notification shall be made to either the next of kin or personal representative if SBH-ASO 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.

iv. 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, SBH-ASO shall notify prominent media outlets serving affected residents, such as local newspapers, in addition to the individual notification as described in this policy.

6. **Notification – U.S. Department of Health and Human Services**: Following the discovery of a breach of unsecured protected health information, SBH-ASO shall notify the Secretary.
    a. If the breach involves 500 or more individuals, SBH-ASO 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, SBH-ASO 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: https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html.

7. **Notification – by a Business Associate (BA)**: Unless there is a law enforcement delay as described in this policy, the SBH-ASO requires that all network Contractors and Subcontractors notify the SBH-ASO Privacy Officer in writing of a breach within five (5) business days of discovery, as well as two (2) business days after determining notifications must be sent to individuals. Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been accessed, acquired, used or disclosed during the breach. The BA shall provide SBH-ASO with any other available information that is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, the BA will be responsible for notifying affected individuals, HHS, and HCA.

8. **Law Enforcement Delay**: If a law enforcement official states to SBH-ASO that a notification, notice or posting required under this policy would impede a criminal investigation or cause damage to national security, SBH-ASO 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, SBH-ASO 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 of the above aforementioned Procedures is consistent with the SBH-ASO Provider Network Selection and Management Monitoring Policy.