



PENINSULA RSN

HIPAA AND MEDICAID COMPLIANCE POLICIES AND PROCEDURES

Policy Name: HIPAA BREACH NOTIFICATION REQUIREMENTS	Policy Number: 5.16
Reference: 45 CFR Parts 164	
Effective Date: 09/23/2009	
Revision Date(s):	
Approved by: PRSN Executive Board	

PURPOSE

Interim final 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 Peninsula Regional Support Network (PRSN), in an effort to be compliant with the Privacy Rules of Health Insurance Accountability and Portability Act's (HIPAA) Administrative Simplification provisions, sets out in this policy, rules regarding notification in the case of a breach.

DEFINITIONS

Breach: The unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected information.

For the purposes of this definition "compromises the security or privacy of the protected health information" means that it poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of protected health information that includes any of the following identifiers compromises 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 addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;

- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- 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 PRSN, 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 PRSN 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 PRSN HIPAA Privacy and Security policies.
- A disclosure of protected health information where PRSN 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:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html>

PROCEDURE

Following a discovery, PRSN shall 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 PRSN.

1. **Timeliness of notification:** Except when there is a law enforcement delay as described in **6. Law Enforcement Delay** of this procedure, PRSN shall provide the

notification without unreasonable delay, and in no case later than 60 calendar days after discovery of the breach.

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 PRSN 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 PRSN determines that imminent misuse of unsecured protected health information is present and that disclosure to affected individuals is urgent, then PRSN 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 PRSN 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, PRSN 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 U.S. Department of Health and Human Services (HHS)

Secretary: Following the discovery of a breach of unsecured protected health information, PRSN shall notify the Secretary.

- a. If the breach involves 500 or more individuals, PRSN 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, PRSN 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, PRSN requires that all network Contractors and Subcontractors the PRSN 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, in addition to notifying the PRSN.

6. Law Enforcement Delay: If a law enforcement official states to PRSN that a notification, notice or posting required under this policy would impede a criminal investigation or cause damage to national security, PRSN 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, PRSN 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.

7. Burden of Proof: Any PRSN staff member; or workforce member of a Network Contractor or Subcontractor, or Business Associate who becomes aware of an incident that may constitute a breach as defined in this policy shall immediately inform the HIPAA Privacy or Security Officer.

- a. The HIPAA Privacy or Security Officer, or individual designated by the HIPAA Privacy or Security Officer shall conduct an investigation and analysis to determine whether the incident constitutes a breach.
 - i. The person conducting the investigation shall document a description of the incident, and any analyses involved in determining whether or not there was a breach using the Breach Determination and Risk Assessment Tool.
 - ii. If it is determined that a breach did occur, all actions taken to notify individuals as required in this policy shall be documented and retained.

MONITORING

This policy is mandated by contract or statute.

1. This policy will be monitored through use of PRSN:
 - Annual PRSN 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 PRSN approval. Reference PRSN Corrective Action Plan Policy.