WASHINGTON STATE UNIVERSITY
Compliance and Risk Management

Protected Health Care Information (PHI) Incident Response

Immediately Report the Incident

Immediately report the incident to the following people:
- Your supervisor or manager;
- The applicable Health Care Component (HCC) Privacy Officer and HCC Security Officer;
- The Pullman Security Operations Center; Email abuse@wsu.edu; Tel: 509-335-0404;
- The WSU HIPAA Privacy and Security Officer. The WSU Chief Information Security Officer (CISO) serves as the WSU HIPAA Security Officer; Email: ciso@wsu.edu; Tel: 509-335-0690; The WSU System Privacy Officer; Email: smakamson@wsu.edu; Tel: 509-335-8864;
- The WSU Chief Compliance and Risk Officer (CCRO); Email: compliance.risk@wsu.edu; Tel: 509-335-5524;

Determining if there has been an incident

The following will be considered by the **WSU Chief Compliance and Risk Officer (CCRO)**, and the **WSU Chief Information Security Officer (CISO)** when determining if there has been an incident:

- Was it an unintentional acquisition, access or use of PHI by workforce members or a business associate who is acting in good faith within the parameters of their position?
- Was it an inadvertent disclosure of PHI between two persons who are both authorized to access PHI?
- Was it a disclosure of PHI to an unauthorized person, who WSU believes, in good faith, would not reasonably have been able to retain such information?
- Was it a situation where a formal risk assessment based on required factors demonstrates that there is a low probability that the PHI has been compromised?

Create a report for the incident

Workforce members are to report any incidents related to unsecured PHI by telephone and secure electronic means (e.g., internal WSU Office365 e-mail services). Shared email services (e.g., Gmail) are not to be used to report any incidents.

If Known:
- A brief description of what happened, including the dates and times;
- Who used the PHI and how was the information disclosed;
- A description of the types and amount of PHI involved in the breach;
- If the PHI was secured by encryption, destruction or other means;
- If any steps were taken to mitigate an impermissible use or disclosure; and
- The recipient of the data including contact information (e.g., name, telephone number, e-mail address)

Failure to report a suspected incident may result in disciplinary action up to and including termination.

How does WSU determine if there has been a breach based on the incident?

WSU's HIPAA Privacy and Security Officer, the Assistant Director of Health Sciences Compliance, and the affected HCC promptly investigate any security and/or privacy incident. Investigations follow the Incident Response Process established in BPPM 87.55.

WSU considers the following to determine if there has been a breach of PHI
- Whether the unauthorized or impermissible acquisition, access, use, or disclosure involved PHI.
- Whether WSU can demonstrate, based on the following factors, a low probability that the PHI has been compromised:
  - The nature and extent of the information involved;
  - Not authorized by the patient or client;
  - Not for treatment, payment, or health care operations;
  - Not otherwise allowed by law.
- WSU must maintain investigation records and final determinations and/or conclusions related to the unauthorized use, access, or disclosure. Documentation of the findings and final actions from the investigation must be retained for ten years as part of WSU's health client files privacy records. (See the All-University Records Retention Schedule - Student Records table in BPPM 90.01.)
- If it is determined that a violation has occurred, WSU must follow the corrective and disciplinary actions policy (BPPM 60.50) and document the violation in the workforce member file.

What happens when WSU determines there has been a breach?

If WSU determines that a breach of unsecured PHI has occurred WSU must notify the affected individual(s) and appropriate government agencies and/or organizations in accordance with the applicable law (e.g., HIPAA, RCW 42.56.590).
For HIPAA breaches, WSU must provide notification to the:
- Affected individuals; and
- U.S. Department of Health and Human Services (HHS);
- and Applicable media (if required).

WSU's HIPAA Privacy and Security Officer must approve and direct any notice provided pursuant to this policy.

When do individuals have to be notified of a breach and what information needs to be included?

When a breach of PHI has occurred, WSU must notify the affected individual(s) without unreasonable delay and in no case later than 60 days after the breach is discovered, unless a shorter period is required by law.

The notice must be in writing and written in plain language, and must include, to the extent known:
- A brief description of the incident (e.g., the date of the breach and the date it was discovered);
- A description of the types of information involved (e.g., whether the breach involved names, social security numbers, birth dates, addresses, diagnoses);
- Any steps the affected individual(s) should take to protect them-self from potential harm resulting from the breach;
- A brief description of the steps WSU is taking to investigate, mitigate, and protect against further harm or breaches; and
- Contact information for WSU (or business associate, as applicable) (e.g., toll-free telephone number, e-mail address, website, or postal address).

What if contact information is insufficient or out-of-date?

If WSU has insufficient or out-of-date contact information that precludes written notification to the individual, WSU must provide a substitute form of notice that is reasonably calculated to reach the individual. **Details on contact process in WSU BPPM 88.05.**

When does WSU notify the local media?

For a breach of unsecured protected health information involving more than 500 residents of a particular state or jurisdiction, WSU must, following the discovery of the breach, notify prominent media outlets serving the state or jurisdiction. The notification must be made without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. The notification must contain the information required for individual notices as described above.

When does WSU notify the Washington State Attorney General?

The Washington State Attorney General must be notified when a privacy breach involves more than 500 Washington state residents, as required by RCW 42.56.590