WASHINGTON STATE UNIVERSITY
Compliance and Risk Management

Protected Health Care Information(PHI) Breach Response

Step 1: Determine if there has been a breach

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?

Step 2: Determine if the acquisition resulted in further disclosure

If there has been a breach proceed to step 3. If not, this is an exception under WSU BPPM 88.05.

Step 3: Immediately report the potential breach

Report to the following people:
Your supervisor or manager, the applicable Health Care Component (HCC) Privacy Officer and HCC Security Officer, and the Pullman Security Operations Center; email: abuse@wsu.edu; tel: 509-335-0404.

Also report to the following administrators:
The WSU Chief Information Security Officer (CISO) serves as
The WSU HIPAA Privacy and Security Officer; email: ciso@wsu.edu; tel: 509-335-1642,
The WSU Chief Compliance and Risk Officer (CCRO); email: compliance.risk@wsu.edu; tel: 509-335-5523.

Step 4: Create a report for the potential breach

Workforce members are to report any suspected breach of unsecured PHI by telephone and secure electronic means (e.g., internal WSU Office365 e-mail services). Shared e-mail services (e.g., gmail) are not to be used to report suspected breaches of unsecured PHI.

If known, include in your report: a brief description of what happened, include 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 breach may result in disciplinary action up to and including termination.

WASHINGTON STATE UNIVERSITY
Compliance and Risk Management

Protected Health Care Information(PHI) Breach Response

Step 5: Investigation

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 WSU BPPM 87.55.

If WSU determines that a breach of unsecured PHI has occurred WSU must notify the affected individual(s) and appropriate government agencies in accordance with the applicable law (e.g., HIPAA, RCW 42.56.590).

For HIPAA breaches, WSU must provide notification to the affected individuals, U.S. Department of Health and Human Services, applicable media (if required). WSU's HIPAA Privacy and Security Officer must approve and direct any notice provided pursuant to WSU BPPM 88.05.

Step 6: Notification

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 plain writing and written in plain language and must include, if known: A brief description of the incident, A description of the types of information involved, Any steps the affected individual(s) should take to protect them-self from potential harm resulting from the breaches, and contact information for WSU.

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.

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.

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

Questions? Contact Us at smakamson@wsu.edu or bethany.loomis@wsu.edu