Protected Health Care Information (PHI) Incident Response

01 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 Privacy and Security Officer; email: ciso@wsu.edu; Tel: 509-335-0690;
- The WSU Chief Compliance and Risk Officer (CCRO); email: compliance.risk@wsu.edu; Tel: 509-335-5524

02 Write a Report

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)

03 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.

The following will be considered 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?

04 Notification

WSU must notify affected individual(s) within 60 days after the breach is discovered.

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. Details on the contact process in WSU BPPM 88.05.