Protected Health Care Information Breach Response

**PURPOSE**
The purpose of this section (BPPM 88.05) is to identify the procedures for responding to potential breaches of protected health information (PHI) and/or health care information that qualifies as personal information as defined by applicable federal and state laws. (See also the U.S. Department of Education and U.S. Department of Health and Human Services' Joint Guidance on the Application of FERPA and HIPAA to Student Health Records.)

The term "PHI" is used throughout this policy to also include health care information as defined by Washington law. (See RCW 70.02.010.)

**POLICY**
The WSU system's Health Care Components (HCC), as defined in WSU Executive Policy Manual EP40, have established the following procedures, in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (45 CFR 164, Subpart D) and RCW 42.56.590.

**HCC Privacy and Security Officers**
Each HCC has an assigned privacy officer and security officer. The functions are often provided by the same WSU administrator. For further information, see Privacy Officers.

**Definitions**
Definitions applicable to both information privacy and information security policies and procedures are provided in BPPM 87.01, unless a specific definition in HIPAA or Washington's Uniform Health Care Information Act, RCW 70.02, is applicable.

**PROCEDURES**

**Exclusions**
Each incident is assessed for a breach unless it meets any of the exclusions listed below, according to the breach definition in 45 CFR 164.402.

The privacy officer for the applicable HCC determines if the action qualifies as an exclusion and maintains a secure database with the incident information. If the privacy officer determines that the incident does not meet any of the following exclusions, the HCC proceeds to report the breach.

- 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, as long as the acquisition does not result in any further use or disclosure;
Protected Health Care Information Breach Response

Exclusions (cont.)

- An inadvertent disclosure of PHI between two persons who are both authorized to access PHI, provided the information received as a result of such disclosure is not further impermissibly used or disclosed;

- A disclosure of PHI to an unauthorized person, who WSU believes, in good faith, would not reasonably have been able to retain such information; or

- A situation where a formal risk assessment based on required factors demonstrates that there is a low probability that the PHI has been compromised.

Reporting Potential Breaches

The following procedures apply to the reporting of potential breaches (e.g., unauthorized access, use, or disclosure) of PHI:

- Workforce members who learn that a potential breach of PHI may have occurred must report immediately after discovery to:
  - Their supervisor or manager;
  - The applicable HCC Privacy Officer and HCC Security Officer (see Privacy Officers); and
  - The Pullman Security Operations Center; e-mail abuse@wsu.edu; telephone 509-335-0404.

- Workforce members are to report any suspected breach of unsecured PHI to all the following administrators immediately after learning of the incident:
  - The WSU HIPAA Privacy and Security Officer. The WSU Chief Information Security Officer (CISO) serves as the WSU HIPAA Privacy and Security Officer; e-mail ciso@wsu.edu; telephone 509-335-1642.
  - The WSU Chief Compliance and Risk Officer (CCRO); e-mail compliance.risk@wsu.edu; telephone 509-335-5524.
Protected Health Care Information Breach Response

Reporting Potential Breaches (cont.)

- 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 email services (e.g., gmail) are not to be used to report suspected breaches of unsecured PHI.

- The report of a potential breach is to include all of the following information, 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 breach may result in disciplinary action up to and including termination.

Assessing and Investigating Potential Breaches

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.

Investigators also refer to BPPM 87.01 and 87.55 for data definitions, usage, and responsibilities.

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.
Protected Health Care Information Breach Response

Assessing and Investigating Potential Breaches (cont.)

• 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;
  ○ The unauthorized person who used or received the information;
  ○ Whether the information was actually acquired or view; and
  ○ The extent to which the risk of the information has been mitigated.

• WSU also determines if the acquisition, access, use, or disclosure of PHI was:
  ○ 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.

Breach Notification

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).
Protected Health Care Information Breach Response

Breach Notification (cont.)  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.

Notice to Individuals  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.

Contents of the Notice  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, birthdates, addresses, diagnoses);

• Any steps the affected individual(s) should take to protect themself 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).

Method of Notification  WSU must notify the affected individual by first class mail to the individual's last known address. Notice may be sent by e-mail if the patient has agreed to accept notification through electronic means.
Protected Health Care Information Breach Response

Substitute Notice
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.

Fewer Than Ten Individuals
Where there is insufficient or out-of-date contact information for fewer than ten individuals, substitute notice may be provided by an alternative form of written notice, telephone, or other means.

Ten or More Individuals
Where there is insufficient or out-of-date contact information for ten or more individuals, substitute notice must:

- Be in the form of either a:
  - Conspicuous posting for a period of 90 days on the home page of the website of the covered entity involved; 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.

Notice to HHS
If WSU determines that a breach of protected health information has occurred, WSU must also notify HHS of the breach as follows:

500 or More Affected Individuals
For breaches of unsecured PHI involving 500 or more individuals, WSU must notify HHS of the breach simultaneously with the notice to the individuals and in the manner specified on the HHS website.

Fewer Than 500 Affected Individuals
For breaches of unsecured protected health information involving fewer than 500 individuals, WSU may report the breach immediately to HHS in the manner specified on the HHS website.

If the WSU HIPAA Privacy and Security Officer does not immediately report the breach to HHS, they must maintain a log or other documentation of such breach and, not later than 60 days after the end of each calendar year, provide the notification to HHS in the manner specified on the HHS website.
Protected Health Care Information Breach Response

Notice to 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 in Contents of the Notice.

Notice to 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.

REFERENCES

Privacy Officers A list of WSU privacy officers, are available on the Compliance and Civil Rights (CCR) website.

HIPAA Guidance Guidance and templates for developing departmental HIPAA policies, risk assessments, and business associate agreements are available at the CCR website.