Role-Based Access to Protected Health Information

POLICY

To comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) 45 CFR 164.312(a)(1) and (a)(2) and the Revised Code of Washington (RCW) 70.02.150, Washington State University (WSU) implements reasonable and appropriate measures to:

• Limit access to protected health information (PHI) only to those persons or automated processes that have been granted access rights based on their required functions (i.e., the minimum necessary PHI for employees to perform their jobs); and

• Prevent those who have not been approved from obtaining access to PHI.

APPLICABILITY

This policy applies to:

• WSU health care components (HCCs), as identified in WSU's Executive Policy Manual EP40, that access, create, use, disclose or maintain PHI) in electronic (ePHI) or paper format; and

• Users requiring access to and administering PHI.

PROCEDURES

Authorized Access

Appropriate WSU employees and business associates who are authorized to access PHI may access and work with the associated PHI or ePHI. Access is based on the necessary roles of the personnel and the legitimate need based on their current roles, responsibilities, and minimum PHI necessary to perform these functions.

Security

WSU employees or visitors who are not authorized to access PHI or ePHI, but who work in or visit locations where PHI might be accessible, are to be supervised, escorted, or otherwise denied access. PHI must be appropriately safeguarded at all times according to all applicable policies, laws, and regulations.

Access Control

The WSU HCCs and their information systems are responsible for granting access to the appropriate personnel. The HCCs are also responsible for creating, modifying, or terminating a user's ability to access PHI or ePHI based on the specific policy requirements in BPPM 87.05.
Role-Based Access to Protected Health Information

User Accounts

A user account, which includes a unique user identification (ID), is established and maintained for each user of an information system to control authentication and access rights.

The HCC must have a departmental policy to establish setup requirements, rights, identification, and authentication based on the employee responsibilities. This includes access rights that determine what data sets the user may view, update, delete, create, copy, etc.

The departmental policy must outline the procedures for system management and all standardized identity, authentication, and access requirements, in accordance with EP8 and BPPM 87.05. Such requirements include:

- Data storage;
- Termination, modifying access, and control logs for documentation of access approvals and reviews, user account creations, modifications, and deletions;
- Emergency access for accessing PHI in an emergency/natural disaster;
- Logging off/locking devices and automated security features;
- Employee training; and
- Encryption and decryption for all institutional data covered by federal or state standards, laws, regulations, or contractual agreements, in accordance with EP8.

REFERENCES

WSU data policy statements are referenced in EP8.

WSU information security requirements are available in EP37.

Information system account and access management and review policy requirements are available in BPPM 87.05.