

Summary of Policy on Information Security and HIPAA Privacy Education/Training Requirements

Institutional policies require UW Medicine¹ workforce members to be educated about privacy, confidentiality and security of protected health information (PHI). The term “workforce member” refers to faculty, employees, trainees (e.g. students, residents, and fellows), volunteers, and other persons who perform work for UW Medicine, and whose work conduct is under UW Medicine’s direct control regardless of whether or not the workforce member is paid by UW Medicine. Education occurs in the following ways:

Execution of UW Medicine Privacy, Confidentiality, and Information Security Agreement

To satisfy UW Medicine Information Security Program requirements, at the time of hire and at each performance evaluation or credentialing, all workforce members, including those in the School of Medicine, must read and sign the *UW Medicine Privacy, Confidentiality, and Information Security Agreement*. By signing this document, individuals accept their responsibilities as users of University and UW Medicine computing resources and data, commit to complying with institutional policies and rules, and acknowledge that there are sanctions for noncompliance. Certain students and other individuals involved only in observational experiences must, instead, read and sign the *UW Medicine Application and Agreement for Observational Activities*.

HIPAA Privacy Training

Depending on job function, education and training may occur during new employee orientation and/or department orientation and may require completion of a Web-based training course. For the School of Medicine, the privacy training requirement applies only to workforce members whose job function² requires the use or disclosure of PHI for, or on behalf of, UW Medicine.

Workforce members covered under this policy with a duration of employment or study of 30 calendar days or longer are trained within 30 days of hire on policies and procedures related to the access, use, and handling of PHI. Students with direct care and/or unsupervised patient contact, and students or others involved only in observational activities may meet the training requirement by showing proof of training at another academic medical center.

Workforce members covered under this policy with duration of employment or study less than 30 calendar days may meet the training requirement by completing a UW Medicine “self-study” module or providing proof of training at another institution. Students and other individuals involved in observational activities must only complete the *UW Medicine Application and Agreement for Observational Activities*.

The description outlined above represents a summary of the policy. The full policy, training requirements, general procedures, and forms are set forth in privacy policy, *PP-04 Privacy, Confidentiality, & Information Security Training*, which is available at: depts.washington.edu/comply/privacy.shtml

Enforcement of Institutional Requirements

UW Medicine policy requires that appropriate sanctions be applied, without regard to role or position, to workforce members, including those in the School of Medicine covered under this policy, who fail to comply with institutional policies and established procedures related to privacy, confidentiality, and information security. Non-compliance with the educational requirements summarized above is considered a failure to comply with institutional policy, which constitutes a Level 3 violation, subject to sanctions up to and including termination (see next section for further information).

The policy, a general description of policy violations and possible sanctions, and general procedures by level of policy violation are set forth in privacy policy, *PP-06 Sanctions for the Failure to Follow Applicable Privacy and/or Information Security Policy or for a Breach of Patient Confidentiality or Information Security*, which is available at: depts.washington.edu/comply/privacy.shtml

Sanctions for Noncompliance

Individuals who have not signed the “security” or “observational activities” agreement, and/or completed the required HIPAA privacy training within 30 days of hire or registration in the training database are subject to sanctions. Sanctions for a Level 3 policy violation may include denial of access to information, retraining, and a range of personnel actions up to and including termination of employment or professional services.

The person responsible for initiating sanctions for noncompliance is based on the workforce member’s constituency and reportage within the organization. UW Medicine officials vested with authority to determine sanctions for noncompliance include, but are not limited to, department chairs and administrators, medical center directors and administrators, and GME program directors. Sanctions initiated by UW Medicine officials are coordinated with appropriate institutional offices such as Human Resources, Graduate Medical Education and Academic Affairs.

Information concerning the range of possible sanctions and designated authority is set forth in privacy policy, *PP-06 Sanctions for the Failure to Follow Applicable Privacy and/or Information Security Policy or for a Breach of Patient Confidentiality or Information Security*, which is available at: depts.washington.edu/comply/privacy.shtml

-
1. The term “UW Medicine” includes the following entities: University of Washington Medical Center and Clinics; Harborview Medical Center and Clinics; UW Medicine Neighborhood Clinics (University of Washington Physicians Network); UW Physicians Sports Medicine Clinic; UW Medicine Eastside Specialty Center; Hall Health Primary Care Center; University of Washington Physicians; as well as certain services and activities that support UW Medicine that are performed by non-healthcare components of the University of Washington as defined within Privacy Policy PP-01 Use & Disclosure of Protected Health Information – Organizational Requirements. UW School of Medicine is subject to the UW Medicine Information Security Program.
 2. Examples of SOM non-health care support functions that might require the use or disclosure of protected health information include: Administrative Support relating to treatment, payment, or healthcare operations; Compliance; Development; Document Retention Services; Environmental and Workplace Safety; Information Systems Management; Investigations involving clinical care or scholarly integrity; Medical Staff Peer Review; Planning; Personnel Services; Risk Management; and, Telemedicine Support Services. Refer to Privacy Policy PP-01 for additional information.

Roles and Responsibilities: Education/Training Requirements

Responsible Party: Department of Hire - Administrator or Designee

Responsibility: Follow the policies and procedures outlined in "PP-04 Privacy, Confidentiality, & Information Security Training" as summarized below:

- Obtain a signature from each new workforce member on form "UW Medicine Privacy, Confidentiality, and Information Security Agreement."
- Obtain the signature of any individual engaging in an observational experience on form "UW Medicine Application and Agreement for Observational Activities."
 - Retain signed form in either workforce member's personnel file or, for observers, in a department file.
 - **Note:** The academic office of each school (dentistry, medicine, nursing, pharmacy) obtains the signature of the student prior to matriculation and retains the form.
- Determine, considering duration of employment/service/study, general and job-specific privacy training requirements.
- Obtain signature on appropriate form of workforce member who has the option to provide proof of training at another facility or complete the UW self-study module.
- Complete, if required, "Request Form to Register Workforce Member for HIPAA Training" and send by email to your entity's privacy office. HIPAA Online Training Contacts are listed at: depts.washington.edu/comply/training_hipaa.shtml
 - Determine curriculum track for Web-based training based on job function.
- Provide workforce member with curriculum track, and logon/training instructions received from UW Medicine Compliance.
 - **Note:** The academic office of each school (dentistry, medicine, nursing, pharmacy), registers students for online privacy training prior to matriculation and retains record of completion.
 - **Note:** The GME Office registers residents/fellows for online privacy training; the department is responsible for ensuring that training is completed.
- Provide guidance and technical assistance to individual user of online training course.
- Use monthly online vendor report entitled, "HCCA HIPAA Training Completion Report" and "Mid-Month Incomplete Report" to monitor status of workforce member training.
- Ensure individual's training is completed within 30 days of hire or registration in training course.

Responsible Party: UW Medicine Entity – Site Coordinator

Responsibility:

- Receive email request from department contact for individual registration in Web-based training course.
- Enter workforce member in training course database.
- Send user logon and letter of instruction, which states the 30-day completion requirement, to department contact.
- Provide policy guidance and technical assistance to department administrator/contact.

Responsible Party: UW Medicine Compliance

Responsibility:

- Distribute the following monthly tracking reports to department contacts:
 - HCCS HIPAA Training Completion Reports (at the beginning of each month)
 - Incomplete Report (mid-month status report)
- Provide clarification of policy and guidance to departments as part of process improvement strategies.

Roles and Responsibilities: Compliance with Education/Training Requirements

Sanctions

Responsible Party: Department of Hire - Administrator or Designee

Responsibility:

- Identify workforce members who are not in compliance with privacy training policy:
 - Identify workforce members who have not shown proof of training at another facility or completed the “self-study” module within 30 days of hire.
 - Identify workforce members who have not completed online training within 30 days of registration in the training course database.
- Follow policies and procedures outlined in PP-06 “Sanctions for the Failure to Follow Applicable Privacy and/or Information Security Policy or for a Breach of Patient Confidentiality or Information Security” to:
 - Notify Department Chair and/or Medical Director of any faculty member who has not completed the required level of training within the designated timeframe.
 - Notify Department Chair, Medical Director, and/or Program Director of a student, resident, or fellow who has not completed the required level of training within the designated timeframe.
 - Notify supervisor/manager of staff or other workforce member who has not completed the required level of training within the designated timeframe.
 - Contact workforce member to outline timeframe/plan for completion of training.

Responsible Party: Department of Hire - Department Chair and/org Medical Director

Responsibility:

- Determine course of corrective action involving faculty in consultation with SOM Human Resources.
- Notify UW Medicine Compliance of corrective action plan.

Responsible Party: Department of Hire - Department Chair, Medical Director and/or Program Director

Responsibility:

- Determine course of corrective action for students, residents, and fellows in consultation with GME Office, or with the Vice Dean for Academic Affairs.
- Notify UW Medicine Compliance of corrective action plan.

Responsible Party: Department of Hire - Department Administrator or Designee

Responsibility:

- Determine course of corrective action for staff or other workforce member in consultation with supervisor and University Health Sciences Human Resources.
- Notify UW Medicine Compliance of corrective action plan.

Responsible Party: UW Medicine Compliance

Responsibility:

- Record policy violation in Privacy Event Database.
- Report, on a regular basis, Privacy Event data to the UW Medicine Board Compliance Committee.

Policy References:

- PP-01 Use & Disclosure of Protected Health Information – Organizational Requirements
- PP-04 Privacy, Confidentiality, & Information Security Training
- PP-06 Sanctions for the Failure to Follow Applicable Privacy and/or Information Security Policy or for a Breach of Patient Confidentiality or Information Security
- SEC-01 Information Security Policy