

Policy Level: UW Medicine Compliance, UW Medicine-Wide  
Policy Title: PP-04 Privacy, Confidentiality, & Information Security Training  
Policy Number: PP-04  
Date Established: June 24, 2002  
Date Revised: April, 2, 2003; August, 23, 2004; October 23, 2006; May 8, 2008;  
July 10, 2008; June 14, 2011  
Date of Last Cyclic Review:

---

### **Purpose**

Due to its personal and sensitive nature patient information is accorded special protections under law. UW Medicine is required to train all workforce members on its policies and procedures about protected health information (PHI). Training must be done for all members of the workforce, as necessary and appropriate to carry out their functions within UW Medicine.

### **Definitions**

- System Operators: Individuals within UW Medicine who are accountable for the operational decisions about the use and management of a computing system.
- System Owner: Individual(s) within UW Medicine who are accountable for the management and use of one or more electronic information systems, electronic databases, or electronic applications that are associated with UW Medicine. System Owners might include members of the UW Medicine professional staff, department heads, faculty members, contracted employees, or students.
- Workforce: Faculty, employees, trainees, 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 they are paid by UW Medicine.

### **Policy**

All members of UW Medicine's workforce must be trained to understand their responsibilities related to protecting the confidentiality and security of patient information. Each member of UW Medicine's workforce is required to sign the "UW Medicine Privacy, Confidentiality, and Information Security Agreement". Each time a material change is made to a UW Medicine Privacy Policy; UW Medicine workforce members whose functions are affected by the change are trained.

#### **I. Workforce Requirement: Privacy, Confidentiality, and Information Security Agreement**

At the time of hire and at each performance evaluation<sup>1</sup> or credentialing, Managers are to ensure that workforce members sign the “UW Medicine Privacy, Confidentiality, and Information Security Agreement.” (Attachment A) The signed UW Medicine Privacy, Confidentiality, and Information Security Agreement must be filed into the entity’s appropriate personnel or academic record.

**II. Workforce Privacy Awareness and Training Requirements**

Managers are to ensure that all members of UW Medicine’s workforce receive privacy training:

A) New workforce members:

- 1) New employee orientation addresses general components for workforce compliance with UW Medicine Privacy and Information Security policies.
- 2) Trained within 30 days of hire regarding essential information that all members of the UW Medicine workforce must know related to the access, use, and handling of PHI (for example, during new employee orientation or UW Medicine on-line HIPAA training);
- 3) Trained during department orientation on all policies and procedures respecting PHI as it relates to department functions within 60 days;

AND

- 4) Trained during department orientation on all policies and procedures respecting PHI as is necessary to address patient information privacy and security functions necessary to job performance.

B) For all workforce members whose job responsibilities are impacted because of new or changed policy or procedure within 30 days of the effective date of the change.

C) If an existing workforce member’s job functions change within UW Medicine, job specific training on privacy and information security is conducted during orientation to the workforce member’s new responsibilities, or within the first 30 days of the workforce member’s first day to a new position.

---

<sup>1</sup> WAC 357-37-030 - When and how often must performance feedback be provided to an employee through the formal evaluation process?

Employers must provide feedback and formally evaluate the performance of:

(1) A probationary employee or a permanent employee serving a trial service period or transition review period before the employee attains permanent status in the position; and

(2) A permanent employee on an annual basis.

- D) Temporary Workforce complete HIPAA training per the following guidelines:
- 1) If employment at UW Medicine is 30 calendar days or more, the individual is required to complete the UW Medicine on-line HIPAA training and sign a “UW Medicine Privacy, Confidentiality, and Information Security Agreement”.
  - 2) If employment at UW Medicine is less than 30 calendar days, the individual is required to review and sign a [UW Medicine Privacy, Confidentiality, and Information Security Agreement](#); and provide proof of training of comparable quality at another facility and review/sign the summary HIPAA training document (Attachment C) or must complete the UW Medicine HIPAA Temporary Workforce Member/Student Self Study Manual (Attachment B). The manager or other individual who is responsible for the temporary workforce member maintains a copy of the signed documentation.
- E) Fellows, Residents, and Students: Direct Patient Care Activities  
Fellows, Residents, and Students whose role includes direct care and/or any unsupervised contact with patients are required to:
- 1). Sign a UW Medicine Privacy, Confidentiality, and Information Security Agreement;
  - 2). Be compliant with UW Medicine entity’s identification badge policies and procedures;
  - 3). Be compliant with UW Medicine entity’s immunization policies and procedures; and
  - 4). Complete HIPAA training per the following guidelines:
    - a). If the duration of the training or other official learning activities at UW Medicine is 30 calendar days or more, the individual is required to complete the UW Medicine on-line HIPAA training. Fellows, Residents, and Students on rotation at a UW Medicine Entity that have received HIPAA training from another Academic Medical Center or reviewed program (Madigan Army Medical Center, Swedish Medical Center, Veterans Administration Health Care System (VA), or Virginia Mason Medical Center) can use the “HIPAA TRAINING CERTIFICATION” (Attachment C) to meet the UW Medicine Privacy and Security training requirement.
    - b). If the duration of the training or other official learning activities at UW Medicine is less than 30 calendar days, the individual is required to have received Privacy and Security HIPAA training of comparable quality at another facility. Such individuals must submit a copy of the certificate of training and read and sign a copy of the “HIPAA TRAINING CERTIFICATION” (Attachment C). The manager or other individual who is responsible for the trainee or visitor maintains a copy of the signed document. If the student has not received previous HIPAA training, the student must complete the “UW Medicine

Temporary Workforce Member/Student HIPAA Self Study” (Attachment B.)

F) Students in a Training Program

A contract with the school must be in place before the student may begin the training program.

Students in a training program at UW Medicine must complete the following steps:

- Sign a “UW Medicine Privacy, Confidentiality, and Information Security Agreement.” (Attachment A).
- Obtain an ID badge for the UW Medicine entity where the training program is to occur.
- Comply with the UW Medicine entity’s immunization policies and procedures where the training program is to occur.
- Complete the training as outlined in section II. E) “Fellows, Residents, and Students: Direct Patient Care Activities” of this policy.

G) Students and Other Individuals: No direct Patient Care Activities

Students and other individuals involved in observational and educational activities are required to:

- 1). Submit the “Application and Agreement for Observational Activities” form with an immunization history to the contact information in the “Return this completed form to:” box on the bottom of the back page.
- 2). If the application is approved, Section C of the “Application and Agreement for Observational Activities” form must be completed on or before the first day of the observational experience. This includes providing the student or visitor with a temporary ID badge for the UW Medicine entity where the observational experience is to occur.
- 3). Complete HIPAA training per the following guidelines:

If the duration of the training or other official learning or observational activities at UW Medicine is 30 calendar days or more, the individual is required to complete the UW Medicine on-line HIPAA training. Students on rotation at a UW Medicine Entity that have received HIPAA training from another Academic Medical Center can use the “HIPAA TRAINING CERTIFICATION” (Attachment C) to meet the UW Medicine on-line HIPAA training requirement;
- 4). Each patient must be informed of the visitor’s presence and be given the opportunity to verbally consent or object;
- 5). Students or visitors who are participating in an observational experience may not provide any direct care to patients, and may not have any unsupervised contact with patients; and

- 6). The manager, preceptor or other employee host is responsible for ensuring that the student/visitor follows the above policies.
- H) Children’s University Medical Group (CUMG) / University of Washington Physicians (UWP) Associate Members, Limited Associates and Volunteers HIPAA Training
- All CUMG/UWP members who are 50% or greater FTE must have the UW Medicine training in order to maintain billing authorization.
  - Associate Members, Limited Associates and Volunteers can meet the HIPAA training requirement through the following options.
    - a) Associate Members, Limited Associates and Volunteers who are less than 50% FTE may meet the UW Medicine on-line HIPAA training requirement, if they have received HIPAA training of comparable quality at another facility prior to their first clinical experience within UW Medicine. Such individuals must complete, submit and receive a copy of the certificate of training. See “HIPAA TRAINING CERTIFICATION” (Attachment C).
    - b) Associate Members, Limited Associates and Volunteers, who are part-time UW faculty and are less than 50% FTE, Limited Associates and Volunteers that have no other clinical activity outside UW Medicine, and have not received HIPAA training of comparable quality at another facility, must complete UW Medicine on-line HIPAA training before they perform clinical services within UW Medicine.
    - c) Locum Tenens, ARNP and other providers that perform clinical services on a daily basis must have UW Medicine on-line HIPAA training to engage in clinical practice after April 13, 2003. If such individuals engage in intermittent clinical practice, the department administrator must determine on a case-by-case basis the source of the training such individuals must complete. Training must be completed in a manner consistent with the parameters described above in a., b. or c.
  - Department administrators must notify the UWP HIPAA training site coordinator of the names of individuals that meet the UW Medicine on-line HIPAA training requirements through alternative means.
  - CUMG/UWP Associate Members, Limited Associates and Volunteers who have received HIPAA training through the Department of Veterans Affairs at the V.A. Puget Sound Medical Center must complete “HIPAA TRAINING CERTIFICATION” (Attachment C) and send it to the UWP HIPAA training site coordinator.

### **III. Workforce Information Security Awareness and Training Requirements**

The frequency and delivery mechanism of ongoing information security awareness training is approved by the UW Medicine's Information Security Officer and advanced by UW Medicine administrators and department managers.

- A) All work force members are required to receive general level information security training<sup>2</sup> upon becoming a workforce member. This general level training is required for all UW Medicine workforce members to ensure user awareness of information security threats and concerns and to equip users to support organizational information security policies in the course of their work. All members of the workforce are provided with reference materials to allow them to properly protect UW and UW Medicine information resources. The specific material provided to members of the workforce varies depending upon the nature of the role or function performed.
- B) Ongoing security communications are provided for all UW Medicine workforce members to ensure continued awareness of information security threats and concerns. The UW Medicine IT Services Information Security Program oversees that security reminders are distributed.
- C) Additionally, as applicable, UW Medicine departments and business units provide workforce members with:
  - Department and job-specific information security training,
  - Information regarding guidelines and responsibilities associated with their computer and network privileges and resources.
  - Direction for reporting information security events, incidents, and/or malfunctions (information security breach, threat, weakness, and/or calculated violation of trust).
- D) Where relevant, workforce members and third party users receive additional information security training. This includes, but is not limited to information security requirements, legal responsibilities, and business controls.
- E) All systems on the UW Medicine network must designate a System Owner and System Operator.
  - UW Medicine IT Services' System Owner/System Operator training is required for each individual who performs the function of a System Owner or System Operator.

#### **IV. Training Related to Updates or Changes in Policies**

Training related to updates or changes in policies are executed through workforce training, departmental training, job specific training, UW Medicine IT Services' System Owner/System Operator training depending on workforce-wide operations impact. Updates and changes are incorporated into the training materials used for new workforce member, department, and job specific training.

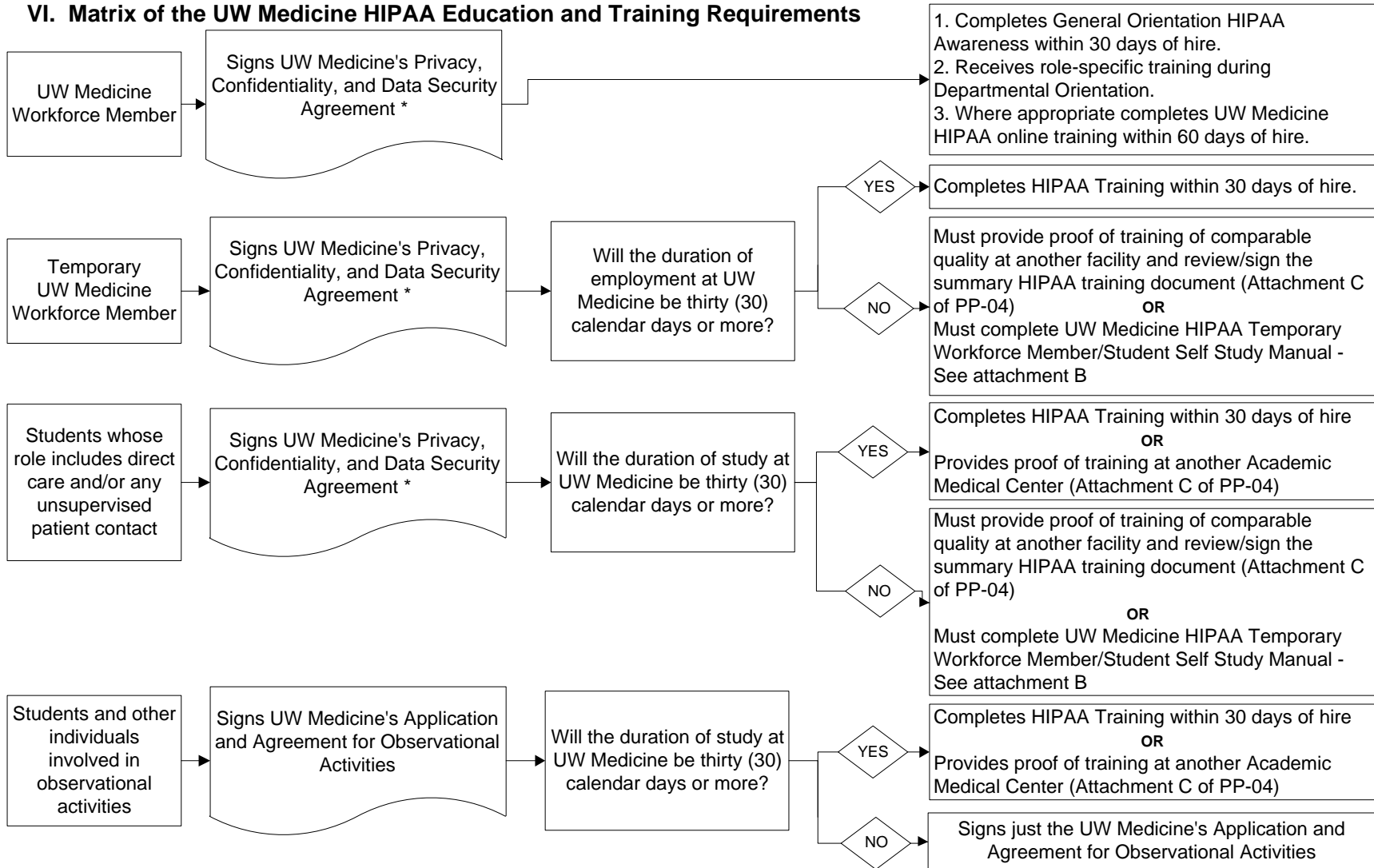
---

<sup>2</sup> General level information security training includes the correct use of information processing facilities. Examples include, but are not limited to log-on procedure, password management, anti-virus, and awareness of organizational policies and procedures.

## **V. Training Documentation Requirements**

- A) The signed UW Medicine Privacy, Confidentiality, and Information Security Agreement must be filed in the workforce member's department personnel or academic record.
- B) Each UW Medicine Entity maintains documentation on all privacy and information security training provided in electronic or written format.
- C) This documentation must be retained for six years from the date of its creation or the date when it last was in effect, whichever is later.

**VI. Matrix of the UW Medicine HIPAA Education and Training Requirements**



\* All members of the UW Medicine Workforce are required to review and sign the Privacy, Confidentiality, and Data Security Agreement at the time of hire and at each evaluation or credentialing.

**References**

- I. 45 CFR Part 164, Section 164.530(b) – “Administrative Requirements - Training”, Section 164.530(j) – “Administrative Requirements – Documentation”
- II. RCW 70.02.005 - Findings.
- III. 45 CFR Part 164; Section 164.308(a)(5) Security Awareness and Training
- IV. WAC 357-37-030 - When and how often must performance feedback be provided to an employee through the formal evaluation process?

**Cross References (where applicable)**

**HHPCC:**

- HHPCC P&P/Administrative Policies/Section4: Personnel/New Employee Orientation
  - Attach A: EPIC Access
  - Attach B: Employee Status Form
  - Attach C: HIPAA Certification Form
  - Attach D1: Checklist CSA & Professional
  - Attach D2: Checklist Hourly
  - Attach E: New Provider Orientation Grid
  - Attach F: Safety Orientation Checklist
  - Attach G: Checklist Grid-All Staff
- Requirements
  - Attach H: New Employee Checklist
  - Attach I: EPIC Training

**Approvals**

\_\_\_\_\_  
UW Privacy Official

\_\_\_\_\_  
Date

Johnese M. Spisso, Chief Health System Officer, UW Medicine & Vice President for Medical Affairs, UW

**Forms/Instructions**

<http://depts.washington.edu/comply/privacy.shtml>

Attachment A: Amendment Request UH2078

Attachment B: Amendment Request Acknowledgement

Attachment C: Amendment Acceptance example letter

Attachment D: Amendment Request Denial

Attachment E: Medical Record Amendments

**Additional Contacts**

UW Medicine Compliance  
206-543-3098  
[comply@uw.edu](mailto:comply@uw.edu)