
Department: UW Medicine Compliance

Subject: PP-04 Privacy, Confidentiality, & Information Security Training

Policy Number: 04

Established Date: June 24, 2002

Revised Date: August, 23, 2004, October 23, 2006

Review Date: April, 2, 2003, May 8, 2008, July 10, 2008

Purpose:

Due to its personal and sensitive nature patient information is accorded special protections under law. UW Medicine¹ 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.

Policy:

All members of UW Medicine's workforce² 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 evaluation³ or credentialing, Managers and/or Supervisors 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

¹ For Purposes of HIPAA, UW Medicine includes the following entities: University of Washington Medical Center and Clinics; Harborview Medical Center and Clinics; UW Physicians Neighborhood Clinics (University of Washington Physicians Network); UW Physicians Sports Medicine Clinic; UW Physician's Eastside Specialty Center; Hall Health Primary Care Center; and University of Washington Physicians, as well as certain services and activities that support UW Medicine that are performed by non-health care components of the University of Washington as defined within Privacy Policy PP-01 Use & Disclosure of Protected Health Information – Organizational Requirements.

² 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.

³ 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.

Information Security Agreement must be filed into the entity's appropriate personnel or academic record.

II. Workforce Privacy Awareness and Training Requirements

Managers and/or Supervisors are to ensure that all members of UW Medicine's workforce receive privacy training:

A) New workforce members:

- 1) 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 HCCS on-line HIPAA training);
- 2) Trained during department orientation on all policies and procedures respecting PHI as it relates to department functions within 60 days;

AND

- 3) Trained during department orientation on all policies and procedures respecting PHI as is necessary to carry out job functions.

(See Procedure I – “Matrix of the UW Medicine HIPAA Education and Training Requirements, Procedure II - “New Employee Training”, Procedure III. – “CUMG/UWP Associate Members, Limited Associates and Volunteers HIPAA Training”, and/or Procedure IV. – “CUMG/UWP Associate Members, Limited Associates and Volunteers Who Receive V.A. Puget Sound Medical Center HIPAA Training” below.)

- 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.
- 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 Privacy and Security General Level 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 Privacy and Security General Level 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 waive the UW Medicine Privacy and Security General Level training.
 - 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.)

(See Procedure V. – "Students in a Training Program")

- F) Students and Other Individuals: No direct Patient Care Activities
Students and other individuals involved in observational and educational activities are required to:

- 1). Sign an Application and Agreement for Observational Activities;
- 2). Be compliant with UW Medicine entity's identification badge policies and procedures;
- 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 Privacy and Security General Level 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 waive the UW Medicine Privacy and Security General Level training;
- 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.

(See Procedure VI. - "Students and Other Individuals Involved in Observational and Educational Activities".)

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 Security Officer and advanced by UW Medicine administrators and department managers.

- A) All work force members are required to receive general level information security training⁴ 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 Security Program oversees that security reminders are distributed.
- C) Additionally, as applicable, UW Medicine departments and business units provide workforce members with:

⁴ General level 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.

- 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 Owner⁵/System Operator⁶ training is required for each individual who performs the function of a System Owner or System Operator.

(See Procedure VII. - "UW Medicine IT Services' System Owner and System Operator Training" below)

IV. 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.

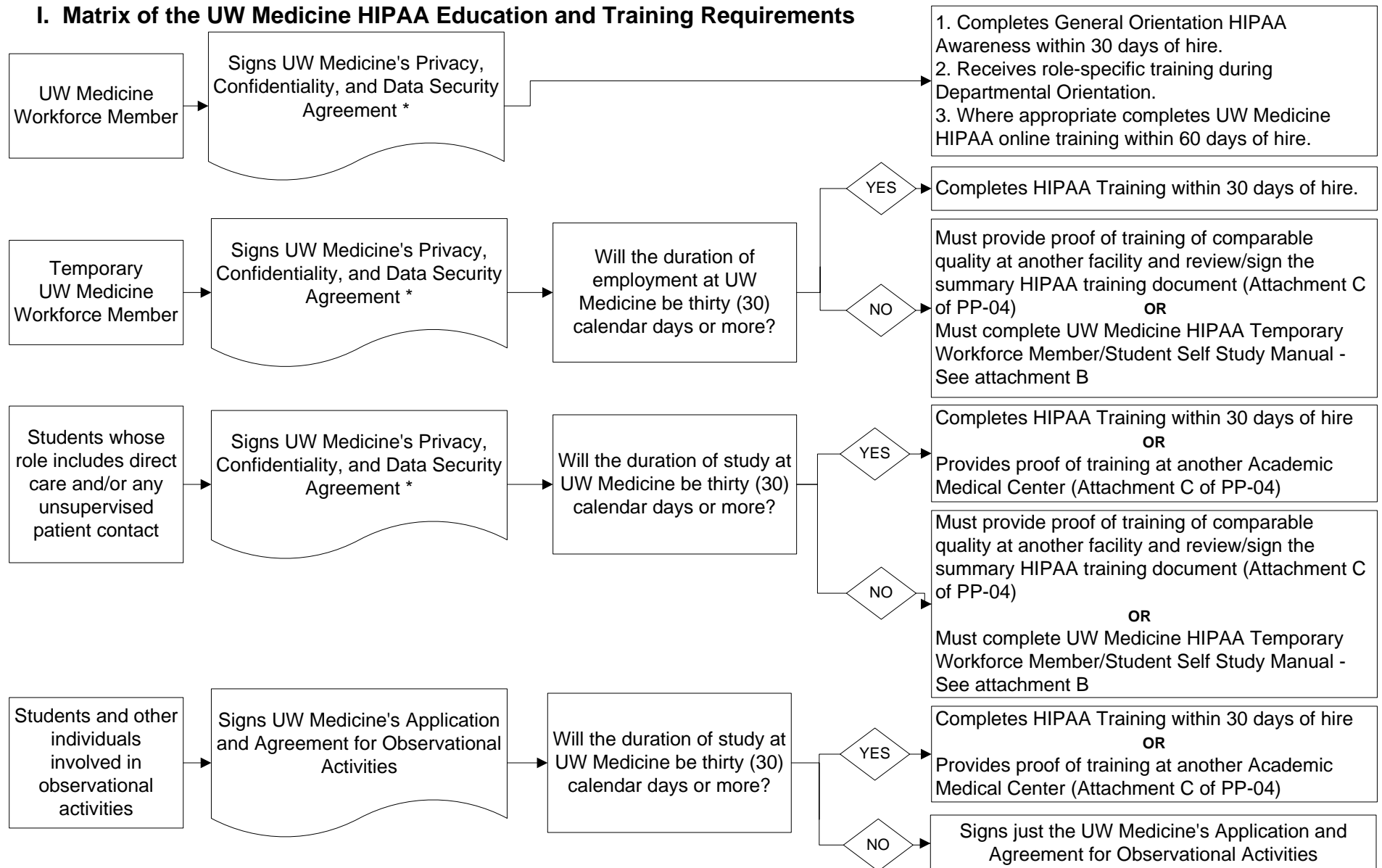
(See Procedure IX - "Documentation of Training" below)

⁵ 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. Their ranks might include members of the UW Medicine professional staff, department heads, faculty members, contracted employees, or students.

⁶ System Operators: Individuals within UW Medicine who are accountable for the operational decisions about the use and management of a computing system.

Procedures:

I. 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.

II. New Employee Training

Step	Action
1	New employee orientation addresses general components for workforce compliance.
2	Department orientation contains department specific training for compliance.
3	Job specific orientation educates workforce members on confidentiality and address PHI privacy and security functions necessary to job performance.
4	At the time of hire and at each performance evaluation 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 workforce member’s personnel or academic record.

III. Children’s University Medical Group (CUMG) / University of Washington Physicians (UWP) Associate Members, Limited Associates and Volunteers HIPAA Training

Step	Action
1	All CUMG/UWP members must have HIPAA training in order to maintain billing authorization.
2	All CUMG/UWP members who are 50% or greater FTE must have the UW Medicine training in order to maintain billing authorization.
3	<p>Departmental Administrators may postpone or excuse the HIPAA training requirement under certain circumstances for specific individual Associate Members, Limited Associates and Volunteers on a case-by-case basis.</p> <ul style="list-style-type: none"> a. Associate Members, Limited Associates and Volunteers who are less than 50% FTE may be excused from the UW Medicine General Level HIPAA training, if they have received HIPAA training of comparable quality at another facility prior to April 14, 2003, or at a time prior to their first clinical experience within UW Medicine after April 14, 2003. 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

	<p>received HIPAA training of comparable quality at another facility, must have UW Medicine HIPAA General Level training before they perform clinical services within UW Medicine.</p> <p>c. Locum Tenens, ARNP and other providers that perform clinical services on a daily basis must have UW Medicine 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.</p>
4	Department administrators must notify the UWP HIPAA training site coordinator of the names of individuals excused from UW Medicine HIPAA General Level training.

IV. CUMG/UWP Associate Members, Limited Associates and Volunteers Who Receive V.A. Puget Sound Medical Center HIPAA Training

Action
CUMG/UWP Associate Members, Limited Associates and Volunteers who have received General Level 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.

V. Students in a Training Program

An affiliation agreement with the school or a letter from a professor or other school official 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:

Step	Action
1	Sign a “UW Medicine Privacy, Confidentiality, and Information Security Agreement.” (Attachment A).
2	Obtain an ID badge for the UW Medicine entity where the training program is to occur.
3	Comply with the UW Medicine entity’s immunization policies and procedures where the training program is to occur.
4	Complete the training as outlined in section II. E. of this policy.

VI. Students and Other Individuals Involved in Observational and Educational Activities

Individuals desiring an observational experience at UW Medicine must complete the following steps:

Step	Action
1	Complete sections A and B of the “UW Medicine APPLICATION AND AGREEMENT FOR OBSERVATIONAL ACTIVITIES” (Attachment D). Each UW Medicine Entity should provide appropriate contact information for the “Return this completed form to:” box on the bottom of the back page.
2	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.
3	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.
4	The student or other individual must complete the training as outlined in section II. F) of this policy.

VII. UW Medicine IT Services’ System Owner and System Operator Training

Step	Action
1	UW Medicine IT Services’ System Owner and System Operator training addresses the required elements of the UW Medicine Security Policies and specific training of security standards, guidelines, and best practices required for compliance.
2	All systems on the UW Medicine network must have a System Owner and a System Operator who have completed this training.

VIII. Training Related to Updates or Changes in Policies

Action
Training related to updates or changes in policies are executed through workforce training, departmental training, job specific training, UW Medicine IT Services’ System Owner training, and/or UW Medicine IT Services’ 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.

IX. Documentation of Training

Step	Action
1	Documentation of training consists of date, time, workforce trainee, and name of the training session attended.
2	Training documentation is placed in workforce department personnel or academic file and/or tracked in UW Medicine entity training databases.

Cross References:

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

References:

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

UW Privacy Officer: _____ Date: _____

Kathryn Waddell, Executive Director, Health Sciences Administration
