

---

Department: UW Medicine Information Technology Services

Policy Number: SEC-03 – Workforce Information Security Policy

Effective Date: June 11<sup>th</sup>, 2007

Review Date: April 27<sup>th</sup>, 2007

---

### **Purpose**

The purpose of the UW Medicine<sup>1</sup> Workforce Information Security Policy is to reduce the information security risks associated with human error, theft, fraud, or misuse of information technology assets. Specific policies in the areas of job definition, security awareness training, and workspace security have been developed to aid UW Medicine in reaching this goal.

### **Definitions**

See UW Medicine Information Security policy: *SEC-REF UW Medicine Information Security Program Glossary of Terms*.

### **Policy**

It is UW Medicine policy that all members of the workforce, as well as affiliates and vendors, manage information security in accordance with applicable law and UW Medicine policies and procedures. Toward that end, UW Medicine includes information security responsibilities in contracts and job descriptions, and addresses information security responsibilities in new employee orientation.

UW Medicine provides training to support the workforce's involvement in information security through new employee orientation, from their assigned department as it relates to department functions, and as is necessary to carry out job functions. Additionally, UW Medicine provides ongoing communications for information security awareness like password management, information security threats, and how to respond to information security events, incidents, and malfunctions.

---

<sup>1</sup> For the purposes of HIPAA, 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.

Workforce separation or transfer procedures are employed to ensure information security.

To reduce risk of unauthorized access, loss of, and damage to information during and outside of normal working hours, UW Medicine establishes secure workspace practices including Clear Workspace, Secure Screen for Workstations, and the Networked Systems Maintenance (Powered-On Standard) which is part of the *SEC-03.01 Workspace Information Security Standard* and supports PC management and security.

## **I. Information Security in Job Definition and Resourcing**

Supervisors of UW Medicine workforce members must define or specify system access in the individual's job description. System access for UW Medicine enterprise systems is role-based. Where system access differs from the standard role, the system access must be defined or specified in the individual's job descriptions. If the requesting of access is delegated, the process must include notification to the individual's supervisor.

University of Washington policy and industry best practices provide that the following principles are applied to job definition and resourcing. (Please see UW Medicine Privacy Policy: *PP-20 Minimum Necessary Requirements for Use & Disclosure of Protected Health Information.*)

- **Principle of Least Privilege:** Access privileges for users are limited to only what is necessary to be able to complete their assigned duties or functions.
- **Principle of Separation of Duties:** Whenever practical, no one person is responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or other harm.
- **Principle of Minimum Necessary:** Access to protected health information is limited to that health information required to perform a particular business activity or to achieve an authorized requestor's specified purpose. Minimum necessary is based on the need-to-know principle.

## **II. User Information Security Awareness Training**

All members of UW Medicine's workforce are required to receive security training.

See UW Medicine Privacy Program policy: *PP-04 Privacy, Confidentiality, & Information Security Training.*

## **III. Workforce Separation or Transfer Events**

All UW Medicine departments and business units establish and maintain all necessary processes to disable user privileges on all computing systems and resources, and to terminate network privileges when a workforce member is separated or transferred.

The following processes and procedures are required when members of the UW Medicine workforce separate or transfer from UW Medicine (or in cases of workforce member suspension, leave of absence, long-term illness or disability):

- The separating or transferring workforce member's supervisor is responsible for notifying all System Owners or their designated system administrator to request that the separating or transferring workforce member's accounts be disabled or modified appropriately based upon *SEC-06 Identity and Access Management Policy*.
- Separating or transferring workforce members may not retain, give away, and/or remove from UW Medicine any protected health information<sup>2</sup> or proprietary information<sup>3</sup> (electronic or hardcopy) other than personal copies of information disseminated to the public and personal copies of correspondence directly related to the terms and conditions of their employment. All other UW Medicine information in the custody of the departing workforce member must be turned over to the workforce member's supervisor at the time of departure.
- At the time of separating or transferring, all UW Medicine property must be returned. This includes, but is not limited to: portable computers, printers, modems, software, cellular telephones, digital pagers, PDAs, documentation, building keys, encryption keys, ID cards, and access cards.

---

---

*References:*

- I.** 45 CFR Part 164; Section 164.308 (a)(3) (i) Workforce Security, (a)(3) Authorization and/or Supervision, Workforce Clearance Procedure, Termination Procedures
- II.** 45 CFR Part 164; Section 164.308(a)(4)
- III.** 45 CFR Part 164; Section 164.310(a)(1) Facility Access Controls
- IV.** 45 CFR Part 164; Section 164.308(a)(5) Security Awareness and Training

---

<sup>2</sup> Protected Health Information (PHI) – Individually identifiable health information maintained in permanent health records and/or other clinical documentation in either paper-based or electronic format.

<sup>3</sup> Proprietary information is any information or material (including, but not restricted to, ideas, concepts, proposals, inventions, instruments, samples, cost estimates, data, and computer programs) that (a) UW Medicine has exclusively developed, (b) is disclosed to the UW Medicine on expressed or implied conditions that limit the UW Medicine's right to use or disclose the information, (c) is specifically identified by the originator (UW Medicine) as proprietary, and/or (d) is classified as sensitive or confidential by UW Medicine. This includes the documents or computer tapes that contain such information.

V. ISO/IEC 17799 Section 6, Personnel Security

VI. University of Washington Information Systems Security Policy

---

---

UW Medicine IT Services: \_\_\_\_\_ Date: \_\_\_\_\_

James S. Fine, M.D., CIO, ISO

---

---