

---

Department: UW Medicine Information Technology Services

Policy Number: SEC-03.01 Workspace Information Security Standard

Effective Date: December 18<sup>th</sup>, 2007

Review Date: December 4<sup>th</sup>, 2007

---

## Purpose

This UW Medicine<sup>1</sup> standard establishes secure workspace practices for workforce<sup>2</sup> members and secure screen practices for workstations. UW Medicine workforce members must be aware of the information security requirements for protecting their unattended computing sessions and must ensure appropriate protection for their own workspace. This standard supports the UW Medicine Information Security Program policy: *SEC-03 Workforce Information Security Policy*.

## Definitions

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

## Standard

All workforce members must protect restricted or confidential material while unattended or not in use. Workstations must be logged off or secured by other means when not in use or unattended. RESTRICTED or CONFIDENTIAL material may include, but is not limited to: hardcopy files printed or copied documents, diagnostic images, and electronic media. This standard applies to all UW Medicine workspaces and/or workstations that access protected health information<sup>3</sup> or proprietary information<sup>4</sup>, regardless of whether there is a

---

<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; Hall Health Primary Care Center; University of Washington Physicians; UW Medicine Eastside Specialty Center, 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.

<sup>2</sup> 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.

<sup>3</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>4</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

computer terminal and regardless of what type of terminal exists at the workstation.

## **I. Clear or Secured Workspace Standard**

UW Medicine's objective for the clear workspace policy is to reduce the risks of unauthorized access, loss of, and damage to information during and outside of normal working hours.

This includes properly storing papers and removable storage media when not in use. Information security classifications<sup>5</sup>, the corresponding risks, and business requirements of UW Medicine will be considered when assessing whether compliance with this policy has been met.

The following controls should be observed:

- Lock away protected health information or critical business information when not in use. Store paper and computer media containing RESTRICTED or CONFIDENTIAL information, such as protected health information, in suitable locked cabinets or areas when not in use or when unattended.
- Clear protected health information or critical business information from printers immediately.
- Protect incoming and outgoing mail points and unattended fax machines from unauthorized access.
- Lock (or protect from unauthorized use in some other way) duplication devices outside of normal working hours.
- Dispose of RESTRICTED or CONFIDENTIAL information in a secure and confidential manner. Please see UW Medicine Information Security policy: *Sec-05.01 – Media Handling Standard*.

## **II. Secure Screen Standard for Workstations**

All members of the UW Medicine workforce are responsible for protecting their workstations from unauthorized access.

Users must:

- A. Terminate active computing sessions when unattended, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;
- B. Log-off networked systems when the computing session is finished.

---

classified as sensitive or confidential by UW Medicine. This includes the documents or computer tapes that contain such information.

<sup>5</sup> Information security classifications: Data is classified into three groups - Public, Restricted, and Confidential. For more information, see UW Medicine Information Security Program policy: *SEC-02 – Information and Information System Classification and Control Policy*.

**III. Networked Systems Maintenance (Powered-On Standard)**

All UW Medicine Networked Systems<sup>6</sup> (PCs) that are part of the AMC Domain or the IT Service's Active Directory are left powered up and connected to the network at all times, including nights, weekends, holidays, and vacations. The purpose is to support general maintenance and information security management activities performed by IT Services.

At the end of each day Users will:

- A. Save data and close applications active on the Networked System.
- B. Initiate a reboot (for Windows systems use Start > Shutdown > Restart).
- C. After the reboot leave the Networked System at the logon prompt.
- D. Leave the PC turned on. (You may turn the monitor off.)

System Owners responsible for any Networked System that is frequently removed from the network, such as a laptop computer, shall ensure that the system is updated on a schedule comparable to general Networked Systems.

---

---

**References:**

- I. 45 CFR Parts 164; Section 164.310(b) Workstation Use
- II. 45 CFR Parts 164; Section 164.310(c) Workstation Security
- III. 45 CFR Parts 164, Section 164.312 (a).(2) (iii) Automatic Logoff

---

---

UW Medicine IT Services: \_\_\_\_\_ Date: \_\_\_\_\_  
James S. Fine, M.D., CIO, ISO

---

---

---

<sup>6</sup> Networked System is a computer system or PC physically interconnected with other computer systems using wired or wireless technology.