

---

---

Department: UW Medicine Information Technology Services

Policy Number: SEC-05 – Communications and Operations Management Policy

Effective Date: June 11th, 2007

Review Date: April 27th, 2007

---

---

## **Purpose**

The purpose of this policy is to set forth network information security standards and system certification standards in order to ensure consistency of communications and operations.

## **Definitions**

- For other definitions see UW Medicine Information Security policy: *SEC-REF UW Medicine Information Security Program Glossary of Terms.*

## **Policy**

It is the policy of UW Medicine<sup>1</sup> to ensure correct and secure management of information on computer and computer networks. System Owners and System Operators must implement controls to prevent, detect, contain, and correct violations to ensure the security of data and the protection of UW Medicine systems and networks from fraudulent activities or unintentional error. All networked systems and system management shall conform to the following operational standards.

## **Standards**

### **I. Integrity Standard**

UW Medicine has policies and standards that protect ePHI at rest, during transmission, and from inappropriate modification. UW Medicine makes efforts to ensure the integrity of ePHI it maintains, integrity of electronic information can be verified using error detection and correction. If intentional modifications are a threat, additional cryptographic-based technologies like MD5 RFC 1321 CRC (Cyclic Redundancy Check) or Digital Signature may be used.

---

<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 Physician's 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.

## **II. Least Privilege Standard**

Users should not have system administrator access unless required by job function.

UW workforce members performing system administrator function(s) must use designated administrative accounts only for system administrative activities and use non-administrative user accounts for all other purposes.

## **III. Software Installation Standard**

Software, including public domain software, must be installed by designated system administrators only.

- The designated system administrator pre-screens the software for viruses;
- The designated system administrator installs only licensed and authorized software on University of Washington and UW Medicine information systems and networks.

## **IV. Protection Against Malicious Software Standard**

All networked systems connected to UW Medicine networks must have controls in place to prevent infection or propagation of malicious software. The method of protection should be enabled to alert the User and/or System Operator of detected malicious software.

On systems where anti-virus software is the designated protection against malicious software, it must be active and up to date. Where appropriate, the notification function must be installed so that the user and System Operator are made aware of virus incidents and actions.

## **V. Information Backup Standard**

System Owners are responsible for ensuring that data backup occurs at an appropriate frequency. Frequency of backups will depend upon how often data changes and how important those changes are. All data backups must be stored according to data classification (See Information Security Policy; *SEC02 Information and Information System Classification Policy*) and UW records retention policies. Backup copies must be tested to ensure that they are usable. System Owners must maintain accurate and complete records of the back-up copies and documented restoration procedures.

## **VI. System Logging**

System logging must be performed on all systems. System Logs are a record of computer activity used for statistical purposes as well as backup and recovery. Log files are written by the operating system or other control program for such purposes as recording incoming dialogs, error and

status messages and certain transaction details. Start and stop times of routine jobs may also be recorded. If an application provides access to ePHI then all access to that data for viewing, editing, or modification must be logged which must include username, date and time accessed, and what activity was performed.

Some System Log examples are:

- Windows – Event Logs, System, Security and Application Logs
- UNIX – syslogd outputs, firewall logs and automated script ‘batch files’

Stored logs must be secured so that they cannot be modified and must be protected from destruction. Only authorized persons have access to stored logs. Because such logs may contain personally-identifiable information, the System Owner and System Operator must comply with University policies related to privacy.

System Operators must review logs of operational events to detect abnormal activities or potential security violations on their systems.

## **VII. Maintenance Log Standard**

System Operators and designees must keep a log of maintenance activities.

Examples of maintenance activities include:

- Restoral of data from backups
- Replacement of failed hardware
- Fail over testing
- Vendor support activities

A. Logs must include:

1. Full name of workforce member or vendor representative
2. System starting and finishing times of activity
3. Problems encountered and corrective action taken

B. System owners must:

1. Review maintenance logs to ensure that problems have been satisfactorily resolved.
2. Review corrective actions to ensure that controls have not been compromised and that the action taken is fully authorized.
3. Maintenance logs must be retained for at least six (6) years.

### **VIII. Logon Banners Standard**

When a logon banner is appropriate for an operating system or application the following language must be used:

“This UW Medicine system is for use by authorized individuals only. Use of this system constitutes an expressed consent to electronic monitoring at all times. If monitoring reveals possible violations of criminal statutes, all relevant information will be provided to law enforcement officials. Individuals using this system without proper authorization will be in violation of UW Medicine security and/or privacy policies. Unauthorized use may be subject to prosecution and/or UW Medicine sanctions.”

### **IX. Minimum Information Security Standard**

All systems must comply with applicable following standards:

Please see the following Minimum Information Security Requirements for the most common operating systems:

- *SEC-05.04-Minimum Workstation and Server Information Security Procedure*
- *SEC-05.05 Other Networked Devices: Minimum Information Security Requirements*
- *SEC-05.06 PDA and Smart Phone Usage in the UW Medicine Environment: Minimum Information Security Requirements*

### **X. Network Access Control Standard**

It is the policy of UW Medicine to deploy network based protection systems such as firewalls, intrusion prevention systems and other controls, as appropriate. The existence of such devices or systems does not in any way substitute for the responsibility of System Owners to ensure that their systems have appropriate host level security, nor does it absolve System Owners of any other responsibilities under UW Medicine security policies.

Provide appropriate means for authentication. If a password management system is used, operating system access controls must ensure quality passwords.

### **XI. Remote Access Control Standard**

The following administrative safeguards must be in place before providing remote access to CONFIDENTIAL and RESTRICTED information:

- Remote access shall only be granted for conduct of official UW Medicine business that is part of the requestor’s official job duties.

- UW Medicine workforce members who telework must comply with the University of Washington Human Resources Telework Policy, <http://www.washington.edu/admin/hr/polproc/telework/index.html>.
- Workforce members must have supervisor approval and/or a documented University of Washington Telework Agreement in place.

Remote access systems must have security controls to appropriately protect the information and information system based on its classification.

- Encryption for example, Virtual Private Networking<sup>2</sup> (VPN), must be used to send or receive information classified as RESTRICTED and/or CONFIDENTIAL over public or unsecured networks. Please see UW Medicine Information Security Policy; *SEC-05.03 – Encryption Standard*.

## **XII. System Certification Standard**

All systems are subject to system security certification to ensure compliance with UW Medicine Information Security Policies.

## **XIII. Media Handling Standard**

See UW Medicine Information Security policy: *SEC-05.01 – Media Handling Standard for Restricted and Confidential Information*.

## **XIV. Automatic Logoff Standard**

To assist in maintaining the confidentiality of protected health information, UW Medicine has standard automatic logoffs for applications and workstations to complement the user's personal responsibility to log out or to secure applications or workstations. These measures are in place to help preserve the confidentiality of patient identifiable information. These measures do not replace employees' personal responsibility to log out or secure applications and workstations or the requirement that only authorized personnel use medical center workstations. The following timeout standards apply for applications and workstations where protected health information is accessible:

1. Applications that contain RESTRICTED or CONFIDENTIAL information must secure inactive sessions. This can be accomplished by the application logging off idle users after fifteen minutes of inactivity or use of application utilities to lock a user's session while allowing other users to use the application. For areas where patients or the public have access to a workstation, these UW Medicine

---

<sup>2</sup> Virtual Private Network (VPN) – a session protected by authentication and encryption of the TCP/IP network layer.

workstations require a screen saver to appear at one minute of workstation inactivity.

2. Exemptions may be granted with approval from the UW Medicine Confidentiality and Access Work Group where inadvertent access risk is lower, staff interruptions are greater, and general timeouts represent a barrier to patient safety.

---

---

**References:**

- I. 45 CFR Part 164; Section 164.308(a) (1) (D) Information System Activity Review
- II. 45 CFR Part 164; Section 164.308(a) (5) (ii) (C) Log-in Monitoring
- III. 45 CFR Part 164; Section 164.308(a) (7) (ii) (A) Data Backup Plan
- IV. 45 CFR Parts 164; Section 164.310(a)(2) (iv) Maintenance Records
- V. 45 CFR Parts 164; Section 164.310 (b) Workstation Use
- VI. 45 CFR Parts 164; Section 164.310 (d) (2) (iv) Data Backup and Storage
- VII. 45 CFR Parts 164; Section 164.312 (b) Audit Controls
- VIII. 45 CFR Parts 164; Section 164.312 (c) (1) Integrity, (2) Mechanism to Authenticate ePHI
- IX. 45 CFR Parts 164; Section 164.312 (e) (1) Transmission Security, (2) (i) Integrity Controls
- X. International Organization for Standardization /International Electrotechnical Commission (ISO/IEC) 17799 Section 8, Communications And Operations Management
- XI. ISO/IEC 17799 Section 9.8, Remote Computing
- XII. UW Information Systems Security Policy 2.1

---

---

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

---

---