
Department: UW Medicine Information Technology Services

Policy Number: SEC-01 Information Security Policy

Effective Date: June 11th, 2007

Review Date: April 27th, 2007

Purpose

UW Medicine¹ systems handle vast amounts of sensitive patient data, support life-critical systems and decision making, and provide crucial information for ongoing operations and attainment of strategic goals.

This policy defines the general approach of UW Medicine to help ensure the confidentiality, integrity, availability, and compliance of UW Medicine information and information systems. It includes UW Medicine's general statement of Information Security policy and defines specific roles and responsibilities within the Information Security program. Subordinate policies, standards, guidelines, and procedures targeting specific topics are provided as separate documents and are only referenced here.

Definitions

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

Policy

It is UW Medicine policy to take all reasonable measures to protect the confidentiality, integrity, and availability of its information and information systems. UW Medicine will ensure full compliance with all applicable state and federal statutes and regulations. As a part of the University of Washington, UW Medicine will also comply with all University of Washington policies.

- A.** All Information Systems purchased or developed for UW Medicine must meet the Information Security Requirements. Contracts for vendor

¹ 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.

purchased products must contain language that the system must meet the Information Security Policies.

- B.** All information entered into or obtained from any UW Medicine information system is the property of UW Medicine, unless otherwise specified by contract.
- C.** All providers and users of UW Medicine information systems and data are required to comply with all established policies, standards, guidelines, and procedures. The requirements for development, approval, review, and revision of these documents are outlined in *SEC-01.01 Management of Information Security Policies, Standards, Guidelines, and Procedures*. In cases where compliance is thought to be infeasible, the department administrator or system owner must apply for an exemption. The exemption process is described in *SEC-01.02 Information Security Policy Exemption Procedure*.

Exemptions to the Information Security Policies may be permitted in rare instances, only when all of the following conditions are met:

- A) A Policy Exemption request has been filled out and sent to the HIPAA Program Office for consideration.
- B) The Security Infrastructure Team (SIT) and the System Operator perform a risk assessment examining the implications of being out of compliance.
- C) The UW Medicine IT Services Director of Information Security and the System Owner prepare a standard risk exemption request.
- D) The UW Medicine Chief Information Officer, the UW Medicine Information Security Officer, and CASC have approved the policy or standard exemption.

The UW Medicine Information Security Policy includes; in addition to this policy, the following policies and their subordinate documents:

SEC-02 Information and Information System Classification Policy

This policy and any subordinate standards, guidelines, and procedures state the requirements for: inventory of information system assets; assignment of system owners and operators; information system classification and data classification; minimum security requirements and advanced system requirements based on classification.

SEC-03 Workforce Information Security Policy

This policy and any subordinate standards, guidelines, and procedures state the requirements for: security in job definition and hiring; security awareness training; management of workforce separations and transfers; workspace security; use of email.

- SEC-04 *Physical and Environmental Information Security Policy***
This policy and any subordinate standards, guidelines, and procedures state the requirements for physical and environmental security.
- SEC-05 *Communications and Operations Management Policy***
This policy and any subordinate standards, guidelines, and procedures state the requirements for: separation of duties; data backup; log management; logon banners; protection against malicious software; media handling; wireless networking; remote access; encryption. Configuration standards for a variety of workstation, server, and other networked device types are also provided.
- SEC-06 *Identity and Access Management Policy***
This policy and any subordinate standards, guidelines, and procedures state the requirements for: user registration and management; system and application access controls; role-based access to ePHI.
- SEC-07 *Business Continuity Policy***
This policy and any subordinate standards, guidelines, and procedures state the requirements for: business impact analysis; data backup plan; disaster recovery plan; contingency plan; applications and data criticality analysis.
- SEC-08 *Audit Policy***
This policy and any subordinate standards, guidelines, and procedures state the requirements for: compliance with audit requests; handling various types of audits; audit reporting; retention of audit documents. This policy also establishes who has the right to conduct audits.
- SEC-09 *Information Security Risk Management Policy***
This policy and any subordinate standards, guidelines, and procedures state the requirements for risk assessment and mitigation.
- SEC-10 *Incident Response and Investigation Policy***
This policy and any subordinate standards, guidelines, and procedures state the requirements for security incident reporting, response, and investigation.

The following UW Medicine Privacy Policies include information security practices and are also part of the UW Medicine Information Security Program.

- PP-04 *Privacy, Confidentiality & Information Security Training***
This policy contains information on the Security training requirements.
- PP-06 *Sanctions for the Failure to Follow Applicable Privacy Policy or for the Breach of Patient Confidentiality or Security***
This policy includes the requirements for corrective actions for Information Security policy violations.
- PP-12 *Use & Disclosure of Protected Health Information by Business Associates***

This policy outlines the requirements for business associate contracts.

I. Applicability

This policy is applicable to all UW Medicine workforce members. Workforce members include faculty, employees, trainees, students, volunteers, Business Associates, and other persons who perform work for UW Medicine, as well as those whose work conduct is under UW Medicine's direct control regardless of whether or not the workforce member is paid by UW Medicine.

All third parties who may have access or permission to use or disclose UW Medicine PHI must have business associate language in the contract. See UW Medicine Privacy Program policy: *PP-12 Use & Disclosure of Protected Health Information by Business Associates*.

II. Roles and Responsibilities

UW Medicine has established a management framework to initiate and monitor the implementation of information security within the organization.

- **Confidentiality and Access Steering Committee (CASC)**

Ensures that there is clear direction and visible management support for UW Medicine security initiatives, reviews and approves UW Medicine information security policies, and approves major UW Medicine initiatives to enhance information security. This committee is chaired by the UW Medicine CIO or designee.

- **Security Implementation Oversight Group (SILOG)**

Drafts and develops UW Medicine Security policies, procedures, and standards with special emphasis on verifying alignment with UW Medicine methodologies and on costs, feasibility, and other implementation concerns. Oversight of enterprise projects with an emphasis on security. This committee is chaired by the UW Medicine Director of Security. Identifies potential impact of proposed projects and technologies on the UW Medicine IT environment and UW Medicine initiatives.

- **Confidentiality and Access Work Group (CAWG)**

Reviews draft UW Medicine Security policies and standards with special emphasis on verifying alignment with UW Medicine Privacy practices and comprehension of policies and standards for UW Medicine workforce members. This committee is responsible for maintaining the Privacy Policies which includes the UW Medicine Access Guide. This committee is chaired by the HIPAA Compliance Officer.

- **University of Washington Chief Information Security Officer**

Responsible for information security compliance at the University of Washington and a member of UW Medicine's Confidentiality and Access Steering Committee (CASC).

- **UW Medicine Information Security Officer (ISO)**

Responsible for development and oversight of UW Medicine security program, assigning security roles, and for approving Information Security Policies and Standards.

- **UW Medicine Chief Information Officer (CIO)**

Responsible for implementation and operating UW Medicine information systems, resources, and services.

- **HIPAA Compliance Officer**

Responsible for ensuring UW Medicine Information Security Program policies comply with federal and state law and other UW Medicine policies.

- **Director of Information Security**

Oversees the development, review, and revision of UW Medicine Security policies, standards, guidelines, and procedures. Approves UW Medicine Security guidelines and procedures. Responsible for the implementation of the Information Security program for IT Services. Directs the UW Medicine Security Infrastructure Team (SIT).

- **Security Policy and Compliance Specialist**

Responsible for developing, reviewing, and modifying UW Medicine Security policies and procedures. Assists departments, partners and alliances in developing and implementing security policies, standards and procedures. Creates plans, tools and training materials to assist UW Medicine management and IT professionals in meeting the requirements of the Information Security Policies and works directly with customers to assess the entity's level of compliance, assess the risk to the enterprise, and identify the gaps and assist in developing a plan of remediation, which is reviewed and updated annually. Also, monitors compliance with UW Medicine IT Services information security policies, procedures, and standards, referring problems to the appropriate departmental contacts, security engineers and administrative teams. When security incidents occur the SPCS will act as lead for the investigation.

- **System Owners and Operators**

System Owners are individuals who are accountable for the appropriate management of one or more UW Medicine information systems. System Operators are individuals with delegated responsibility for routine operation of information systems. System Owners are required to designate a system operator for each of their systems. The System Owner and System Operator may be the same person.

System Owners and System Operators are required to take IT Services System Owner/System Operator (SOSO) training. Information Security responsibilities of System Owners include but are not limited to the following (any of these may be delegated to the System Operator):

- Ensuring systems comply with University of Washington and UW Medicine policies as well as federal and state statutory and regulatory requirements;
- Protecting the confidentiality of sensitive data, especially personally identifiable information and valuable intellectual property (see University of Washington's *Electronic Information Privacy Policy on Personally Identifiable Information*);
- Implementing system 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;
- Ensuring that access controls for the system are implemented in compliance with *SEC-06 Access Control Policy*;
- Ensuring information availability through data backup procedures, contingency planning, and disaster recovery planning (see *SEC-07 Business Contingency and Disaster Recovery Policy*);
- Maintaining system documentation regarding compliance with UW Medicine Information Security Policies and Standards, following the University of Washington and UW Medicine retention policies.
- Ensuring that requests for policy exemptions are submitted as specified in *SEC-01.02 Information Security Policy Exemption Standard*; and
- Ensuring that incident response activities that involve the owner's system(s) follow *SEC-11 Incident Response and Investigations Related to Suspected Breach of Information Security Policy*.

- **Data Custodians**

The *University Of Washington Electronic Privacy Policy On Personally Identifiable Information* delineates the custodial authority for the various types of personally identifiable information. During the course of day-to-day operations of University of Washington business, research, and educational activities, designated individuals representing the interests and specific direction of the senior UW Medicine administrators mentioned above will act as Data Custodians.

A Data Custodian is an individual who has been officially designated accountable for protecting the confidentiality of specific data that is

transmitted, used, and stored on a system or systems within a department, college, school, or administrative unit of UW Medicine.

The role of the Data Custodian is to provide direct authority and control over the management and use of the information contained within a system. These individuals might be deans, department heads, managers, supervisors, or designated staff. They might serve dual roles as System Owners and/or System Operators as well as Data Custodians.

The responsibilities of Data Custodians include, but are not limited to:

- Ensuring compliance with University of Washington and UW Medicine policies as well as statutory and regulatory requirements,
- Working with System Owners and/or System Operators in developing requirements and access control measures for the system to meet the following requirements:
 - Ensuring that users are only supplied access to information needed to perform their work duties, e.g. principle of minimum necessary,
 - Supporting regular review and control procedures that ensure that users and associated access privileges are current and appropriate, and
 - Ensuring that all access granted to users is based on the principle of least privilege where required², and separation of duties where appropriate.

- **Supervisors**

Supervisors fill a vital role in ensuring information security compliance by members of the workforce under their supervision. This section refers to all people who perform the role of Supervisor, which may include many levels of personnel, including managers, administrators and department chairs.

The Supervisors are:

- Responsible for ensuring that each of their direct reports signs the Privacy, Confidentiality, and Information Security Agreement.
- Responsible for ensuring that access to information systems are deactivated immediately for every direct report who separates from employment or transfers out of their reporting area.

- **Users**

Any individual who uses a computer connected to UW Medicine networks or who has been granted privileges and access to UW Medicine computing, network services, applications, and/or resources.

² For more information, see UW Medicine Privacy policy: *PP-20 Minimum Necessary Requirements for Use & Disclosure of Protected Health Information*. https://know1.mcis.washington.edu/proj_hipaa/

Users of University of Washington & UW Medicine computing resources and data are responsible for the following:

- Comply with University of Washington and UW Medicine policies;
- Support compliance with federal and state statutory and regulatory requirements;
- Protect access accounts, privileges, and associated passwords (examples: Not sharing my password and Not logging on for others);
- Maintain the confidentiality of information to which access privileges are given;
- Accept accountability for all activities associated with the use of individual user accounts and related access privileges;
- Not to change the computer configuration unless specifically approved to do so;
- Report all suspected security and/or policy violations to user's Help Desk, See UW Medicine Information Security policy: SEC 10 Incident Response Policy;
- Ensure that use of UW & UW Medicine computers, email, computer accounts, networks, and information accessed, stored, or used on any of these systems is restricted to authorized duties or activities;
- Use only licensed and authorized software;
- Not to download, install or run unlicensed or unauthorized software;
- Not to disable or alter the anti-virus and/or firewall software;
- Make no unauthorized network modifications and/or additions (i.e., wireless access points, mini-hubs or switches); and
- Report all known privacy violations to the appropriate entity's Privacy Official or the UW Medicine Privacy Office.

Recommended Practice: Do not store data on workstation hard drive.

III. Inventory of Information System Assets

The entities and departments of UW Medicine shall establish an inventory that documents the assets associated with each information system including ownership and information security classification. The inventory should be updated on a regular basis as assets are added or removed from the system.

Information and information system assets include, but are not limited to:

- Information assets: databases and data files, system documentation, user manuals, training material, operational or support procedures,

continuity plans, fallback arrangements, archived information, and electronic media (CD-ROM disks, tapes and floppy disks);

- Software assets: application software, system software, development tools and utilities;
- Information Systems: computer equipment (for example, computer systems, computer hardware components, and laptops), and communications equipment (for example network cabling and components, routers, PBXs, fax machines, voice mail).

IV. Accountability for Information and Information System Assets

All UW Medicine information and information systems shall have a designated System Owner. System Owners are responsible for maintaining appropriate security, which includes classifying the information and information system. Although information security responsibilities may be delegated, accountability remains with the designated System Owner.

The System Owner is to maintain the documentation regarding the classification of the information and/or information system.

V. Software Licensing and Unauthorized Use Standard

A. Software Licensing

Proprietary software products are supplied under a license agreement that limits the use of the products for specific users and may limit copying to the creation of back-up copies only.

- Unauthorized use of software or files is regarded as a serious matter and any such use is without the consent of the UW Medicine. If abuse of computer software or files occurs, those responsible may be held legally accountable as well as be held accountable for violation of UW Medicine policy.

To ensure compliance with Federal software licensing laws, the following standards should be observed:

- Supervisors provide awareness of the software copyright requirements including UW Medicine's intent to take corrective and/or disciplinary action if members of the workforce breach policy.
- System Owners and System Operators maintain proof of ownership of licenses, original disk(s), and manual(s).
- System Owners and System Operators implement controls to ensure that any maximum number of users permitted is not exceeded.

- System Owners and System Operators comply with terms and conditions for software and information obtained from public networks.

B. Unauthorized Use

1. Washington State Law

State of Washington Executive Ethics Board restricts personal activities on State owned computers to *occasional* and *de minimus* (e.g., of minimal cost to the State) use. This limitation is similar to permitted personal use of non-computer resources, such as telephone calls. Limited personal use of computer resources is acceptable only when the use:

- Results in little or no cost to the State;
- Does not interfere with the employee's official duties;
- Is brief in duration, occurs infrequently, and is the effective use of time and resources;
- Does not disrupt or distract from the conduct of State business due to volume or frequency;
- Does not compromise the security or integrity of State property, information or software; or
- Does not disrupt other State employees and does not obligate them to make personal use of State resources.

If known or suspected use exceeds de minimus, UW Medicine shall immediately report to University of Washington Internal Audit. Internal Audit will immediately notify the State Auditor's Office and follow the policy and procedures per University of Washington Administrative Policy 47.10: Policy on Financial Irregularities and Other Related Illegal Acts.

Washington State law prohibits the use of UW Medicine computers for personal business-related, commercial, campaign or political purposes, to promote an outside business or group, or to conduct illegal activities. In particular, employees are also prohibited from:

- Allowing any member of the public to make personal use of state computers and computing resources;
- Placing notices for selling of personal items on any State owned computer system; and
- Posting notices for charity/fund raising events, whether selling an item or raising money, unless the activity is University sponsored.

2. Many Internet Activities Expressly Prohibited

Although de minimus personal Internet use is now allowable, many Internet activities are still prohibited. Downloading files that violates copyright laws, such as MP3 music files, subjects UW to lawsuits. Internet activities can be traced back to your computer, and Internet sites can download software affecting the operation of your computer and the privacy of confidential information. Other examples of improper or excessive use are included in the Executive Ethics Board web site: <http://www.wa.gov/ethics> and the UW Administrative Policy web site <http://www.washington.edu/admin/adminpro/APS/47.02.html>

References:

- I. University of Washington Information Systems Security Policy (Security Policy)
- II. University of Washington's Electronic Information Privacy Policy on Personally Identifiable Information
- III. 45 CFR Part 164; Section 164.306(a) General Requirements
- IV. 45 CFR Part 164; Section 164.306 (a) (iv) Ensure Compliance with this subpart by its Workforce
- V. 45 CFR Part 164; Section 164.308(a)(1) (i), (ii) (A) Risk Analysis, (ii) (C) Sanction Policy
- VI. 45 CFR Part 164; Section 164.308(a)(2) Assigned Security Responsibility
- VII. 45 CFR Part 164; Section 164.308(a)(5) (i) Security Awareness and Training, (ii) (A) Security Reminders, (ii) (B) Protection from Malicious Software, (ii) (D) Password Management
- VIII. 45 CFR Part 164; Section 164.308(a)(8) (b) (1) Business Associate Contracts and other Arrangements
- IX. 45 CFR Part 164; Section 164.314 (a) Business Associate Contracts or other Arrangements
- X. 45 CFR Part 164; Section 164.316 Policies and Procedures and Documentation Requirements
- XI. RCW 42.17 Public Records - Personal Information – Notice of Security Breaches

- XII. RCW 42.52.360; Authority of executive ethics board.
- XIII. RCW 43.09.185: Loss of public funds -- Illegal activity -- Report to state auditor's office
- XIV. WAC 292-110-010; Use of state resources
- XV. International Organization for Standardization /International Electrotechnical Commission (ISO/IEC) 17799 Section 3, Security Policy
- XVI. ISO/IEC 17799 Section 4, Organizational Security
- XVII. National Institute of Standards and Technology (NIST) Special Publication 800-18; "Guide for Developing Security Plans for Information Technology Systems"

UW Medicine IT Services: _____ Date: _____

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