
Department: UW Medicine Information Technology Services

Policy Number: SEC-08 –Information Security and Privacy Audit Policy

Effective Date: June 11th, 2007

Review Date: April 27th, 2007

Purpose

Audits to ensure compliance are an important part of UW Medicine's Information Security and Privacy programs. This policy establishes the authority to conduct audits, outlines audit scope and applicability, and lists requirements for audit documentation and reporting.

Definitions

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

Policy

I. Authority to Audit

The UW Medicine Compliance Office and the University of Washington Internal Audit have the authority to perform audits on Information Security Practices. This authority provides the UW Medicine Compliance Office or University of Washington Internal Audit Department full access to any and all University records and personnel necessary to conduct an audit (for example, any documents, computer files, property, and personnel of UW Medicine.)

II. Audit Scope and Applicability

All areas, systems, processes, and workforce members within UW Medicine are subject to audit to ensure compliance with Information Security and Privacy policies and standards.

The University of Washington has created the following document to help in the managing of an audit - <http://www.washington.edu/admin/audit/manage.html> or <http://www.washington.edu/admin/audit/externalauditors.html>

For further assistance with a UW Medicine audit please contact the HIPAA Program Office at hipaa@u.washington.edu

III. Types of Audits

A. Self Audits

System Owners should routinely perform self audits of their system(s). This should include but not be limited to an evaluation of the system(s) compliance with the UW Medicine security policies.

Supervisors should also perform self audits to determine their departments overall security readiness. This should include but not be limited to evaluations of procedures and practices being used by end users, physical security and account maintenance.

B. UW Internal Audits

The UW Internal Audit may perform an audit of any University of Washington department or workforce member. This may include any department or workforce member that is part of UW Medicine. These audits could be for financial, accountability, or performance reasons.

C. UW Medicine Internal Audits

Internal audits are conducted as part of a proactive program to verify that all reasonable and appropriate measures have been taken to safeguard UW Medicine information and information systems, to identify areas needing improvement, and to ensure there is accountability for remediation plans. The intent of the audits is to improve UW Medicine's privacy and security practices. If audits reveal repeated lapses, malicious intent, or reckless negligence, appropriate investigations will be conducted in accordance with *PP-05 Complaints and Investigations Related to UW Medicine Privacy Practices* and *SEC-10 Incident Response Policy*.

D. External Audits at UW Medicine's Request

The UW Medicine Information Security Officer will periodically obtain an externally provided and independent review of information security. These reviews will include efforts to determine adequacy of security controls and compliance with applicable requirements. These audits may be conducted by vendors, independent consultants, or other third-parties as deemed appropriate.

E. Regulatory Investigations and Audits

As part of an investigation, the Office of Civil Rights, the Department of Justice or the Centers for Medicare & Medicaid Services (CMS) may order an external audit regarding privacy or information security. It is the policy of UW

Medicine to fully cooperate with external auditors. The UW Medicine HIPAA Compliance Officer will serve as a liaison between UW Medicine and external auditors.

IV. Documentation and Reporting

A. Reporting to Authorities

If known or suspected illegal acts (i.e. computer use exceeds de minimus) are discovered in the course of an audit, UW Medicine shall immediately report to University of Washington Internal Audit Department.

B. Distribution of Findings

Audit findings must be documented and distributed to:

- Manager or Supervisor of an individual, department, or system that was subject of an audit
- The Confidentiality and Access Steering Committee

As appropriate, the results may also be distributed to:

- System Owner and/or System Operator
- Individual who was subject of an audit
- Entity Privacy Official
- UW Medicine HIPAA Compliance Officer
- UW Medicine Information Security Officer
- University of Washington Privacy Officer

If an audit finds that a patient's private data was inappropriately disclosed or otherwise mishandled, UW Medicine Privacy Officer's will be notified to initiate the Privacy Incident Response process.

C. Retention of Documentation

Documentation will be maintained for 3 years, per General Schedule # GS04001: INTERNAL AUDITS, WORKING PAPERS AND REPORTS

<http://www.secstate.wa.gov/archives/pdf/STATE%20GS%20MANUAL%204-2002.pdf>

References:

- I. 45 CFR Part 164; Section 164.308(a)(1)(ii)(d); Information System Activity Review
- II. 45 CFR Part 164; Section 164.308(a)(8); Evaluation
- III. 45 CFR Part 164; Section 164.312(b) Audit Controls

- IV. RCW 42.52.360: Authority of executive ethics board.
 - V. RCW 43.09.185: Loss of public funds -- Illegal activity -- Report to state auditor's office.
 - VI. WAC 292-110-010: Use of state resources.
 - VII. 5 U.S.C. § 552a The Privacy Act of 1974
-
-

UW Privacy Officer: _____ Date: _____
John A Coulter, Associate Vice President for Medical Affairs

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