
Department:	UW Medicine Information Technology Services
Policy Number:	SEC-10 Policy for Responding to Information Security Incidents and Complaints
Effective Date:	February 8, 2008
Review Date:	January 25, 2008

Purpose

When an information security incident occurs or there is a potential violation of information security policy, it is critical that the event is reported, an investigation occurs, and appropriate actions are taken in response. These responses will help limit damages and identify targets for improving UW Medicine information security. This policy establishes requirements for reporting, investigating, and responding to information security incidents and complaints.

Definitions

- **Information security complaint:** A report of a suspected violation of UW Medicine policy, state or federal law, or other regulation.
- **Information security incident:** An event involving a breach or potential breach of UW Medicine security controls, or an unauthorized exposure of data through other means.

Policy

UW Medicine Compliance will triage all reported security incidents and complaints and ensure that they are responded to in an appropriate and timely manner. The following general requirements must be met:

- All investigations and subsequent responses must be handled consistently, regardless of who reported the problem or who an investigation may target.
- Based on the results of the investigation, appropriate actions must be taken to terminate unauthorized access or misuse, contain damages, and reduce the likelihood of recurrence.
- The Department Chair, Medical Director, Program Director, Supervisor, Manager, or Vice Dean for Academic Affairs will evaluate and carry out corrective actions in accordance with applicable personnel policies and UW Medicine privacy policy PP-06 (see References).
- All security incidents, complaints, investigations, and subsequent responses must be thoroughly documented.

I. Incident Reporting Requirements

- A) UW Medicine workforce members are required to report any potential security incident or violation of policy that they become aware of by any means. This requirement applies to workforce members who monitor UW Medicine networks and systems, as well as the owners, operators, and users of these networks and systems. Reports must be directed to the IT Services Help Desk at 206-543-7012 or mcsos@u.washington.edu. Workforce members should direct questions about

reporting requirements to the Compliance Department at their entity.

- B) The Help Desk will open tickets for all incoming reports, assign them to the Compliance queue, and set them to Severity 1.

II. Assignment of a Lead Investigator

- A) When a security incident or complaint involves patient information or systems from only one UW Medicine entity, the Privacy Officer of that entity leads the investigation.
- B) When a security incident or complaint involves patient information or systems from more than one UW Medicine entity, the UW Medicine HIPAA Compliance Officer leads the investigation.

III. Formation of the Incident Response & Investigation Team

The lead investigator will establish an incident response and investigation team on an as-needed basis. Team members will be drawn from the following areas, as appropriate:

- **University of Washington:** Chief Information Security Officer, Privacy Officer, Health Sciences Risk Management
- **UW Medicine:** Information Security Officer, HIPAA Compliance Officer, News & Community Relations
- **IT Services:** Information Security Director, Security Team, technical experts as needed
- **UW Medicine Entity:** Medical Director, Associate Administrator, Chief Nursing Officer, Privacy Officer, Human Resources
- **Department Involved in Incident:** Chair/Service/Division Chief, System Owner, System Operator, Department Administrator/Manager, other technical experts.

IV. Roles & Responsibilities During Investigation and Response

A) Lead Investigator

The lead investigator is responsible for:

- Working with Health Sciences Risk Management to assess the risks, likelihood of exposure and potential impact associated with the incident.
- Determining if an incident response and investigation team is needed and appointing appropriate team members. If an investigation involves the conduct of a School of Medicine workforce member, the SOM Compliance staff must be involved.
- Developing and managing execution of the investigation plan for each incident and complaint.
- Notifying UW Internal Audit if, during the course of an investigation, it is determined that a workforce member violated University of Washington Policy, *AP 47.2 Personal Use of University Facilities, Computers, and Equipment by University Employees*.
- Recommending corrective actions in accordance with UW Medicine privacy policy PP-06 (see References).
- Recommending remediation strategies to reduce risks.
- Documenting all events and outcomes.

B) UW Medicine HIPAA Compliance Officer

The UW Medicine HIPAA Compliance Officer is responsible for:

- Managing the Help Desk Compliance queue.
- Acting as lead investigator, as appropriate.
- Participating on the incident response and investigation team.
- Prioritizing forensics cases in the Security Team's queue.
- Communicating with appropriate UW and UW Medicine officials such as the CEO, COO, CFO, Associate Vice Presidents, UW Information Security Officer, and UW Privacy Officer.
- Providing general oversight of all investigations to ensure consistent and timely handling of all related matters.

C) UW Medicine Entity Privacy Officers

UW Medicine Privacy Officers are responsible for:

- Acting as lead investigator, as appropriate.
- Participating on the incident response and investigation team.
- Communicating with appropriate entity officials such as the Executive Director, COO, Medical Director, CNO, Associate Administrators, Department Chiefs, Department Directors, Department Managers, and System Owners.
- Managing the notification process.
- Reporting aggregate information to the UW Medicine Board Compliance Committee, the UW Medicine Confidentiality and Access Steering Committee, and the entity Compliance Committee.

D) Incident Response and Investigation Team

The incident response and investigation team is responsible for:

- Identifying business operations that may be impacted by the team's decisions.
- Determining the likelihood that PII or PHI was obtained in a readable form by unauthorized individuals, taking into consideration the use of encryption and other access controls.
- Determining whether or not to notify individuals included in the PII or PHI, taking into consideration the evidence from the investigation, legal requirements, and the standard of due care.
- If a decision to notify is made, determining how notification will be provided.
- Deciding whether to notify law enforcement officials.
- Establishing a timely and effective communication plan regarding the incident, working closely with appropriate UW Medicine officials to develop public announcements and press releases.
- Identifying a member of the team to serve as primary point of contact for communication and presentations.

E) IT Services Security Team

The Security Team serves as a technical consultant as required for security incidents and will conduct forensic investigations when requested by the lead investigator through the IT Services Help Desk. Forensics will be completed in priority order, as set by the UW Medicine HIPAA Compliance Officer.

F) System Owners

System Owners are responsible for working with the incident response and investigation team to stop unauthorized access to their systems, contain any damage, and mitigate the risk of future incidents. System Owners also assist the Privacy Officer with the notification process.

G) Department Directors and Department Managers

Department Directors and Department Managers are responsible for identifying the funds to cover the cost of notifying individuals whose information was exposed by an event within their department. They are also responsible for an evaluation of departmental policies, procedures, and training related to the incident or complaint.

H) Workforce Members

UW Medicine workforce members must cooperate with the investigation of any security incident or complaint. Failure to do so may constitute grounds for corrective action.

V. Notification For Potential Breach Of Personal Information

If the Incident Response and Investigation Team decides to notify individuals that are potentially affected by a breach of personal information, the following requirements apply:

- A) Notices to each affected individual shall be made within ten (10) working days from the date of the confirmation that an individuals' personal information was compromised. This timeline shall be extended if a law enforcement agency determines that notification will impede a criminal investigation. In such cases, notification shall not be made until authorized by the law enforcement agency.
- B) Written notice will be sent to each affected individual unless the cost of providing notice would exceed \$250,000, or more than 500,000 individuals need to be notified, or if there is insufficient contact information to make individual notification. In such cases, notification shall be made as follows:
 - 1. Email notice when an email address for the subject person is available;
 - 2. Conspicuous posting of a notice on the UW Medicine web sites; and
 - 3. Notification to major statewide media.

VI. Security Event Documentation

The Lead Investigator must document all security events and outcomes in the Security Events Database operated by UW Health Sciences Risk Management. This documentation must be retained in accordance with established records management rules.

References:

- I. 45 CFR Part 164; Section 164.308(a) (6) (i) Security Incident Procedures, (ii) Response and Reporting.
 - II. PP-06 Sanctions for the Failure to Follow Applicable Privacy and/or Information Security Policy or for the Breach of Patient Confidentiality or Information Security.
 - III. RCW 42.56.590 Public Records - Personal Information – Notice of Security Breaches.
 - IV. WAC 292-110-010; Use of state resources.
 - V. ISO/IEC 17799 Section 11, Business Continuity Management.
-
-

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