
Department: UW Medicine Compliance

Subject: PP-06 Sanctions for the Failure to Follow Privacy and/or Information Security Policies

Policy Number: 06

Effective Date: January 25, 2008

Review Date: January 25, 2008

Policy:

Each UW Medicine entity¹ reviews and investigates reported and identified failures to comply with policies related to information privacy, confidentiality, and security, and imposes appropriate sanctions where indicated. See, UW Medicine Policy: *PP-05 Complaints and Investigations Related to UW Medicine Privacy Practices and SEC-10 Policy for Responding to Information Security Incidents and Complaints*.

UW Medicine sanctions are commensurate with the severity, frequency, and intent of violations. UW Medicine applies sanctions to members of its workforce² without regard to role or position. The level of breach in addition to the workforce member's corrective action record determines actual sanctions.

Failure to follow Privacy and Information Security Policies will subject the individual to an investigation and corrective actions in accordance with this policy. The corrective actions include, but are not limited to: verbal warning, written warning/reprimand, counseling, counseling with re-education, or termination/dismissal. This is in accordance with the provisions of applicable Code of Federal Regulations, University of Washington policy, UW Medicine entity specific policies, Washington Administrative Code, Medical Staff By-Laws, and current labor agreements.

When contracts are established for third parties (Business Associates), the third party's workforce members are held to the same expectations as UW Medicine Workforce Members. All such contracts must include a business associate agreement that contains termination clauses for violating the terms of the contract. See UW Medicine Privacy Policy: *PP-12 Use & Disclosure of Protected Health Information by Business Associates*.

¹ 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.

² Workforce: Faculty, employees, trainees (e.g. students, Residents, Fellows), 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 the workforce member is paid by UW Medicine.

Sanctions will not be applied to a workforce member who:

- Discloses protected health information (PHI) to a health oversight agency **or**
- An individual or attorney who reports either an allegation of unlawful conduct by the entity or a violation of professional standards or clinical standards, or conditions in the entity that endanger patients (whistleblower).

Additionally, sanctions will not be applied for:

- Filing complaints,
- Testifying,
- Participating in investigations,
- Compliance reviews,
- Proceedings or hearings, **or**
- Good faith disclosures concerning real or perceived unlawful acts or practices.

The UW Medicine entity Privacy Official or Compliance Specialist follows the process outlined in *PP-05 Complaints and Investigations Related to UW Medicine Privacy Practices and/or SEC-10 Policy for Responding to Information Security Incidents and Complaints* to conduct and document investigations of reported events. Once an investigation is completed, the Privacy Official or Compliance Specialist follows the process outlined below to determine the violation level and to recommend corrective action(s) to the appropriate authority that determines the course of disciplinary/correction actions/terminations..

The authority that determines the course of disciplinary/corrective actions/termination should include the workforce member's past corrective actions to determine the actual sanctions to be administered. Entity Privacy Official or Compliance Specialist maintains records of findings and workforce member's department places findings in individual's personnel, Dean's Office or academic file. The workforce member's supervisor or manager must report the final corrective action to the Entity Privacy Official or Compliance Specialist within 30 days of the Privacy or Security Event Report being issued.

I. **Violation Levels** – There are five (5) levels of privacy and security infractions as described below:

A. **Level 0: No Breach of Confidentiality**

This level occurs when a workforce member has a clear business need to access PHI or handles information appropriately given his or her job function.

Examples, which are not meant to be an all inclusive listing, of Level 0 violations include:

- Workforce member accesses PHI within the scope of their job functions.
- Workforce member discloses PHI according to authorization or required by law.

B. Level 1: Unable to Determine Whether a Breach Occurred

This level of violation occurs when there is insufficient information/evidence to support or confirm either a breach of confidentiality or a failure to follow Privacy and/or Information Security Policy.

Examples, which are not meant to be an all inclusive listing, of Level 1 violations include:

- Workforce member is accused of disclosing PHI inappropriately, but the investigation results in either no or insufficient evidence to support the accusation.
- A breach or potential breach was discovered after the system in question was re-deployed and evidence of the breach has been tampered with or completely destroyed by someone other than the workforce member at issue.

C. Level 2: Policy Violation with Mitigating Circumstances

- Uses or discloses PHI without a business need to know, but with mitigating circumstances.
- Violates UW Medicine Privacy and/or Information Security Policy, but with mitigating circumstances.
- Takes action or inaction that exposes UW Medicine to a potential security breach, but with mitigating circumstances.

Examples, which are not meant to be an all inclusive listing, of Level 2 violations include:

- Workforce member intends to email PHI for appropriate treatment, payment, or healthcare operations, but mistakenly sends email to unintended recipients.
- Workforce member discusses patient care with another care team member in public location; other individuals in the listening area make a complaint.
- Workforce member stuffs letter into wrong envelope, leading to accidental disclosure of PHI.
- Workforce member misunderstood secure configuration or implementation of technology.
- Workforce member attempted to implement or supplement security controls believing them to be in compliance or meant to improve security.

D. Level 3: Policy Violation Without Reasonable Appearance of Malicious Intent

This level of violation occurs when a workforce member deliberately accesses, reviews, discloses, or discusses confidential information or systems, without documented authorization to do so. Workforce member violated Information Security Policy or exposed UW Medicine to a potential security breach that does not appear to be intended as malicious, harmful, or to demonstrate a reckless disregard for information security.

Examples, which are not meant to be an all inclusive listing, of Level 3 violations include:

- Workforce member is not providing care to the family member, but nevertheless accesses health record.
- Workforce member accesses a patient record out of curiosity.

- Workforce member accesses a record of a fellow clinician who had/is having medical problems.
- Workforce member shares details of a patient's treatment while at a social function. The clinician names the patient or provides sufficient detail that others know to whom clinician is referring.
- Workforce member shares his or her password.
- Workforce member fails to follow policy such as obtaining appropriate release of information prior to releasing information.
- Workforce member uses aggregate data without institutional approval.
- Workforce member fails to report a known breach or violation of policy.
- Workforce member fails to complete required HIPAA training.
- Workforce member purposefully disregards policy or repeats policy violations.
- Workforce member disables information security controls such as anti-virus software.

E. Level 4: Policy Violation With Reasonable Appearance of Malicious Intent, Personal Gain or Motivation, Willful Disregard of Policy, or Repeated Offenses

This level of violation occurs when a workforce member uses, accesses, alters, or discloses PHI without a business need to know or inappropriately disseminates individually identifiable information or repeatedly violates policy. This is considered a breach even if the member of workforce took no further action relating to the PHI. Workforce member violates the UW Medicine Privacy and/or Information Security policies with reasonable appearance of personal gain (monetary or non-monetary), malicious intent, or that demonstrates a willful disregard for UW Medicine policies.

Examples, which are not meant to be an all inclusive listing, of Level 4 violations include:

- Workforce member access a medical record of an estranged family member.
- Workforce member intentionally alters or destroys data or equipment.
- Workforce member releases data for personal gain (monetary or non-monetary) or motivation.
- Workforce member releases data with intent to harm an individual or the organization.
- Workforce member purposefully disregards policy or repeats a violation.
- Workforce member fails to implement standards after repeated notification.
- Workforce member works in conjunction with another to breach UW Medicine security.
- Workforce member compiles, uses, or discloses PHI for personal or commercial use.
- Workforce member intentionally releases PHI outside of UW Medicine against UW Medicine Policy.

II. Authority That Determines Course of Disciplinary/Corrective Actions/Termination:

A. Level 1 Violations

1. Authority that determines course of action

- a. For faculty and medical staff: the Department Chair and/or Medical Director.
- b. For Residents and Fellows: the Department Chair, Medical Director, and/or Program Director.
- c. For other members of the workforce: the workforce member's supervisor/manager.
- d. For medical students: the Vice Dean for Academic Affairs and/or Medical Director.

B. Level 2 , 3, and 4 Violations

1. Authority that determines course of action

- a. For faculty and medical staff: the Department Chair and/or Medical Director, in consultation with SOM Human Resources, determines the course of corrective action, including the initiation of corrective or disciplinary action, depending on the terms of the employment/service contract or agreement.
- b. For Residents and Fellows: the Department Chair, Medical Director, and/or Program Director in consultation with the GME Office.
- c. For other members of the workforce: the workforce member's Department Manager, in consultation with Human Resources.
- d. For medical students: the Vice Dean for Academic Affairs and/or Medical Director.

III. Range of Recommended Disciplinary/Corrective Actions:

A. Level 0 Violations

- No corrective action is recommended.

B. Level 1 Violations

- Training or coaching may be deemed appropriate.

C. Level 2 Violations

1. UW Medicine entity may require workforce member to renew his/ her understanding by signing another UW Medicine "Privacy, Confidentiality and Information Security Agreement" (*PP-04 Privacy, Confidentiality, & Information Security Training -Attachment A*) within 30 days.
2. The workforce member's access to the Electronic Medical Record may be monitored for three months.
3. Non-exclusive examples of corrective action:
 - Re-evaluation of competence and a plan to build competency level
 - Loss of access privileges
 - Coaching
 - Retraining
 - Counseling (includes informal, formal, and final)
 - Suspension(Note: The above are only examples and not necessarily intended to be the preferred or required actions.).

D. Level 3 Violations

1. Workforce member may be placed on a leave of absence during investigation in accordance with the terms of the employment/service contract or agreement.
2. If workforce member's association with UW Medicine is not terminated, then UW Medicine entity requires workforce member to renew his/her understanding by signing another UW Medicine "Privacy, Confidentiality and Information Security Agreement" (*PP-04 Privacy, Confidentiality, & Information Security Training -Attachment A*) within 30 days.
3. The workforce member's access to the Electronic Medical Record may be monitored.
4. Non-exclusive examples of corrective action:
 - Re-evaluation of competence and a plan to build competency level
 - Loss of access privileges
 - Reduction in pay
 - Retraining
 - Counseling (includes, among other things, informal, formal, and final)
 - Suspension
 - Demotion
 - Termination or dismissal(Note: The above are only possibilities and not intended to be the actions of choice or requirement.)

E. Level 4 Violations

1. Workforce member may be placed on a leave of absence during investigation in accordance with the terms of the employment/service contract or agreement.
2. Non-exclusive examples of corrective action:
 - Termination of employment/services or dismissal.

IV. Supervisor or Manager Responsibilities

- A. Work with Entity Privacy Official and appropriate authorities to investigate and provide due process for potential failures to follow applicable UW Medicine Privacy and Information Security policies or for a breach of patient confidentiality or information security.
- B. Report the final corrective action administered to the Privacy Office within 30 days of Privacy/Security Event Report being issued.

References:

- I. 45 CFR Parts 160 and 164; Section 164. 530(e) "Administrative Requirements – Sanctions"
 - II. 45 CFR Parts 164; Section 164.308(a)(1) (ii) (C) Sanction Policy
-
-

UW Privacy Officer: _____ Date: _____

Kathryn Waddell, Executive Director, Health Sciences Administration
