Information Security Policy

COMP.107

TABLE OF CONTENTS

Applicability: UW Medicine

Policy Title: Information Security Policy

Policy Number: COMP.107

Superseded Policies: SP-01 Electronic Data Policy
SP-02 Computing Device and Server Security Policy
SP-03 Workforce Member Policy

Date Established: June 21, 2019

Date Effective: August 19, 2022

Next Review Date: August 19, 2025

PURPOSE

This policy establishes UW Medicine requirements for protecting the confidentiality, integrity, and availability of electronic protected health information (ePHI).

This policy applies to UW Medicine workforce members (including faculty, employees, interns/trainees, contractors, volunteers and other persons who perform work for UW Medicine), devices, and information systems that access, use, maintain and transmit ePHI. ePHI is classified as confidential in accordance with University of Washington (UW) Administrative Policy Statement (APS) 2.6 Information Security Controls and Operational Practices.

DEFINITIONS

See UW Medicine Compliance Glossary.

POLICY

This policy and related standards, procedures and guidance are in place to ensure the confidentiality, integrity and availability of the ePHI UW Medicine creates, receives, maintains or transmits. This policy includes UW Medicine's administrative, physical and technical safeguards to prevent, detect, contain and correct security violations related to ePHI.

In order to manage the facilitation and implementation of activities related to the privacy and security of protected health information (PHI), UW Medicine has assigned information security responsibility to the Chief Information Security Officer (CISO). The CISO serves as the focal point for the information security compliance-related activities and responsibilities outlined in this policy.

UW Medicine follows the UW APS 2.4 Information Security and Privacy Roles, Responsibilities, and Definitions and UW APS 2.6 Information Security Controls and Operational Practices for data ownership and classification. When establishing security standards implementing this policy, UW Medicine may consider "recognized security practices" developed under section 2(c)(15) of the National Institute of Standards and Technology Act, the approaches promulgated under 405(d) of the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity under other statutory authorities.

I. Administrative Processes

UW Medicine implements reasonable and appropriate administrative safeguards to establish the foundation for UW Medicine's information security program.

A. Applications and Data Criticality Analysis

UW Medicine designates a tier classification based on the criticality and necessity of a system, helps to define its impact to business operations, including how the business continuity plan should be structured, and provides users with expectations of the computing device or server's performance.

Computing devices and servers must have a criticality assigned based on their importance to UW Medicine business operations and the overall risk to the enterprise.

B. Risk Analysis

UW Medicine conducts accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity and availability of its ePHI.

1. Any UW Medicine computing device or server that stores, transmits or processes ePHI must have a risk assessment documented. The UW Medicine workforce member/system owner is required to inform UW Medicine Information Security of their UW Medicine-owned computing devices/servers that store, transmit or process ePHI so that a risk assessment can be performed.

2. Risk assessments must be updated according to the UW Medicine Information Security Risk Assessment Standard requirements.

See the requirements in SS-02 Information Security Risk Assessment Standard.

C. Risk Management

UW Medicine implements security measures to reduce risks and vulnerabilities to a reasonable and appropriate level by:

1. Developing and implementing a risk management plan.

2. Implementing appropriate security measures:

    a. System owners are responsible for mitigation of the identified risks through implementation of security controls as approved through data governance processes.

    b. System owners of non-enterprise systems are only responsible for non-enterprise security controls.

3. Evaluating and maintaining security measures.

4. Documenting risk acceptance — Risks identified and classified[1] as "critical" or "high" must be mitigated. If mitigation is not possible, these risks must have a risk acceptance on file.

See the requirements in SS-06 Information Security Risk Management Standard.

UW Medicine Vulnerability Management Program, see SS-04 Vulnerability Management Standard.

D. Evaluation

UW Medicine conducts evaluations that consider the elements of the HIPAA Security Rule.

1. The tools used provide reports on the level of compliance, integration or maturity of a particular security safeguard deployed to protect ePHI.

2. The evaluations document known gaps between identified risks and mitigating security controls, as well as any acceptance of and justification(s) for risk.

3. The evaluations may be conducted with internal staff resources or external consultants. External expertise may be used to assist the internal evaluation team where additional skills and expertise is determined to be reasonable and appropriate.

E. Business Associate Contracts and Other Arrangements

See COMP.106 Use and Disclosure of Protected Health Information by Business Associates.

II. Integrity and Availability of ePHI

UW Medicine protects ePHI from improper alteration or destruction. This includes considering the various risks to the integrity of ePHI identified during risk analysis.

A. Security Incident Procedures

UW Medicine workforce members must report any suspected security events and security policy violations as soon as they are discovered. This includes any personally or UW Medicine-owned devices that are lost or stolen and have been used to connect with systems that have ePHI. Workforce members may have additional reporting requirements pursuant to contractual obligations.

[1] The Security Program Executive Committee (SPEC) maintains and sets the risk levels requiring mitigation.

Contact
UW Medicine Compliance: 206.543.3098 855.211.6193 comply@uw.edu *OR*
Harborview Medical Center (HMC) University of Washington Medical Center (UWMC) UW Physicians (UWP) Airlift Northwest (ALNW) 206.520.2200 mcsos@uw.edu University of Washington School of Medicine: 206.221.2459 domhelp@uw.edu Valley Medical Center (VMC): 425.228.3440 x6200 "ITHELP" in web browser or email

See UW Medicine Privacy, Confidentiality, and Information Security Agreement For Patient, Confidential, Restricted and Proprietary Information.

B. Contingency Planning & Operations

The UW Medicine contingency plan enables the continuation of critical business processes while protecting the integrity of ePHI while the organization operates in emergency mode.

1. Data Backup Plan
   There are accessible backups of ePHI and procedures to restore lost ePHI in the event of an emergency:
   a) ePHI must be backed up at a frequency that meets the business need for that data.

   b) ePHI retained on backup media must be encrypted when not in use.

2. Disaster Recovery Plan
   a) UW Medicine has contingency procedures that can be invoked for identified impacts, including emergency mode operation for systems with ePHI.

   b) The strategies used are adaptable to the existing operating environment and address allowable outage times and associated priorities.

3. Emergency Mode Operation Plan

Systems with ePHI that are used to provide clinical care must have operational and/or electronic procedures to support emergency mode operations, should the ePHI become lost or unavailable.

4. Contingency Plan Testing and Revision Procedures
   a. Managed computing devices and servers that contain ePHI must have a documented business continuity plan that outlines how business operations will continue in the event that the computing device or server fails.

   b. UW Medicine conducts checks of the data to ensure accuracy and validity.

C. Maintenance Records

UW Medicine documents repairs and modifications to the physical components of a facility that are related to the security of ePHI.

D. Facility Security Plan

1. UW Medicine controls physical access to the location where ePHI is stored, which includes the use of safeguards to prevent unauthorized physical access, tampering and theft.

2. UW Medicine takes appropriate measures to provide physical security for facilities and equipment that contain ePHI (facility access controls).

III. Information Access Control and Management / Identity and Access Management

Computing devices must use an authorization and authentication control that meets the Identity and Access Management Standard.

See the requirements in SS-07 Identity and Access Management Standard.

A. Person or Entity Authentication

UW Medicine computing devices use an authorization and authentication control that meets the Identity and Access Management Standard.

1. User access must be assigned using role-based access and must have the necessary authorization and authentication methods to restrict ePHI access to authorized users only.

2. UW Medicine requires that users know their passwords and, where implemented, also have a secondary method of authentication (e.g., a tap in/tap out token).

B. Access Control, Access Authorization and Validation Procedures

1. Access Control

    a. UW Medicine complies with the minimum necessary standard for information access management and provides role-based access to information systems that contain ePHI.

    b. UW Medicine workforce members are provided role-based access for UW Medicine information systems containing ePHI, as is required to perform their official job responsibilities and enabling UW Medicine to meet the minimum necessary standard.[2]

2. Access Authorization
   UW Medicine may provide non-workforce members with role-based access to UW Medicine information systems that contain ePHI when a business relationship or continuity of patient care creates the need for access (for example, Organized Healthcare Arrangement members, business associates, external healthcare facilities or professionals, regulators and auditors).

3. Authorization and/or Supervision
    a. Managers and workforce members (including faculty, employees, trainees, volunteers and other persons who perform work for UW Medicine) have obligations related to authorization and/or supervision of access to information systems containing ePHI. See section below entitled Roles and Responsibilities for additional information.

    b. Identity Access Management Systems are used to manage UW Medicine workforce member accounts and provide the level of access sufficient for the workforce member to perform their job functions. Access granted to UW Medicine workforce members must be documented.

4. Administrative Privileges
   UW Medicine workforce members who are granted administrator rights on managed computing devices must only use their administrator access to perform administrator level job functions.

    a. Workforce Clearance Procedure
       UW Medicine implements procedures to determine that the access of a workforce member to ePHI is appropriate.
    b. Access Control and Validation Procedures

[2] The minimum necessary standard is a key protection of the HIPAA Privacy Rule. It is based on the practice that PHI should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The minimum necessary standard requires UW Medicine to limit unnecessary or inappropriate access to and disclosure of PHI. See COMP.103 Use and Disclosure of Protected Health Information.

UW Medicine has centrally controlled unique usernames and passwords for each user and has established procedures to govern the release or disclosure of ePHI during an emergency.

c. Unique User Identification
UW Medicine assigns each account a unique user ID.

d. Automatic Logoff
Where feasible, UW Medicine employs controls that terminate an electronic session after a pre-determined time of inactivity.

e. Emergency Access Procedure
- UW Medicine has a process through the IT Services Help Desk to provide access in emergency situations.
- All workforce members that grant administrative privileges must have a procedure in place to add or remove those rights in case of an emergency (e.g., fire, vandalism, system failure and natural disaster).

f. Access Modification and Separation from UW Medicine
UW Medicine requires prompt removal or modification to the access of workforce members who have terminated or had job changes functions.

Additional resources regarding access:
- UW Medicine Privacy, Confidentiality, and Information Security Agreement For Patient, Confidential, Restricted and Proprietary Information
- COMP.002 Compliance Education and Outreach
- COMP.102 Safeguarding the Privacy and Security of Protected Health Information
- SS-01 Minimum Computing Device Security
- SS-03 Minimum Server Security Standard.

C. Workforce Security

1. Password Management
   a. UW Medicine workforce members are required to use strong passwords with their accounts. A strong password includes uppercase and lowercase letters, numbers, special characters, and must be a minimum of 8 characters in length.

   b. UW Medicine workforce members are responsible for changing the passwords of their assigned UW NetID and AMC/UW Medicine account that they use to perform UW Medicine business operations at least every 120 days.

2. Security Awareness, Training and Reminders
   a. UW Medicine develops and implements healthcare compliance education and training, including security reminders; creating, changing, and safeguarding passwords; log-in monitoring; and procedures to guard against, detect and report malicious software.

b. At each performance evaluation or credentialing, managers are to ensure that workforce members sign the UW Medicine Privacy, Confidentiality, and Information Security Agreement. The signed agreement is to be filed into the entity's appropriate personnel or academic record.

   See COMP.002 Compliance Education and Outreach.

3. Sanctions
   a. UW Medicine workforce members are personally responsible for ensuring the security of all ePHI to which they are given access.

   b. The sanctions for findings of noncompliance with privacy and information security policies will comply with COMP.006 Corrective Actions, which requires institutional officials to consider the following factors in determining what corrective actions are appropriate for workforce members: 1) prior violations and sanctions, 2) the nature, severity and extent of the violation; 3) whether the violation is a result of conduct that is intentional, willful or with reckless for the law; 4) terms and conditions of the workforce member's relationship with UW Medicine, as determined by constituent-specific policies, state regulations, conduct codes and applicable guidelines; and 5) whether or not the violation was self-reported (self-reporting does not exempt a workforce member from corrective action but will be taken into account).

IV. Workstation, Device and Media Security and Controls

A. Workstation Use

UW Medicine implements different ways workstations are accessed by both workforce members and non-workforce members. These physical safeguards and other security measures are designed to minimize the possibility of inappropriate access to ePHI through workstations.

B. Protection from Malicious Software

UW Medicine requires anti-malware security controls be installed on computing devices to minimize compromises to ePHI.

See the requirements in SS-01 Minimum Computing Device Security.

C. Encryption and Decryption

1. ePHI in transit (including text messages) must be encrypted or otherwise physically secured in a manner that prevents its theft or inappropriate use. This includes computing server-to-server communications via shared public networks.

2. ePHI at rest on any computing device (including mobile devices) that is used for UW Medicine business operations must be encrypted or physically secured in a manner that prevents unauthorized access.

Multiple UW Medicine Information Security Standards have encryption requirements dependent on device and activity (including Minimum Computing Device Security, Minimum Server Security, Electronic Communication, Identity, and Authentication).

D. Disposal

1. Media containing ePHI must be physically destroyed, securely overwritten or degaussed rather than using normal file deletion functions.

2. Computing devices must have all confidential ePHI rendered inaccessible prior to being transferred to an authorized University department for disposal. Personally owned devices must comply with the requirement prior to selling, disposing of or trading them in.

E. Media Re-use

UW Medicine requires the removal of ePHI from electronic media before the media is made available for re-use. This includes computing devices that are being re-allocated to another UW Medicine workforce member or retired to surplus.

F. Data Backup and Storage

1. Before equipment other than mobile computing devices that store ePHI is moved, UW Medicine requires a backup to be created and a record kept of its movements in and out of UW Medicine facilities.

2. Electronic ePHI data retained on backup electronic media must be tested for use and integrity on a regular basis.

V. Transmission Security

UW Medicine employs many methods to ensure transmission security of ePHI, including various types of encryption technology, data or message authentication codes, secure VPN and protocols. For integrity controls, UW Medicine validates that data transmissions have not been altered or shared between source and destination.

VI. Information System Activity Review

Computing devices and servers with ePHI log and monitor for unauthorized access, misuse of access and potential service-disrupting events.

A. Audit Controls, Logging and Monitoring

1. UW Medicine implements software and procedural mechanisms that record and examine activity in information systems that contain or use ePHI.

2. Event logs are reviewed for unauthorized access, misuse of access, and potential service disrupting events.

3. Event logs are retained according to the UW Medicine Records Management requirements.

REGULATORY/LEGISLATION/REFERENCES

- Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 160
- General Provisions, 45 C.F.R. § 164, Subpart A
- Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. § 164, Subpart C
- Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164, Subpart E
- Recognition of Security Practices, Pub. L. 116-321, 134 Stat. 5072.

PROCEDURE REFERENCES/LINKS

- UW Medicine Compliance Glossary
- COMP.002 Compliance Education and Outreach
- COMP.006 Corrective Actions
- COMP.106 Use and Disclosure of Protected Health Information by Business Associates
- 002.F1 UW Medicine Privacy, Confidentiality, and Information Security Agreement For Patient, Confidential, Restricted and Proprietary Information
- UW APS 2.4 Information Security and Privacy Roles, Responsibilities, and Definitions
- UW APS 2.6 Information Security Controls and Operational Practices
- UW Medicine Information Security Standards
- SS-01 Minimum Computing Device Security
- SS-02 Information Security Risk Assessment Standard
- SS-03 Minimum Server Security Standard
- SS-04 Vulnerability Management Standard
- SS-06 Information Security Risk Management Standard.
- SS-07 Identity and Access Management Standard
- UW Medicine Records Retention Schedule

ROLES AND RESPONSIBILITIES

Workforce Members

UW Medicine workforce members are responsible for the following:

- Completing the UW Medicine Privacy, Confidentiality, and Information Security Agreement before access is granted.
- Ensuring the privacy and security of ePHI to which they are given access.
- Being accountable for the ePHI on workstations, devices and media they use.
- Keeping accounts or passwords secure and not sharing this information with any other individuals (this does not apply to service accounts).
- Using accounts to log in only for oneself and not having other users log in for them.
- Changing passwords to accounts that allow access to ePHI every 120 days.
- Creating strong passwords with accounts. A strong password includes uppercase and lowercase letters, numbers, special characters and are at least 8 characters in length.
- Reporting any suspected security events and security policy violations as soon as they are discovered or suspected. This includes any personally owned or UW Medicine owned devices that are lost or stolen and have been used to conduct UW Medicine business operations.

Managers of Workforce Members

Managers of UW Medicine workforce members are responsible for all of the above AND the following:

- Authorizing role-based access to UW Medicine information systems containing ePHI for the workforce members supervised as required for the performance of the workforce members' official job responsibilities; while managers may execute this through a delegate, they still retain the authorization responsibility.

Information Technology (IT) Administrator Rights

IT administrators are responsible for all of the above AND the following:

- Using administrator access only to perform administrator level job functions.

System Owners / Departmental IT

System owners and departmental IT are responsible for all of the above AND the following:

- Classifying ePHI on servers as confidential in accordance with UW APS 2.6 Information Security Controls and Operational Practices.
- Ensuring servers that manage the information related to UW Medicine workforce member accounts have appropriate safeguards.
- Ensuring computing devices and servers, regardless of criticality, have the event logs monitored for unauthorized access and potential service disrupting events.
- Retaining event logs according to the UW Medicine Records Management requirements.

Enterprise IT

Enterprise IT is responsible for all of the above AND the following:

- Ensuring any computing device or server that stores, transmits or processes ePHI has a written risk assessment documented.
- Ensuring risk assessments are updated according to the UW Medicine Information Security Risk Assessment Standard requirements.

- Ensuring risks identified as a critical or high classification[3] are mitigated. If mitigation is not possible it must have a risk acceptance filed for it.

APPROVALS

/s/ Beth DeLair
Beth DeLair,
Chief Compliance Officer, UW Medicine
Associate Vice President for Medical Affairs, UW

9/14/2022
Date

[3] The Security Program Executive Committee (SPEC) maintains and sets the risk levels requiring mitigation.