
Department: UW Medicine Information Technology Services

Policy Number: SEC-06 Identity and Access Management Policy

Effective Date: June 11th, 2007

Review Date: April 27th, 2007

Purpose

This policy describes the requirements for identity and access management in order to safeguard the confidentiality, integrity, and availability of UW Medicine information and information systems.

Definitions

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

Policy

It is UW Medicines¹ policy to ensure systems are properly protected with appropriate access control measures based on the criticality of their systems and the data involved.

I. User Account Access Life Cycle Management

The life cycle of user account access includes user registration, account creation, user identity and account maintenance, and account de-activation.

A. User Registration

- The registration authority must verify users are who they claim to be before they are registered.
- Each user has one unique registration entry.
- User registrations are maintained permanently.

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.

B. User Account Creation

It is the workforce member's supervisor or supervisor's designee responsibility to fill out the form to request accounts and ensure that all users sign a *UW Medicine Privacy, Confidentiality, and Information Security Agreement*. It is also the supervisor or supervisor designee's responsibility to maintain an account of all direct reports account privileges and account status.

- Accounts are only created for registered users – No Shared Accounts are allowed.
- Accounts are created on systems based on the principles of minimum necessary, least privilege, and separation of duties.
- If a user requires administrator level access to systems or applications, a separate account for these administrative purposes is created.
- The System Owner must have and maintain a formal record, on all systems and applications containing ePHI, for all persons registered to use that information system, which must include the level of privilege provided.
- System Owner(s) must establish and maintain rules for role-based access within their systems. Role-based access is based on authorization from an account request by the workforce member's supervisor or supervisor's designee. Exceptions to defined role-based access must follow an established process and be clearly documented. When access is provided to non-workforce, these rules for role-based access must define relationships with partner, external providers, referrals, contractors, regulators and/or insurers. Where appropriate, Business Associate contractual language and/or a Memorandum of Understanding (MOU) must be in place.
- For all systems, users must be in control of their password(s). Systems must have the ability for the user to change their own password(s).

C. User Account Identity & Account Maintenance

During the life cycle of a user it is likely that there will be many changes relevant to access management.

- For any changes to the user role (and related access) or when a user transfers, it is the workforce member's supervisor or supervisor's designee responsibility to contact the providers of access.
- To maintain the requirements of minimum necessary and least privilege, when a user transfers, all accounts should first be

disabled, privileges removed, then accounts re-enabled and privileges added that are required in the user's new role.

- When an account will not be used for extended periods of time, the account should be disabled.
- All applications that contain ePHI must maintain a history of access changes for no less than 2 years. These records should include by whose approval the change was made.
- Where supported by technology, all passwords must be changed every 120 days.
- Password history should be maintained to limit the reuse of passwords.
- Passwords shall be a minimum of eight characters long and contain at least one special character and two of the following three character classes: upper case letters, lower case letters, and numerals where supported. Passwords should not be a word found in a dictionary or be "associated" with the user.
- UW Medicine Compliance will provide periodic reminders regarding password management to UW Medicine work force members.

D. User Account De-activation

It is the workforce member's supervisor or supervisor's designee responsibility to report separations for timely modification when workforce members are reassigned, promoted, or separated.

- At account deactivation time, retain information necessary to support required auditing logs. See system logging requirements in UW Medicine Information Security policy: *SEC-05 – Communications and Operations Management Policy*.
- Where technically feasible, systems must not re-cycle user-IDs because it may inadvertently provide inappropriate access.
- For Termination with cause, deactivation must occur immediately.

II. System and Application Access Controls

A. Authentication

All systems and applications must use encrypted authentication mechanisms.

- Authentication must be encrypted.
- Authentication credentials will not be coded into programs or queries unless they are encrypted, and only when no other reasonable option exists.

- Each user of a system that maintains “Restricted” or “Confidential” information must have a unique individual credential. No shared logins are permitted to access this type of information.

B. Authorization

The system or application should determine if the user has permission to perform requested operation.

C. Audit Trail

The system or application should record or write event details into a log file. See UW Medicine Information Security policy: *SEC-05 – Communications and Operations Management Policy*.

References:

- I. 45 CFR Part 164; Section 164.308(a)(3) (i) Workforce Security, (ii) (A) Authorization and/or Supervision, (B) Workforce Clearance Procedure, (C) Termination Procedures
- II. 45 CFR Part 164; Section 164.308(a)(4) (i) Information Access Management, (ii) (B) Access Authorization, (ii) (C) Access Establishment and Modification
- III. 45 CFR Part 164; Section 164.308(a)(5) (ii) (D) Password Management
- IV. 45 CFR Part 164; Section 164.310(a)(2) (iii) Access Control and Validation Procedures
- V. 45 CFR Part 164; Section 164.312(a)(1) Access Control, (2) (i) Unique User Identification
- VI. 45 CFR Part 164; Section 164.312(d) Person or Entity Authentication
- VII. International Organization for Standardization /International Electrotechnical Commission (ISO/IEC) 17799 Section 9 Access Control
- VIII. UW Information Systems Security Policy
- IX. Washington Information Technology Security Standards, Policy No: 401-S2

UW Medicine IT Services: _____ Date: _____

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