
Department: UW Medicine Compliance
Subject: PP-20a - Access Guide
Policy Number: 20a
Established Date: September 28, 2007
Revised Date: January 25, 2008, January 23, 2009
Review Date:

Audience

This document is intended for UW Medicine¹ workforce members with the following roles.

- Data Custodians (Individuals who have been designated as accountable for protecting the confidentiality of specific data that is transmitted, used, and stored on a system or systems within a department, college, school, or administrative unit of UW Medicine),
- User Access Administration,
- Privacy Officials,
- Compliance Officials,
- UW Medicine Information Technology Services Support for Online Services (Help Desk), **and**
- System Owners, System Operators, and Department Administrators/Managers.

Purpose

To meet minimum necessary requirements, access to UW Medicine enterprise-wide information systems that contain electronic Protected Health Information (PHI and/or ePHI) is role-based. This guide outlines the processes regarding:

- Making decisions regarding appropriate user access (including clearly defined PHI-sharing relationships with partners, external providers, referrals, contractors, regulators, researchers and insurers)
- The roles and responsibilities of groups and individuals within UW Medicine;
- Documentation of user roles and privileges;
- Processing any exceptions to established role-based access.

I. Roles & Responsibilities for Access to Enterprise Clinical Information Systems

A. Confidentiality and Access Work Group (CAWG)

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.

1. Approval body for definitions regarding role-based access to enterprise systems that contain PHI.
2. Provides guidance to all database and application owners regarding the minimum necessary access privileges for all roles within UW Medicine.

B. UW Medicine Information Security Program

1. Development, implementation and enforcement of practices related to identification, authentication, and administration.

C. UW Technology

1. Establishes and maintains the UW NetID.
2. Maintains email accounts in accordance with UW Medicine policies.
3. Maintains mainframe systems.

D. User Access Administration (UAA)

1. Maintains the user records in the Provider User Maintenance Authority (PUMA). The PUMA database provides the provisioning information to most enterprise-wide clinical systems and is database of all providers associated with UW Medicine.
 - Activates, Modifies, and Deactivates accounts.
 - Responds to PUMA database information requests.
2. Maintains the clinician record in cooperation with UW C&C.
3. Maintains the process that supervisors or their delegates use to create, modify, or deactivate user privileges.

E. EPIC Systems Group

1. Activates, Modifies, and Deactivates accounts within the Epic database.
2. Responds to Epic database information requests.

F. Provider Maintenance Group (PMG)

1. Responsible for maintaining, administering and providing data quality and integrity of provider information which is used to determine access to the clinical, financial and administrative systems of UW Medicine.
2. Maintains provider signatures for ORCA and MINDscape.
3. Reviews provider's access levels for enterprise systems and reports discrepancies to UAA.

G. System Owners & System Operators

1. Responsible for maintaining the functionality of their systems.
2. Responsible for informing data custodians of changes to functionality that impact the relationship of role to access. (For example: if new functionality is added or if there is a change to an existing level of access)
3. If system has PHI, must maintain documentation of the role-based access model as applied to that application.

H. Managers / Supervisors

1. Request activations, modifications, and deactivations for the workforce under their supervision.
 - Submit the request for job-related access to UW Medicine's User Access Administration (UAA), or other provisioning group.
 - If higher than normal access is requested for the user, the entity Privacy Officer must review and approve the exception before it is implemented.
 - Promptly report changes in end-user duties or employment status to interested enterprise access provisioning groups and any departmental system security administrators in order to keep system privileges up-to-date and restricted to current job requirements. Examples of reportable changes include promotion, extended leave and separation.
 - New user account:
https://info.medical.washington.edu/online/support_Forms/iris_new.asp
 - Modify existing user account:
https://info.medical.washington.edu/online/support_Forms/iris_change.asp
 - Account deactivation:
https://info.medical.washington.edu/online/support_Forms/iris_deactivation.asp
 - UWMC Epic maintains the following URL to facilitate account requests:
<http://depts.washington.edu/uwmcepic/>
 - HMC Epic maintains the following URL to facilitate account requests:
<http://depts.washington.edu/acshelp/schedule.html>
2. Maintains documentation of user privileges for the workforce under their supervision. (See Attachment PP-20a Attachment C Document IT Systems' Access for a Member of the Workforce)
3. Ensure appropriate education and training for the workforce under their supervision.

I. Users

1. Comply with UW Medicine policies and guidelines.
2. Protect against unauthorized access to accounts, privileges and associated passwords.
3. Maintain confidentiality of sensitive information to which they are given access privileges.
4. Accept accountability for all activities associated with individual user accounts and related access privileges assigned to them.
5. Report all suspected and known security or privacy violations to an appropriate authority (e.g. manager, supervisor, system administration, SIT or an entity Privacy Officer.)

II. Authorizing Users for Clinical Information Systems (for example, Epic, MINDscape, ORCA, and Reg/ADT)

A. UW Medicine Workforce Access²

UW Medicine workforce members are provided access to ePHI for the purposes of Treatment, Payment, and Health Care Operations based upon location, department, and job function as authorized by their Managers/Supervisors. UW Medicine provides access for research purposes as approved by IRB (see Section 1. F).

Practitioners (i.e. professionally licensed or certified individuals who provide patient care such as MDs, DOs, DPMs, optometrists, ARNPs, CRNAs, PA-Cs) who are credentialed by the Office of Medical Staff Appointments (OMSA) must be appointed to the medical staff before electronic access to clinical systems is granted. The access provided is based on job title, location, department and medical staff appointment criteria.

All Accreditation Council of Graduate Medical Education (ACGME) Residents and Fellows must be entered into UW Medicine's Graduate Medical Education's database (currently the Graduate Medical Education Tracking and Billing System - GMETABS) before electronic access to clinical systems is granted. The access provided is based on job title, location, department and medical appointment criteria.

Contracts for vendors and their respective personnel requiring access to any PHI are required to include Business Associate Agreement language (See UW Medicine Privacy Policy: *PP-12 Use & Disclosure of Protected Health Information by Business Associates*) prior to commencing any work. Whenever a vendor or contractor comes to work as a member of the workforce with individual departments, programs or support service areas, they are required to follow the same policies, procedures, and standards as other workforce members.

B. Organized Health Care Arrangements

The Seattle Cancer Care Alliance (SCCA) and Children's University Medical Group (CUMG) are in Organized Health Care Arrangements with UW Medicine. These arrangements allow SCCA and CUMG workforce members to have access to the UW Medicine enterprise clinical information systems for the purposes of joint treatment, payment, and health care operations. SCCA and CUMG both have designated individuals that submit all access requests for their respective users' credentials.

C. Contractual Agreements for Access to Electronic PHI

Under certain criteria, the Confidentiality and Access Work Group (CAWG) can approve other health care organizations to have access to enterprise clinical information systems. For each approved organization, UW Medicine Compliance

² "Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity." Title 45 C.F.R. § 160.103.

maintains the documentation of the allowed access. Users' privileges are granted according to the contractual agreement. (See UW Medicine Privacy Policy: *PP-20a Attachment A - Agreement for Electronic Access to PHI*).

D. Referring Providers

UW Medicine provides access to the enterprise clinical information systems through “ULink” authorized community providers for purposes of treatment. Each community provider signs a contract with the Physician Liaison Office. (See UW Medicine Privacy Policy: *PP-20a Attachment – UW Medicine U-Link Program Account Enrollment and Agreement Form*)

E. External Providers for Continuity of Care

UW Medicine provides access to the enterprise clinical information systems through appropriate mechanisms (specifying U-Link or Just-In-Time) to authorized community providers for purposes of continuity of care. Each community provider signs a contract with the Physician Liaison Office. (See UW Medicine Privacy Policy: *PP-20a Attachment – UW Medicine U-Link Program Account Enrollment and Agreement Form*)

F. Researchers

Researchers are granted access to PHI by authorization of their approved IRB studies. Research staff that are not UW Medicine workforce members are granted access to UW Medicine enterprise clinical information systems under an Agreement for Electronic Access to Protected Health Information. The terms of the Agreement for Electronic Access to Protected Health Information guide the handling of these users. An entity privacy officer must approve research access to an entity’s clinical information systems. When Researchers are provided access to the enterprise clinical information systems an end date must be put in the UAA database for termination of their access.

G. Other Non-UW Medicine Workforce

All other non-UW Medicine workforce member (i.e. auditors, insurers, regulators) access to enterprise clinical information systems must be approved by the entity Privacy Officer.

III. The following list documents the access that UW Medicine’s IT Services’ User Access Administration provides to users based on their department and job title.

Application	Description	Entity	PHI	VENDOR	Owner Dept.	Local Prov.	UAA-PUMA Prov.	UAA Manual Prov.
3M HDM System	The Health Information Management software used for coding for clinical services.	Enterprise	Y	3M	PDS		Y	
3M UM	HIM software used for utilization management for clinical services	Enterprise	Y	3M	PDS		Y	
A19 Reg	Runs on the UW/UNISYS Mainframe - available through pclRIS	Enterprise	Y	In-House	IT Services			Y
ACIS	Acuity Charge Information System - available through pclRIS	Enterprise	Y	In-House	IT Services		Y	

Accounting of Disclosures	Web-App for Data Upload & Reporting for disclosures of patient information	Enterprise	Y	In-House	IT Services	Compliance		
AMC Domain	A windows domain supported by IT Services	Enterprise		Custom	IT Services		Y	
ARE005	Application developed in-house which runs on the UW/UNISYS Mainframe for month-end processing.	Enterprise	Y	In-house	IT Services			Y
CHILD Profile	Tracks immunizations - available through pclRIS	Enterprise	Y	CHILD			Y	
CLePHI	PHI Access Tracking / Auditing database application for Compliance	Enterprise	Y	In-house	IT Services	Compliance		
Clinical Information Systems (CIS)	Multi-disciplinary documentation	UWMC	Y	Eclipsys	IT Services		Y	
Clinical Information Systems (CIS)	Multi-disciplinary documentation	HMC	Y	Eclipsys, Custom	HMC		File	
CORES	Computerized Rounding and Sign-out. Web application developed in-house and used primarily by residents	Enterprise	Y	In-house	IT Services	IT Services		
Epic	The Epic suite of applications includes registration and appointments for UW Medicine. Additionally, UWP, UWPN and other UW Medicine Outpatient Clinics use it for their Patient Electronic Medical Record and billing system.	Enterprise	Y		EPIC	IT Services		
MAP	MIND Access Project (MAP) is a report tool developed in-house to abstract aggregate data out of the MasterMIND repository.	Enterprise	Y	Custom	IT Services			Y
MINDscape	A web based application developed in-house that displays the clinical records of patients.	Enterprise	Y	Custom, reliant on Cerner for Transcripts, Allergies and Meds.	IT Services		Y	
MINDscape - ACE	Automated Charge Entry	Enterprise	Y	Custom	IT Services		Y	
MINDscape - ChIP/SMS	Chronic Illness Profile / Self management system	Enterprise	Y	Custom	IT Services		Y	
MINDscape - FlexNote	Document uploading into MINDscape	Enterprise	Y	Custom	IT Services		Y	
MINDscape - MasterMIND CROS	MasterMIND non-Web application	Enterprise	Y	Custom	IT Services		Y	
MINDscape - MasterMIND MDS	MasterMIND non-Web application - Minimum Data Set	Enterprise	Y	Custom	IT Services		Y	
MINDscape - Perinatal	MasterMIND non-Web application - Perinatal Tracking and Reports System	UWMC	Y	Custom	IT Services		Y	
MINDscape - RCE/A	Remote Charge Entry/Acuity	HMC	Y	Custom	IT Services		Y	
MINDscape - U-Link	MasterMIND Web-based Referring Provider application	Enterprise	Y	Custom	IT Services		Y	
ORCA INET	Multi-disciplinary inpatient and procedure documentation	Enterprise	Y	Cerner	IT Services		Y	
ORCA Retail Pharmacy	Outpatient Pharmacy	Enterprise	Y	Cerner	IT Services		Y	
ORCAMTM	Transcription	Enterprise	Y	Cerner	IT Services		Y	
ORCAPharmnet	Inpatient Pharmacy	Enterprise	Y	Cerner	IT Services		Y	
ORCAPowerchart	Results review, Powernote - documentation, CPOE	Enterprise	Y	Cerner	IT Services		Y	
ORCAProfile	Medical Records system, ROI	Enterprise	Y	Cerner	IT Services		Y	
ORCAProvision	Document imaging	Enterprise	Y	Cerner	IT Services		Y	
Pathology System	Pathology Information System -	Enterprise	Y	Tamtron	Pathology		Y	

	available through pciRIS							
Premis	Electronic Claims and Remittance	Enterprise	Y	National Data Corporation	IT Services			
Remote Charge Entry (RCEA)					IT Services		Y	
Reg/ADT	Registration, Admit, Discharge and Transfer application developed in house which is used by the medical centers for inpatient registration.	Enterprise	Y	Custom	IT Services		Y	
RiskMaster	Risk Management	Enterprise	Y	RiskMaster	IT Services	RiskMgmt		

IV. UW Medicine Department Systems.

Systems not included in Section III are provisioned by individual departments. Please contact the individual department to request user accounts.

V. Documentation of User Privileges

- A. UAA and System Owners are required to maintain records of the associated privileges for each role defined within their system.
- B. Department managers are required to maintain documentation on what systems their employees have access to. This documentation must be maintained in their personnel/academic file. The UW Medicine Document "IT Systems' Access for a Member of the Workforce" form can be used to document this access. (See Attachment PP-20a Attachment C Document IT Systems' Access for a Member of the Workforce)

VI. Exceptions to Established Access Privileges

A request for an exception to system access standards for a particular role must satisfy the following requirements:

- The user's manager must provide written justification of the need to the appropriate Privacy Officer:
 UWMC - Director of Health Information Management or UWMC Privacy Officer
 HMC - HMC Privacy Officer
 UWP - UWP Privacy Officer
 HHPCC - HHPCC Privacy Officer
 UW Medicine Sports Medicine - Sports Medicine Privacy Officer
- The appropriate entity's Privacy Officer must concur with you that you have a genuine business need AND sign off on your documented justification for access.
- The appropriate entity's Privacy Officer must send documented acknowledgement/approval to UAA.

UW Privacy Officer: _____ Date: _____

Johnese M. Spisso, Vice President for Medical Affairs, UW & COO UW Medicine
