

UW School of Dentistry Workforce Members Privacy, Confidentiality, and Information Security Agreement

It is the responsibility of all UW School of Dentistry workforce members to protect the privacy, security, and confidentiality of any information to which they are given access. All UW School of Dentistry workforce members (including faculty, employees, trainees, students, volunteers, and other persons who perform work for UW School of Dentistry) who utilize computing systems, resources, and data, are responsible for the confidentiality and security of their User ID (s) and Password(s) which provide access to University of Washington and/or UW School of Dentistry computer systems. It is also the responsibility of all workforce members to protect the confidentiality of the information they are provided using those credentials. Examples of access credentials are the UW Net ID and password and the axiUm login and password. **I understand and acknowledge the following:**

Policies and Regulations:

- I will comply with UW and UW School of Dentistry policies.
Privacy: <http://depts.washington.edu/comply/privacy.shtml>
Information Security: <http://security.uwmedicine.org/Policies/default.asp>
- I will support compliance with federal and state statutory and regulatory requirements (45 CFR Parts 160 and 164, American Recovery and Reinvestment Act of 2009 (ARRA) Health Information Technology for Economic and Clinical Health (HITECH) Act).
- I will report all known privacy violations to the UW School of Dentistry Compliance Program – 206 543-5331 or compliance@dental.washington.edu.
- I will report all suspected security events and security policy violations to my IT Support/Help Desk.

Confidentiality of Information:

- I will limit my access, use, and disclosure of patient information to the minimum amount necessary to perform my authorized activity or duty.
- I will maintain the confidentiality of all information, including patient information, confidential information, restricted information, and/or proprietary information to which I am given access privileges.
- I will use and/or disclose patient, confidential, or restricted information only as allowed by my job duties.
- I will only discuss patient, confidential, or restricted information in the work place and only with those who have a need-to-know and the authority to receive the information.
- I will take care to discuss patient, confidential, or restricted information in a private setting and not hold such conversations where they can be overheard by those without a need-to-know.

Inappropriate Use or Disclosure:

- I will report any improper access or disclosures to Compliance.
- I understand that my access will be monitored to assure appropriate use.

Computer Access Privileges:

- I will ensure that my use of UW & UW School of Dentistry computers, email, computer accounts, networks, and information accessed, stored, or used on any of these systems is restricted to authorized duties or activities.
- I will only use my UW, UW School of Dentistry or affiliates email account to conduct work related responsibilities and will not forward my email account or individual business related emails to a non-UW, UW School of Dentistry or affiliates email account (e.g. personal email account or other employer provided email account).
- I will not electronically access the records of any person if not an assigned or job-related duty.

- I will not electronically access the UW School of Dentistry or UW Medicine records of my family members, including minor children, except for assigned job related duties. This also applies in cases where I may hold authorization or other legal authority from the patient.
- I will protect access to patient and other job-related accounts, privileges, and associated passwords; for example:
 - Commit password to memory or stored it in a secure place;
 - Not sharing my password;
 - Not logging on for others;
 - Not making accesses or looking up information for others without proper authority.
- I understand that I will be held accountable for all accesses made under my login and password and any activities associated with the use of my account access privileges.
- I will only use my own credentials in accessing patient accounts and/or systems as provided to me for my job duties.
- I will log out or lock computer sessions prior to leaving a computer.

Computer Security:

- I will store all patient information, confidential information, restricted information, and/or proprietary information on secure servers, encrypted mobile devices, or other secure media.
- I will not change the computer configuration unless specifically approved to do so.
- I will not to disable or alter the anti-virus and/or firewall software.
- I will use only licensed and authorized software;
 - I will not download, install or run unlicensed or unauthorized software.
- I will use administrative permissions only when I am approved to do so and when required by job function;
 - If I perform system administrator function(s) I must use designated administrative accounts only for system administrative activities and use non-administrative user accounts for all other purposes.

I understand that failure to comply with this Privacy, Confidentiality, and Information Security agreement may result in disciplinary action up to and including termination of my status as a workforce member at the University of Washington. Additionally, the Department of Justice has the ability to levy criminal or civil penalties for inappropriate uses or disclosures of patient information.

By signing this Agreement, I understand and agree to abide by the conditions imposed above.

Print Name: _____

Department _____ Job Title: _____

Signature: _____ Date: _____

Copy provided on _____ by _____
Date Name supervisor, manager or designee Signature

- Provide copy of this Agreement to the workforce member.
- File original Agreement in departmental personnel or academic file.
(All signed Agreements must be maintained for 6 years)

The following table is a glossary of terms used in the Privacy, Confidentiality, and Information Security Agreement.

Policies and Standards References:

1. University of Washington Administrative Policy Statements (APS):
 - APS 2.4 Information Security and Privacy Roles, Responsibilities, and Definitions
 - APS 2.5 Information Security and Privacy Incident Management Policy
 - APS 2.2 Privacy Policy
2. UW Medicine Privacy Policies (adopted by The School of Dentistry): <http://depts.washington.edu/comply/privacy.shtml>
3. UW Medicine Information Security Policies & Standards (adopted by the School of Dentistry):
http://security.uwmedicine.org/policies/sec_policies.asp

Term	Definition
Access	To use, change, or view information.
Authorized duties or activities	Duties or activities that are established by those with appropriate authority related to the role or function of the workforce member, like a supervisor, manager or director.
Authorized software	Software that is authorized for use by the designated System Owner or Department Manager.
CONFIDENTIAL Information	CONFIDENTIAL Information is information that is very sensitive in nature, and requires careful controls and protection. Unauthorized disclosure of this information could seriously and adversely impact UW School of Dentistry or interests of patients, other individuals, and organizations associated with UW School of Dentistry. Examples include: personally identifiable information, patient information, workforce records, student records, social security numbers, legally protected University records, research data, passwords, intellectual property.
Confidentiality	Expectation that information will be protected from unauthorized use or disclosure.
Disclose	Release, transfer, provision of access to, or divulging information in any other manner outside the entity.
Licensed software	Software that the University of Washington has been granted permission from the owner to use under a written license agreement or contract.
Minimum amount of information necessary	Minimum Necessary Standard: When using or disclosing patient information, UW School of Dentistry must make reasonable efforts to limit patient information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. The minimum necessary standard does not apply to <ul style="list-style-type: none"> • Disclosures to or requested by a health care professional for treatment purposes • To the patient or pursuant to an authorization • Uses and/or Disclosures required by law • Uses or disclosures that are required for compliance with the HIPAA Privacy Regulations.
Protected Health Information (PHI)	Protected health information is a subset of individually identifiable health information maintained in permanent health records and/or other clinical documentation in either paper-based or electronic format.
Proprietary information	UW School of Dentistry possesses exclusive rights over the information within its systems. This includes business plans, intellectual property, financial information or other sensitive materials and information in printed, electronic or verbal form that may affect employee rights or organization's operations.
RESTRICTED Information	RESTRICTED Information is information that is business data, which is intended strictly for use by designated UW School of Dentistry employees and agents. This classification applies to information less sensitive than CONFIDENTIAL information. Dissemination of this information shall only be made to UW School of Dentistry workforce with an established need-to-know.
Workforce	Faculty, employees, trainees, volunteers, and other persons who perform work for UW School of Dentistry, and whose work conduct is under UW School of Dentistry's direct control regardless of whether or not the workforce member is paid by UW School of Dentistry.
UW Medicine	UW Medicine includes the following entities: Harborview Medical Center and clinics; UW Medical Center and clinics; Northwest Hospital & Medical Center and clinics; Airlift Northwest; Hall Health Primary Care Center; UW Physicians Sports Medicine Clinic; The Association of University Physicians d/b/a University of Washington Physicians; UW Medicine Neighborhood Clinics; Reference Lab; Collagen Diagnostic Lab; Molecular Diagnostic Lab; Summit Cardiology; Sports Medicine Group; Neurosurgical Consultants of Washington; The Seattle Arthritis Clinic; Richmond Internal Medicine; The Bone & Joint Center of Seattle; and Primary Care Partners Northwest, as well as certain services and activities that support UW Medicine that are performed by non-health care 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.
Use	The sharing, employment, application, utilization, examination, or analysis of information within UW School of Dentistry.