

**UW School of Dentistry Workforce Members
Privacy, Confidentiality, and Information Security Agreement
For Patient, Confidential, Restricted and Proprietary Information**

All UW School of Dentistry workforce members (including faculty, employees, students, trainees, volunteers, and other persons who perform work for UW School of Dentistry) are personally responsible for ensuring the privacy and security of all patient, confidential, restricted, and proprietary information to which they are given access including research data and student information (referred to throughout this document as protected information).

I understand and acknowledge the following:

Policies and Regulations:

- I will comply with UW and UW School of Dentistry policies governing protected information (School of Dentistry has officially adopted UW Medicine HIPAA policies).
 - Privacy: <https://depts.washington.edu/comply/privacy-policies/>
 - Information Security: <https://depts.washington.edu/uwmedsec/restricted/policies/>
- I will report all concerns about inappropriate access, use or disclosure of protected information, and suspected policy violations to UW School of Dentistry Compliance (206-543-5331 or dcomply@uw.edu).
- I will report all suspected security events and security policy violations to UW School of Dentistry Compliance (206-543-5331 or dcomply@uw.edu).

Confidentiality of Information:

- I will access, use, and disclose protected information only as allowed by my job duties and limit it to the minimum amount necessary to perform my authorized duties. I understand that my access will be monitored to assure appropriate use.
- I will maintain the confidentiality of all protected information to which I have access.
- I will only discuss protected information in the workplace for job-related reasons, and will not hold discussions where they can be overheard by people who have neither a need-to-know nor the authority to receive the information.
- I will keep patient information out of view of patients, visitors, and individuals who are not involved in the patient's care.
- I will keep protected information taken off-site fully secured and in my physical possession during transit, never leaving it unattended or in any mode of transport (even if the mode of transport is locked). I will only take protected information off-site if accessing it remotely is not a viable option.

Computer, Systems, and Applications Access Privileges:

- I will only access the records of patients for job-related duties.
- I will not electronically access the 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.
 - I will commit my password to memory or store it in a secure place;
 - I will not share my password;
 - I will not log on for others or allow others to log on for me;
 - I will not use my password to provide access or look up information for others without proper authority.
- I am accountable for all accesses made under my login and password, and any activities associated with the use of my access privileges.

- I will only use my own credentials as provided to me for my job duties in accessing patient accounts and/or systems.
- I will not forward my email account or individual business-related emails to non-UW or external email accounts.

Computer Security:

- I will store all protected information on secured systems, encrypted mobile devices, or other secure media.
- I will not change my UW computer configuration unless specifically approved to do so.
- I will not disable or alter the anti-virus and/or firewall software on my UW computer.
- I will log out or lock computer sessions prior to leaving a computer.
- 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), the designated administrative accounts will only be used for system administrative activities, and I will use non-administrative user accounts for all other purposes.
- If I use a personally-owned computing device for UW School of Dentistry business operations, I will not connect it to a UW School of Dentistry network unless it meets the same security requirements as a UW School of Dentistry-owned device.

My responsibilities involving protected information continue even after my separation from UW School of Dentistry and I understand that it is unlawful for former workforce members to use or disclose protected information for any unauthorized purpose.

Failure to comply with this agreement may result in disciplinary action up to and including termination of my status as a workforce member at the University of Washington. Additionally, there may be criminal or civil penalties for inappropriate uses or disclosures of certain protected information. By signing this Agreement, I understand and agree to abide by the conditions imposed above.

Note: UW SOD Faculty, Staff and Students are now required to sign this form electronically in the LMS <https://dental.washington.edu/compliance/compliance-training/>. Contact SODIT@UW.edu for more information.

Policy and Standards References

- 1) UW Administrative Policy Statements (APS): <http://www.washington.edu/admin/rules/policies/APS/TOC00.html>
 - a) APS 2.4 Information Security and Privacy Roles, Responsibilities, and Definitions
 - b) APS 2.5 Information Security and Privacy Incident Management Policy
 - c) APS 2.2 Privacy Policy
- 2) UW Medicine Privacy Policies: <https://depts.washington.edu/comply/privacy-policies/>
- 3) UW Medicine Information Security Policies & Standards: <https://depts.washington.edu/uwmedsec/restricted/policies/>