PP-04 Attachment A

Rev. 10/23/06

UW Medicine

Workforce Members

UW Medicine COMPLIANCE

Privacy, Confidentiality, and Information Security Agreement

As a user of UW & UW Medicine computing resources and data, I understand that I am responsible for the security of my User ID (login) (s) and Password(s) to any UW and/or UW Medicine computer system for which I am granted access. I understand that it is my responsibility to protect my password's confidentiality. I understand that I have the following responsibilities:

- Comply with UW and UW Medicine policies;
- Support compliance with federal and state statutory and regulatory requirements;
- Protect access accounts, privileges, and associated passwords (examples: Not sharing my password and Not logging on for others);
- Maintain the confidentiality of information to which I am given access privileges;
- Accept accountability for all activities associated with the use of my individual user accounts and related access privileges;
- Not to change the computer configuration unless specifically approved to do so;
- Not to disable or alter the anti-virus and/or firewall software;
- Not to download, install or run unlicensed or unauthorized software;
- Use only licensed and authorized software;
- Ensure that my use of UW & UW Medicine computers, email, computer accounts, networks, and information accessed, stored, or used on any of these systems is restricted to authorized duties or activities;
- If I have clinical systems access, I may access my own PHI;
- Workforce members may not access the records of their family members, including minor children, nor any other person if not an assigned or job-related duty. This also applies in cases where staff members hold authorizations or other legal authority from the Patient;
- Report all suspected security and/or policy violations to my Help Desk;
- Report all known privacy violations to the appropriate entity's Privacy Official or the UW Medicine Privacy Office

I understand that where I have access to or use of information classified as RESTRICTED or CONFIDENTIAL, additional protections are expected. Proprietary information, which includes business plans, intellectual property, financial information or other sensitive materials and information in printed, electronic or verbal form that may affect workforce member's rights or organizational operations, is an example of a RESTRICTED classification. Protected health information, which includes individually identifying patient information in any form, sensitive student information, and workforce records are examples of a CONFIDENTIAL classification.

I understand that any RESTRICTED and/or CONFIDENTIAL information collected or obtained from, analyzed, or entered into any UW Medicine information management system(s) or database(s) is the property of UW Medicine unless otherwise specified by contract. I understand that I must maintain and safeguard the confidentiality of any and all UW Medicine RESTRICTED and/or CONFIDENTIAL information accessed or obtained in the performance of my authorized duties or activities. I will not access, use, and/or disclose RESTRICTED and/or CONFIDENTIAL information for any purpose other than the performance of authorized activities or duties. I will limit my access, use and disclosure to the minimum amount of information necessary to perform my authorized activity or duty.

I will safeguard all RESTRICTED and/or CONFIDENTIAL information by holding it in the strictest confidence and by refusing to allow others to access information unless my authorized activities require that I do so. In such cases, I will disclose or allow access only to individuals having appropriate authority to access, receive and use such information.

I understand that my access to systems that have RESTRICTED and/or CONFIDENTIAL information may be monitored to assure appropriate access and compliance with system integrity. I understand that authorized use carries with it the responsibility to follow the UW Medicine Privacy and Information Security policies that govern the use of RESTRICTED and/or CONFIDENTIAL information, computers, and networks.

I understand that failure to comply with the above Privacy, Confidentiality, and Information Security agreement may result in disciplinary action up to and including denial of access to information and termination of my employment at the University to Washington. I have been given access to all of the UW Medicine Privacy and Information Security Policies:

http://depts.washington.edu/comply/privacy.shtml

http://depts.washington.edu/comply/security.shtml

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.

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 Medicine or interests of patients, other individuals, and organizations associated with UW Medicine. Examples include: personally identifiable information, protected health 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.
Individually identifiable patient information	Individually identifiable health information is information that is a subset of patient information, including demographic information collected from an individual, and: • That identifies the individual; or • With respect to which there is a reasonable basis to believe the information can be used to identify the individual. and (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
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 Protected Health Information, UW Medicine must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. The minimum necessary standard does not apply to • Disclosures to or requested by a health care provider 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.
Orally disclosed	Spoken words either in person or over any communication device.
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.
Privacy Official	Each entity within UW Medicine has designated a Privacy Official who assists the UW Privacy Officer in developing and implementing UW Medicine's policies and procedures. The entity Privacy Official may identify or appoint designee(s) to assist in the performance of these functions.
Proprietary information	UW Medicine 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 Medicine employees and agents. This classification applies to information less sensitive than CONFIDENTIAL information. Dissemination of this information shall only be made to UW Medicine workforce with an established need-to-know.
Safeguard	Protect or cover from exposure, using precautionary measures.
Workforce	Faculty, employees, trainees, volunteers, and other persons who perform work for UW Medicine, and whose work conduct is under UW Medicine's direct control regardless of whether or not the workforce member is paid by UW Medicine.
UW Medicine	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; 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 and the University of Washington Health Care Components are subject to the UW Medicine Information Security Program.