UW Medicine

Workforce Members
Privacy, Confidentiality, and Information Security Agreement
For Patient, Confidential, Restricted and Proprietary Information

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

I understand and acknowledge the following:

Policies and Regulations:

- I will comply with UW and UW Medicine policies governing protected information.
  - Patient Information Privacy Policies: https://depts.washington.edu/comply/privacy-policies/
  - UW Administrative Policy Statements: https://washington.edu/admin/rules/policies/APS/TOC00.html
- I will report all concerns about inappropriate access, use or disclosure of protected information, and suspected policy violations to UW Medicine Compliance (206-543-3098 or comply@uw.edu).
- I will report all suspected security events and security policy violations to the UW Medicine ITS Security team (mcsos@uw.edu) and my entity-specific IT support desk.

Confidentiality of Information:

- I will access, use and disclose protected information and limit it to the minimum amount necessary to perform my authorized job duties. I understand that my access will be monitored to assure appropriate use.
- I will maintain the confidentiality of all protected information that I have access to.
- 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 protected information out of view of patients, visitors and other individuals who are not involved in the patient's care.
- I will use UW Medicine resources, including computers, email, photographic, or audiovisual equipment for job-related duties or under conditions permitted by institutional policy.
- I will only take protected information off site with my manager's prior approval and keep it secured and in my physical possession during transit. I will never leave protected information unattended or in any mode of transport even if the mode of transport is locked.

Computer, Systems, and Applications Access Privileges:

- I will only access UW Medicine clinical systems to perform my authorized job duties and will only use my own usernames and passwords. I am accountable for all accesses made under my login and password.
- I will only access my own or a family member's PHI as permitted under my employer 's approved process or for job related duties.
  - I will not use clinical information systems to access my own or a family member's PHI for personal reasons if I am a VMC workforce member. I may only use MyChart or make a request through the VMC Release of Information (ROI) process.
  - Unless I am a VMC workforce member, I may access my own PHI in UW Medicine clinical information systems for personal reasons. I may only access the PHI of an adult family member for personal reasons if my family member signs a HIPAA authorization form granting me electronic access to their PHI and it is submitted to the applicable HIM department before accessing their PHI. I may only access the PHI of family members under the age of 18 through MyChart or by making an ROI request to the applicable entity.
  - I will not use Epic Care Everywhere for personal reasons.

- 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 in for others or allow others to log in for me;
  - I will not use my password to provide access or look up information for others without proper authority.
- I will not forward my email account or individual work-related emails containing protected information to unapproved email domains. The UW Medicine Approved Email Domain list: https://depts.washington.edu/uwmedsec/restricted/guidance/encryption/approved-email-domains/. VMC workforce will follow entity-specific protocols and policies found on MyValley.

Computer Security:

- I will store all protected information on secured systems, encrypted mobile devices, approved third party applications or other secure media.
- I will not change my computer configuration or perform any action that might circumvent authentication or security on any UW Medicine system without prior approval.
- I will not disable or alter my UW Medicine workstation's antivirus or firewall software.
- I will log out or lock computer sessions prior to leaving my workstation unattended.
- 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 will ensure that my personally-owned computing devices are secured according to UW Medicine's information security requirements before using them to perform UW Medicine business operations.
- I will ensure that protected information is removed from any media or computing devices prior to disposal, or that the media or computing devices are securely destroyed.

My responsibilities involving protected information continue even after my separation from UW Medicine 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. 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.

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)