haring center

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

All Haring Center employees working in ITP 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 policies governing protected information
    - Website: http://depts.washington.edu/comply/patient_privacy/
- 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 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 use UW resources, including computers, email, photographic, video, audio or other recording equipment only for job-related duties or under conditions expressly permitted by applicable institutional policy or law.
- 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 only access my own PHI through my entity approved process or for job related duties.
    - Accessing the records of family members is not allowed for non-job related duties without an authorization from the patient for electronic access by their workforce family member.
- 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 in accessing patient accounts and/or systems as provided to me for my job duties.
- Outlook is the only approved email domain. I will not forward my email account or individual work-related emails containing protected information to unapproved email domains including Gmail.

Computer Security:

- I will store all protected information on secured systems, encrypted mobile devices, or other secure media.
  - Any documents containing patient data must be stored locally on your computer.
  - Documents containing patient data must NOT be stored on the shared drive.
  - ITP employees may share documents containing patient data using OneDrive.
- 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 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.
- If I use a personally-owned computing device Haring Center business operations, I will not connect it to a Haring Center network unless it meets the same security requirements as a Haring Center-owned device.

My responsibilities involving protected information continue even after my separation from the Haring Center, 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: _____ Job Title: _____
Signature: _____ Date: _____
Name of supervisor, manager or designee: _____
Signature of supervisor, manager or designee: _____

☐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)