

Patient Care Services Credentialing at UW Medical Center

Attestation Application: YOUR APPLICATION WILL NOT BE APPROVED IF NOT COMPLETE

Step 1 - Your information, checklist of required documents & proposed role description

- Applicant full name.

- Applicant job title & employer organization.

- Contact phone & email. Please provide a reliable contact as well as a backup contact number, as you will be required to provide a copy of your file **within 24 hours** of our call or email.

I am responsible for:

- HIPAA training per employer.

- Immunizations per UWMC Employee Health and (CDC) guidelines:
Annually updated documentation of immunity to tuberculosis, measles, mumps, rubella, varicella, hepatitis B, pertussis. Proof of an initial COVID-19 vaccine series and a bivalent booster administered after 9/2022. Call (206) 598-4848 with specific questions.

- Annually updated confidentiality form, attached.

- Photo ID Worn While at UWMC:
For UW/UW entity personnel (e.g. Harborview, Valley Medical Center, Airlift NW, UW School of Medicine departments, UW School of Pharmacy, UW School of Public Health, and colleagues at Fred Hutch Cancer Center), upon approval you will wear the photo ID badge issued by your employer. Photo ID is to be worn at all times in the Medical Center.

OR

- For Non-UW/UWM entity personnel** (e.g. Puget Sound Blood Center, Kaiser, Seattle Children's, VA, Puget Sound Health Care System), upon approval you will obtain a UWMC photo ID badge from Public Safety. Photo ID is to be worn at all times in the Medical Center.
Contact with Public Safety with specific questions by calling (206) 598-4909.

- A background check is required for all non-UW/UWM entity personnel. Complete the Criminal Background Authorization attached.

My proposed role at UWMC:

RESEARCH.

CLINICAL PRACTICE.

LICENSURE:

If proposed role requires licensure then you must have record of current licensure or certification with the State of Washington.

Note: Medical Assistant - phlebotomist is required by law for venipuncture.

[Washington State Health Medical Assistants](#)

My proposed role requires CURRENT LICENSURE with the State of Washington.

License type

License number

Expiration

ROLE ACTIVITIES.

Research non-clinical: recruit patients, obtain consent, administrate surveys, interview patients, data/record review, chart in patient record.

Other activities with patients: including physical assessment, culture swab, etc. Please specify.

Clinical practice:

Blood draw.

Venous: from central venous access, peripheral venous access, venipuncture.

Arterial: from indwelling line, arterial puncture.

Invasive procedures (describe).

Medication administration (list meds).

Other (describe).

Work Area When On-site at UWMC:

7S General Clinical Research Center.

Other areas (please specify).

Step 2 - Your manager's information & signature

Required Signature:

I attest that the applicant is competent to perform the proposed role as described.

I understand that I may need to produce a copy of the documentation above **within 24 hours** upon request by University of Washington Medical Center, Patient Care Services Administration.

Access to Patient Records:

If access to electronic medical records is applicable to the applicant's role, it is my responsibility as Manager to contact the UW Medicine Online Information Portal.

Employee Manager:

Print full name

Signature & date

Organization/Phone/Email

Step 3 - Your signature

Required Signature:

I attest to the truth and accuracy of the information provided. I understand that my file may be audited and that I may be required to provide proof of HIPAA training, immunization records, a signed confidentiality agreement and proof of current licensure **within 24 hours** upon request by University of Washington Medical Center, Patient Care Services Administration.

Signature & date

Step 4 - Submission of application & retention of records

Email as PDF attachments ONLY the signed *Attestation Application, Criminal Background Authorization Form* (if applicable) and **A COPY OF YOUR COVID-19 VACCINATION CARD** to University of Washington Medical Center, Patient Care Services Administration. Paper applications and incomplete applications will NOT be accepted.

Please allow at least 2 weeks for processing.

Retain these records in your employee file. ***You are responsible for maintaining and keeping these records current.*** Your file may be audited and a copy must be provided to University of Washington Medical Center, Patient Care Services Administration ***within 24 hours*** of our call or email.

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.
 - 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 Medicine 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.
 - Except for VMC, workforce members who have access to UW Medicine clinical information systems may access their personal PHI. VMC workforce members may only access their personal PHI using [MyChart](#) or the VMC Health Information Management (HIM) Release of Information process.
 - 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. The authorization must be submitted and processed through the applicable HIM department. VMC workforce members may NOT access family members' electronic medical records; they must use the VMC HIM process.
- 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;

UW Medicine

- 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.
- 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/email-encryption/approved_email_domains/.
Valley Medical Center workforce will follow entity-specific protocols and policies found on My Valley.

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 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 for UW Medicine business operations, I will not connect it to a UW Medicine network unless it meets the same security requirements as a UW Medicine-owned device.

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)

Policies and Standards References:

1. UW Administrative Policy Statements (APS): <http://www.washington.edu/admin/rules/policies/APS/TOC00.html>
 - APS 2.4 Information Security and Privacy Roles, Responsibilities, and Definitions
 - APS 2.5 Information Security and Privacy Incident Reporting and Management Policy
 - APS 2.2 University Privacy Policy
2. UW Medicine Compliance, HIPAA/Patient Privacy Policies: http://depts.washington.edu/comply/patient_privacy/