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 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.

UW Medicine

- 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/resources/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: School of Medicine Job Title: Visiting Medical Student

Signature: _____ Date: _____

Copy provided on  by Laura Ellis _____

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/

Please review the University of Washington School of Medicine Essential Requirements of Medical Educaion: Admission, Retention, Promotion, and Graduation Standards before signing below.

****

APPLICANT/STUDENT ACKNOWLEDGMENT OF REVIEW

Name: _____ Date: _____

I have read and understand the expectations for successful completion of the MD degree described in the following documents and can meet these with or without accommodations (please initial each line):

_____ Essential Requirements of Medical Education

_____ Technical Standards Expanded Examples

_____ UW School of Medicine's Foundations of Clinical Medicine's Physical Examination Checklist

_____ Services available through the UW Office of Disability Resources for Students

Before signing this acknowledgment of review, if you have any questions about the School of Medicine's Essential Requirements and Technical Standards and/or the process for requesting accommodations, please contact the School of Medicine's Office of Admissions, Student Affairs, or Disability Resources for Students.

Applicant or Medical Student Signature Date

****

Rev. 12/2013
Rev. 09/1/15

UW Medicine

UW Medicine
Temporary Workforce Member/Student HIPAA Self Study

UW Medicine is committed to protecting patient privacy and maintaining this information securely. UW Medicine has compiled this Student Self Study to assist your understanding of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), rules on Privacy, Security, and Transaction Code Sets that began to be enforceable in April 2003.

UW Medicine Compliance serves as a resource for HIPAA compliance.

UW Medicine Compliance
Box 358049
Seattle, WA 98195-8049
206.543.3098
comply@uw.edu

The penalties for violating HIPAA can lead to individual or organization fines, jail time, and/or disciplinary action up to and including termination. Additionally, the Department of Justice has the ability to levy criminal or civil penalties for inappropriate uses or disclosures of patient information.

It is essential that everyone who has access to and handles patient information fully understand their responsibility under HIPAA both to avoid personal liability and to protect UW Medicine.

The **Privacy Rule** establishes a federal standard of privacy protection for information about patients and defined Protected Health Information (PHI).

PHI includes things such as:

- *any information about the patient's physical or psychological condition*
- *all the information in the patient's medical record*
- *the patient's name, address, or birth date, social security number, and other personal demographics*
- *any other information that might reveal something about the patient's situation (for example, the charges on a patient's billing account, the name of the clinic where the patient is being treated, the reason the patient has made an appointment or is in the hospital, etc.)*

Such information may exist in written, electronic, verbal, or any other form.

It is the responsibility of each of us to protect the confidentiality of patient information.

The **Security Rule** focuses on keeping patient health information safe; limiting access to health information; and ensuring that information does not go out to the wrong people. Each member of the UW Medicine workforce has responsibilities for Information Security based upon their specific role(s). To protect the security of patient information, you are asked to follow certain safeguards.

The Office for Civil Rights (OCR) oversees and enforces the HIPAA Privacy Rule and Security Standard.

The **Employer Identifier Standard** requires that employers have standard national numbers that identify them on standard transactions. The Employer Identification Number (EIN), issued by the Internal Revenue Service (IRS), was selected as the identifier for employers.

The **Transactions and Code Sets Rule** directs that claims submissions and other transactions among healthcare entities be done electronically, according to certain federal standards.

The Center for Medicare & Medicaid Services (CMS) oversees and enforces the HIPAA Transactions and Code Sets Rule.

UW MEDICINE PRIVACY POLICIES

UW Medicine has policies and procedures to facilitate the protection of patient information and compliance with HIPAA regulations and Washington State Law. HIPAA does not affect state laws that provide additional privacy protections or greater access for patients. The confidentiality protections are cumulative; and when state law requires a certain disclosure -- such as reporting an infectious disease outbreak to the public health authorities -- the federal privacy regulations do not preempt the state law.

Appropriate corrective actions will be applied to workforce members (including trainees) who fail to comply with these policies and procedures. Corrective actions are based upon the relative severity of the violation. Corrective action is up to and including termination of your status as a workforce member at the University to Washington.

You may view the policies in their entirety at the following website:

http://depts.washington.edu/comply/patient_privacy/

Below is a summary of the core policy information you need to know before working, training or observing at UW Medicine:

Every patient who receives care at UW Medicine receives our Notice of Privacy Practices. This Notice explains the rules we follow when using or disclosing patient information. Please pick up a copy of the Notice in the main lobby so that you are familiar with UW Medicine practices.
UW Medicine includes many entities 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 COMP.101 Patient Information Privacy and Security Compliance Program and Administrative Requirements (http://depts.washington.edu/comply/comp_101) and 101.G1 University of Washington HIPAA Designation (http://depts.washington.edu/comply/docs/101_G1.pdf). UW School of Medicine is subject to the UW Medicine Information Security Program. Within these entities, patient information may be shared for treatment, payment and healthcare operations (TPO). Patient information may not be shared with the non-healthcare components of the University without patient authorization unless it is with a non-health component that supports the treatment, payment or healthcare operations of UW Medicine. UW Medicine may share patient information with any non-UW Medicine healthcare professional for treatment purposes. That is, to facilitate continuity of care, different healthcare professionals who are involved in treating the patient may communicate about the patient's medical care. When using or disclosing patient information for payment and healthcare operations, healthcare professionals may only disclose to non-UW Medicine entities the minimum necessary patient information required to accomplish the intended purpose.

UW Medicine may use or disclose patient information to relatives or other persons involved in the treatment or care of the patient, provided the patient does not object. When a patient is unable to express his or her wishes, the caregiver should exercise professional judgment on whether or not to release any patient information. If a disclosure occurs under these circumstances, UW Medicine will let the patient know of the disclosure as soon as possible.

UW Medicine may disclose patient information to a business associate that is performing an activity on its behalf (such as a consultant) when UW Medicine obtains satisfactory assurance that the business associate will safeguard the information. Such assurances are documented in writing

through a business associate agreement. Relationships between healthcare professionals involving the treatment of a patient do not require such agreements.

Outside of treatment, payment or healthcare operations, UW Medicine may use or disclose patient information without an individual's authorization for the following:

- public health activities
- health oversight activities
- specialized government functions
- to avert a serious threat to the health or safety of any person
- to law enforcement when required to do so by law
- pursuant to legal process

Other than the list above, or for treatment, payment or healthcare operations reasons, the use or disclosure of patient information must be authorized in writing by the patient.

Upon admission, patients have the opportunity to decide whether or not to be included in the hospital's inpatient directory. If a patient opts against being included in the directory, UW Medicine will not include the patient in the directory, and therefore cannot acknowledge the presence of the patient in response to inquiries. If a patient opts to be included in the directory, UW Medicine may release the condition and location of the patient when a requestor asks for the patient by name. With permission of the patient, clergy of the same faith as the patient may be given directory information without asking for a patient by name.

Psychotherapy notes maintained by behavioral health providers are a subset of patient information subject to heightened confidentiality protections. Without the patient's authorization, such notes may **only** be used or disclosed to conduct UW Medicine training programs, for treatment by the behavioral health professional, to defend against legal action, to protect the health or safety of any person, or when required by law. If you work or train in an area that might create Psychotherapy notes, please ask your manager for more information about the use of psychotherapy notes.

Research involving human subjects (either directly or indirectly through patient information) requires review by an approved Institutional Review Board (IRB). Researchers may use or disclose patient information for research **only** when authorized by the human subject, or pursuant to an IRB-approved waiver of authorization.

As someone who may have direct contact with patients, you should be aware that patients with have certain rights regarding their medical information. These rights, listed in our Notice of Privacy Practices, are generally initiated with the help of the UW Medicine Compliance.

Patients have the right to:

- Request restricted use of their health information.
- Request that UW Medicine not disclose their health information to their health plan for those items or services that they pay in full.
- Request UW Medicine to contact them in an alternate way.
- View and receive copies of their health record.
- Request for an amendment (change or addition) to their record.
- Request for a list of disclosures of their health information.
- File a complaint about how UW Medicine and individual healthcare professionals use or disclose their patient information. Complaints may be made to the UW Medicine Compliance, the individual UW Medicine entity, or the Office for Civil Rights (OCR). If any person complains to a member of the UW Medicine Workforce about a use or disclosure of patient information, the workforce member must contact the UW Medicine Compliance immediately. UW Medicine will not retaliate, or tolerate retaliation, against any one who files a complaint.

Your Role In Protecting Patient Privacy

The protection of patient information ultimately depends on the actions of each and every person who has legitimate access to this information. You will likely encounter patient information during your time at UW Medicine. Following is a list of the things you as an individual must do to protect patient information:

- Access, provide, and use patient information only for job or study-related reasons.
- Access or provide only the minimum information needed.
- Only share/disclose information on a legitimate "need to know" basis.
- When you must discuss patient information, do so in private or speak softly to lessen the chance that others will overhear.
- Maintain the confidentiality of information to which you are given access privileges;
- If you have clinical systems access, may access your own patient information but must comply with state restrictions on use of state resources for private purposes.
- 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.
- Secure or logoff of applications when you leave a workstation.
- Keep printed materials and computer screens containing patient information from public view.
- Dispose of documents containing patient information properly - in a secure recycling bin.
- Follow guidelines for using email, fax machines and for leaving patient phone messages.
- Patient information taken off site must be kept fully secured, remain in the workforce member's physical possession during transit, never left unattended, and never left in any mode of transport (even if the mode of transport is locked).
- Report all known privacy violations (examples: improper access or disclosures) to UW Medicine Compliance at 206.543.3098 or comply@uw.edu.

UW Medicine Information Security Policies, Standards & Guidelines

UW Medicine has policies, standards, and guidelines to facilitate information security and compliance with HIPAA regulations and Washington State Law. These information security policies apply to any individual who uses a computer connected to UW Medicine networks or who has been granted privileges and access to UW Medicine computing, network services, applications, and/or resources.

You may view the policies in their entirety at the following website:

https://depts.washington.edu/uwmedsec/

Check with your organization's Information Security unit for entity-specific policies.

UW Medicine information security policies and standards impose the following user responsibilities: Any individual who uses a computer connected to UW Medicine networks or who has been granted privileges and access to UW Medicine computing, network services, applications, and/or resources.

- Comply with UW and UW Medicine policies.
- Support compliance with federal and state statutory and regulatory requirements.

- Report all concerns about inappropriate access, use or disclosure of protected information, and suspected policy violations to your IT Support/Help Desk.

Confidentiality of Information:

- Limit your access, use, and disclosure of patient information to the minimum amount necessary to perform your authorized activity or duty.
- Maintain the confidentiality of all information, including patient information, confidential information, restricted information, and/or proprietary information to which you are given access privileges.
- Use and/or disclose patient, confidential, or restricted information only as allowed by your job duties.
- Discuss patient, confidential, or restricted information in the work place only with those who have a need-to-know and the authority to receive the information.
- Take care to discuss patient, confidential, or restricted information in a private setting and not hold such conversations where they can be overheard by those without a need-to-know.

Computer Access Privileges:

- Ensure that your 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 or under conditions expressly permitted by applicable institutional policy or law.
- Use your UW, UW Medicine or affiliates email account only to conduct work related responsibilities and not forward UW email account or individual business related emails to a non-UW, UW Medicine or affiliates email account (e.g. personal email account or other employer provided email account).
- Never electronically access the records of any person if not an assigned or job-related duty.
- Never electronically access the UW Medicine records of family members, including minor children, except for assigned job related duties. This also applies in cases where there is an authorization or other legal authority from the patient.
- Protect access to patient and other job-related accounts, privileges, and associated passwords; for example:
    - Commit password to memory or stored it in a secure place;
    - Not sharing password;
    - Not logging on for others;
    - Not making accesses or looking up information for others without proper authority.
- Be accountable for all accesses made under UW Medicine login and password and any activities associated with the use of account access privileges.
- Use credentials to access patient accounts and/or systems as provided only for job duties.
- Log out or lock computer sessions prior to leaving the computer.

Computer Security:

- Store all patient information, confidential information, restricted information and/or proprietary information on secure servers, encrypted mobile devices (examples include: laptops, netbooks, smart phones, USB flash drives, iPads), or other secure media.
- Never change the computer configuration unless specifically approved to do so.

- Never disable or alter the anti-virus and/or firewall software.
- Use only licensed and authorized software;
    - Never download, install or run unlicensed or unauthorized software.
- Use administrative permissions only when approved to do so and when required by job function;
    - Use designated administrative accounts only for system administrative activities and use non-administrative user accounts for all other purposes.

Safeguarding Patient Information:

- Safeguard patient information at all times (on and off-site).
- Verbal:
    - Hold discussions about patient information in areas where patients, visitors, and workforce members who are not involved in the patient's care cannot overhear and speak in a controlled volume.
    - Only discuss patient information in the appropriate workplace setting and only with those who have a need-to-know and the authority to receive the information.
- Paper:
    - Never leave patient information unattended in exam rooms or work areas.
    - Patient information taken off site must be kept fully secured, remain in the workforce member's physical possession during transit, never left unattended, and never left in any mode of transport (even if it is locked).
    - Patient information taken off site must be secured at that location, stored in a suitable locked receptacle when not in use or unattended, and removed from printers immediately.
    - Disposal of patient information must be done in a secure and confidential manner.
- Electronic Data:
    - Workforce members that use mobile computing devices (e.g. laptops, tablet computers, PDAs, smart phones) or mobile data storage devices (e.g. floppy disks, CDs, DVDs, flash memory, portable hard drives) are responsible for the protection of the data on those devices. This responsibility includes the use of encryption.

Workforce members who are assigned to multiple UW Medicine departments and/or business units are required to follow all specific policies, guidelines, and procedures established by those departments or units.

UW Medicine
HIPAA Student Self Study
Signature Page

The preceding materials are for the student to keep.

This signature page for the UW Medicine HIPAA Student Self Study is to be removed from the document and turned in to your manager.

Date: _____

Signature: _____

Print Name: _____

Name of Manager: _____

Department: _____

Manager:

☐ **File original in departmental personnel file.**

UW Medicine
SCHOOL OF MEDICINE

University of Washington School of Medicine

Required Background Check for Admission and Continuation
Request for Criminal History Information
Self-Disclosure, Consent, and Release of Information

The Washington State Child and Adult Abuse Information Act (RCW 43.43.830 through 43.43.845) requires that certain individuals who have access to children under sixteen years of age, developmentally disabled persons, and vulnerable adults, disclose criminal history information. This criminal history information includes certain crimes against children and other persons, related to abuse of these populations, and crimes relating to financial exploitation. They do not include offenses such as traffic violations. In addition, the law includes requirements for background checks through the Washington State Patrol (WSP) concerning these crimes and offenses.

The University of Washington School of Medicine (UWSOM) medical degree requirements include rotations at clinical training sites that require a WSP and other background check information. Admission to the UWSOM is contingent upon satisfactory completion of this and other criminal background checks. Additional background checks will be done every two years to remain compliant with UWSOM policy.

Castle Branch, Inc. is requesting the WSP check on the UWSOM's behalf. **Please complete this Self-Disclosure, Consent, and Release form and upload all pages to your application in VSAS.** A copy of the WSP response will be available to you through Castle Branch, Inc.

Consent and Release of Criminal Background Check

I authorize background checks, including any repeat checks as necessary, through Castle Branch, Inc. and the Washington State Patrol, that are necessary for my admission as a Visiting Student at the University of Washington School of Medicine. I authorize the release of my self-disclosure information all background check results and any information provided by me related to the background checks, to the University of Washington School of Medicine and to clinical training sites, whether in or outside the state of Washington, as deemed necessary by the School of Medicine.

Name: _____

Signature: _____

Date: _____

Please select:

☐ Newly Accepted UWSOM Student

☐ Current UWSOM Student

☐ Visiting Student

CRIMINAL HISTORY INFORMATION – SELF DISCLOSURE

Name: _____ Date of Birth: _____
(please print) Last First MI

For the questions below, please circle either 'yes' or 'no.'

Have you ever been convicted in any jurisdiction of any of the following crimes?

Aggravated murder; first or second degree murder; first or second degree kidnapping; first, second, or third degree assault; first, second, or third degree assault of a child; first, second, or third degree rape; first, second, or third degree rape of a child; first or second degree robbery; first degree arson; first degree burglary; first or second degree manslaughter; first or second degree extortion; indecent liberties; incest; vehicular homicide; first degree promoting prostitution; communication with a minor; unlawful imprisonment; simple assault; sexual exploitation of minors; first or second degree criminal mistreatment; child abuse or neglect as defined in RCW 26.44.020; first or second degree custodial interference; malicious harassment; first, second, or third degree child molestation; first or second degree sexual misconduct with a minor; first or second degree rape of a child; patronizing a juvenile prostitute; child abandonment; promoting pornography; selling or distributing erotic material to a minor; custodial assault; violation of child abuse restraining order; child buying or selling; prostitution; felony indecent exposure; criminal abandonment; or any of these crimes as they may be renamed in the future.

First, second, or third degree extortion; first, second, or third degree theft; first or second degree robbery; forgery; or any of these crimes as they may be renamed in the future.

No
Yes If yes, specify and explain_____
_____

Have you ever been found in any dependency action under RCW 13.34.040 to have sexually assaulted or exploited any minor or to have physically abused any minor?

No
Yes If yes, specify and explain_____
_____
_____

Have you ever been found by a court in a domestic relations proceeding under Title 26 RCW to have sexually abused or exploited any minor or to have physically abused any minor?

No
Yes If yes, specify and explain_____
_____
_____

Have you ever been found in any disciplinary board final decision to have sexually or physically abused or exploited any minor or developmentally disabled person or to have abused or financially exploited any vulnerable adult?

No
Yes If yes, specify and explain_____
_____
_____

Have you ever been found by a court in a protection proceeding under Chapter 74.34 RCW to have abused or financially exploited a vulnerable adult?

No
Yes If yes, specify and explain_____
_____
_____

I certify, under penalty of perjury, that the statements above are true and correct. I understand that if any of the above statements is found to be false, it may result in my offer of admission being rescinded or dismissal from the program.

_____ _____
Signature (must be handwritten signature, NOT typewritten) Date

Visiting Students:
Upload all 3 pages of this form to your application in VSAS.
A handwritten signature or image of a handwritten signature is required.
Typewritten signatures are not accepted.

Checklist of Supplemental Documents to Upload to VSAS:

1. **UW Privacy, Confidentiality, and Information Security Agreement Form (PCISA):** Complete Data Stewardship Training (review the Power Point slides located on the UW website) and upload both pages of the signed and dated PCISA form to VSAS. Provide handwritten signature or an image of a handwritten signature. Typewritten signatures are not accepted. Leave blank the line starting with "copy provided on". This is for official use.

2. **UW SOM Essential Requirements for Medical Education Form:** Review the 13 page document then sign and date the last page of the form (included in this packet) and upload to VSAS. Provide handwritten signature or an image of a handwritten signature. Typewritten signatures are not accepted. Initial each line on the form.

3. **Temporary Workforce Member/Student HIPAA Self Study:** Review the 6 page document then sign and date the last page of the form (included in this packet) and upload to VSAS. Keep the preceding pages for your records.

4. **UW Self Disclosure, Consent, and Release of Information Form:** Provide handwritten signature or an image of a handwritten signature. Typewritten signatures are not accepted. Upload all 3 pages of the signed and dated form to VSAS.

   Criminal Background Check: Please complete a criminal background check through the University of Washington School of Medicine portal on the CastleBranch website: https://portal.castlebranch.com/ur95. There is a flat fee of $48.50. It is not necessary to upload the report to VSAS. We can view the completed report on the CastleBranch website.

5. **Personal Health Insurance Card:** If your school cannot verify on VSAS that you have personal health coverage, upload a copy of your health insurance card to VSAS.

6. **BLS or CPR:** If your school cannot verify your BLS dates on the VSAS application, you must upload a copy of your card to VSAS. Please note: we do not accept ACLS or EMT certifications as a substitute for BLS/CPR training. We do not accept online BLS certifications without an in person skills test. The card must be valid through the end date of your requested elective.

7. **AAMC Standardized Immunization Form:** Students must submit the AAMC immunization form and the requisite lab reports. We do not accept immunization forms from your home school. All required dates must be entered and the form signed by your school official or by your primary care physician. Upload the completed AAMC form and required documentation to VSAS.

   *** Hepatitis B vaccine: Per CDC guidelines, we require quantitative results with a reference range for the hepatitis b titer. All 3 dates of the hepatitis b vaccine series must be documented on the AAMC form, even if your hepatitis b titer is positive. Titer lab reports must be uploaded to VSAS.***

8. **Processing Fee**: The $100 processing fee is due as soon as you are offered a clerkship. If applying to more than one department send in a $100 fee **for each department**. For instance if you are offered three PEDs electives you owe $100 and if you are offered 2 PEDS and 1 MEDECK you owe $200. Fees are non-refundable. Payment may be made by credit card or check. Checks should be made out to the University of Washington. We will notify you when this fee is due. **THIS FEE IS NOT DUE UNTIL YOU ARE OFFERED A CLERKSHIP.**

Once all items have been received your application will then be reviewed by the department(s) where the clinical elective has been requested. **An approved application does not guarantee an elective**. The department will contact you within 6 weeks of the start date of the elective to confirm availability of the requested rotation. If you have questions about clerkship availability contact the departmental coordinator under the **Departmental Course Listings** page on our website.
http://uwmedicine.washington.edu/Education/MD-Program/visiting-students/US-Canadian/Departmental-Course-Listings/Pages/default.aspx

Additional notes about application processing timelines:

1. When you submit your application on VSAS, you will receive an automated email generated by VSAS stating that your application has been received.
2. Beginning in May 2018, departments will begin scheduling students with approved eligibility status.
3. Official clerkship offers will be issued via the VSAS software. Any unofficial clerkship offers issued by faculty or staff via email will not be honored by the UW Visiting Student Program. Once you have accepted the clerkship offer via VSAS and paid the UW Processing Fee, your clerkship is guaranteed.

Common mistakes which delay application processing times:

1. MOST COMMON mistake: hepatitis b titer result is qualitative, not quantitative.
2. Hepatitis b vaccine dates are not documented on the AAMC form.
3. Tuberculosis screening date expires prior to the requested elective.
4. AAMC immunizations form indicates that documents are attached but the actual documents are not uploaded to VSAS.
5. The documents included in this packet are not uploaded to VSAS, or they are not completed correctly.
6. The documents in this packet are missing pages when they are uploaded to VSAS.
7. The online criminal background check application is not completed prior to submitting the application.
8. The malpractice insurance expiration date will expire prior to the requested elective. Home Schools need to enter “N/A” for the expiration date on the VSAS verification page if the policy automatically renews on a future date (usually July).
9. The Home School does not enter the correct year of graduation.
10. The BLS certification date expires prior to the requested elective.

.