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@u.washington.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 health care 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/privacy.shtml

**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-health care components of the University of Washington as defined within Privacy Policy PP-01 Use & Disclosure of Protected Health Information – Organizational Requirements: [http://depts.washington.edu/comply/docs/PP_01.pdf](http://depts.washington.edu/comply/docs/PP_01.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 health care operations (TPO). Patient information may not be shared with the non-health care components of the University without patient authorization unless it is with a non-health component that supports the treatment, payment or health care operations of UW Medicine. UW Medicine may share patient information with any non-UW Medicine health care professional for treatment purposes. That is, to facilitate continuity of care, different health care 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 health care operations, health care 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 health care 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 health care 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 – 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:

http://security.uwmedicine.org/Policies/default.asp
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;
  o Never download, install or run unlicensed or unauthorized software.
• Use administrative permissions only when approved to do so and when required by job function;
  o 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:
  o 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.
  o 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:
  o Never leave patient information unattended in exam rooms or work areas.
  o 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).
  o 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.
  o Disposal of patient information must be done in a secure and confidential manner.
• Electronic Data:
  o 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.