

UW Medicine Temporary Workforce Member/Student HIPAA Self Study

UW Medicine is committed to privacy, confidentiality, and information security. 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.

Each UW Medicine entity has a privacy official who serves as a resource for HIPAA compliance.

University of Washington Medical Center & Clinics	(206) 598-5701
Harborview Medical Center & Clinics	(206) 744-9003
University of Washington Physicians' Network	(206) 520-5505
University of Washington Sports Medicine Clinic	(206) 543-6630
University of Washington School of Medicine	(206) 685-7369
UW Medicine Eastside Specialties Clinic	(206) 598-5701
University of Washington Hall Health Primary Care Center	(206) 685-1081
University of Washington Physicians	(206) 520-5144

The penalties for violating HIPAA can lead to individual or organization fines, jail time, and/or disciplinary action up to and including termination.

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** went into effect in April 14, 2003. It established 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, oral, or any other form.

It is the responsibility of each of us to protect the confidentiality of PHI.

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

The **Security Rule** went into effect April 21, 2005, which 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 PHI, you are asked to follow certain safeguards.

The Center for Medicare & Medicaid Services (CMS) oversees and enforces the HIPAA Security Standard.

The **Employer Identifier Standard** was adopted effective July 30, 2002. This portion of the law 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** went into effect in October 2003. This portion of the law 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 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 sanctions will be applied to workforce members (including trainees) who fail to comply with these policies and procedures. Sanctions will be based upon the relative severity of the violation.

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 PHI. Please pick up a copy of the Notice in the main lobby so that you are familiar with UW Medicine practices.

UW Medicine is comprised of the University of Washington Medical Center and Clinics; Harborview Medical Center and Clinics; UW Medicine Neighborhood Clinics (University of Washington Physicians Network); UW Physicians Sports Medicine Clinic; UW Medicine Eastside Specialty Center; Hall Health Primary Care Center; and UW Physicians. Within these entities, protected health information (PHI) may be shared for treatment, payment and health care operations (TPO). PHI may not be shared with the non-health care components of the University without patient authorization unless it is for the component to support the treatment, payment or health care operations of UW Medicine. UW Medicine may share PHI with any non-UW Medicine health care provider for treatment purposes. That is, to facilitate continuity of care, different providers who are involved in treating the patient may communicate about the patient's medical care. When using or disclosing PHI for payment and health care operations, providers may only disclose to non-UW Medicine entities the minimum necessary PHI required to accomplish the intended purpose.

UW Medicine may use or disclose PHI 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 PHI. 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 PHI 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 providers involving the treatment of a patient do not require such agreements.

Outside of treatment, payment or healthcare operations, UW Medicine may use or disclose PHI 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 PHI 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 disclosure 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 PHI 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 or supervisor for more information about the use of psychotherapy notes.

Research involving human subjects (either directly or indirectly through PHI) requires review by an approved Institutional Review Board (IRB). Researchers may use or disclose PHI 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 Privacy Officers.

Patients have the right to:

- Be informed how their PHI will be used;
- Decline disclosures in the inpatient directory;
- View and copy information in the designated record set;
- Request restrictions on the use and disclosure of PHI, including to family members;
- Request confidential communications about their PHI;
- Request amendments to the medical record;
- Ask for an accounting of disclosures made that do not fall under TPO or other disclosures authorized by, and known to, the patient;
- File a complaint about how UW Medicine and individual health care providers use or disclose their PHI. Complaints may be made to the UW Medicine Privacy Office, 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 PHI, the workforce member must contact the Privacy Officer of the entity rendering the care 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 PHI 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 PHI, 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 PHI 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.
- Logoff when you leave a workstation.
- Keep printed materials and computer screens containing PHI 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
- Report privacy violations or suspected breaches to your supervisor or any UW Medicine Privacy Officer.

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.

If you have a UW Net ID, you may view the policies in their entirety at the following website:

<http://depts.washington.edu/comply/security.shtml>

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 University of Washington and UW Medicine policies;
- Support compliance with federal and state statutory and regulatory requirements;
- Protect access accounts, privileges, and associated passwords (examples: Not sharing my password);
- Accept accountability for all activities associated with the use of individual user accounts and related access privileges;
- Not to change the computer configuration unless specifically approved to do so;

- Report all suspected security and/or policy violations to user's Help Desk;
- Ensure that 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;
- Use only licensed and authorized software;
- Not to download, install or run unlicensed or unauthorized software;
- Not to disable or alter the anti-virus and/or firewall software;
- Make no unauthorized network modifications and/or additions (i.e., wireless access points, mini-hubs or switches); and
- Report all known security violations to the appropriate entity's Privacy Officer or the UW Medicine Privacy Office.

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 supervisor/manager.

Date: _____

Signature: _____

Print Name: _____

Name of Supervisor/Manager: _____

Department: _____

Supervisor/Manager:

File original in departmental personnel file.