

UW Medicine

PRIVACY POLICIES SUMMARY

Throughout this summary, references to UW Medicine include UW Medicine's workforce.

COMP.101: Patient Information Privacy and Security Compliance Program and Administrative Requirements

The University of Washington (UW) is a *hybrid entity* with both healthcare and non-healthcare components. UW has designated certain of its healthcare components and related covered entities as one affiliated healthcare entity known as "UW Medicine" (for current list see [101.G1 University of Washington HIPAA Designation](#)). Within the entities included, protected health information (PHI) may be shared for treatment, payment and healthcare operations. Additionally, UW Medicine participates in *Organized Healthcare Arrangements* which allow entities to share PHI for clinical care services, payment for clinical care services, and any healthcare operations activities of the arrangement.

UW Medicine has established compliance policies, procedures, technical standards and guidelines addressing administrative, technical and physical safeguards for PHI, whistleblowers, mitigation strategies, prohibition of retaliatory acts, patients' non-waiver of rights, maintenance of the designated record set, personnel designations, and revisions and documentation of privacy policies and procedures.

COMP.102: Safeguarding the Privacy and Security of Protected Health Information (PHI)

UW Medicine safeguards the confidentiality, integrity and availability of PHI in all forms (including verbal, paper and electronic) and in all locations. UW Medicine uses a role-based model to identify appropriate levels of access to PHI.

UW Medicine workforce members are personally and professionally responsible for appropriately *protecting PHI* to which they are given access. For example, workforce members must 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. Workforce members must keep paper-based patient information out of view of patients, visitors and workforce members who are not involved in the patient's care, and dispose of it in a secure and confidential manner. Patient information taken off-site must be kept fully secured, remain in the workforce member's physical possession during transit, never be left unattended and never be left in any mode of transport (even if it is locked).

UW Medicine verifies the identity of all requestors and the requestors' legal authority for obtaining PHI. For disclosures made on a routine or recurring basis, UW Medicine departments implement policies and procedures that limit the PHI disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

COMP.103: Use and Disclosure of Protected Health Information (PHI)

UW Medicine may use and disclose PHI for treatment, payment, and healthcare operations (TPO), as authorized by the patient, or as required by law. When using or disclosing PHI for payment and healthcare operations, or when the patient has not authorized the use or disclosure, UW Medicine makes reasonable efforts to ensure that the use, disclosure or request of PHI is limited to the *minimum necessary* PHI required to accomplish the intended purpose. This standard does not apply to disclosures for treatment, to the individual patient, pursuant to patient authorization, or when required by law.

UW Medicine

UW Medicine may use or disclose PHI without a valid patient authorization in certain circumstances, such as for public health activities, health oversight activities, or to avert a serious threat to the health or safety of any person. Regarding *fundraising*, UW Medicine may use or disclose an approved set of patient demographic information and the dates of healthcare services to raise funds for its own benefit. UW Medicine must obtain an authorization for the use or disclosure of any other PHI for fundraising purposes. Individuals also have the right to opt out of fundraising communications.

Heightened standards of confidentiality are required when using or disclosing PHI pertaining to sexually transmitted diseases (STDs), reproductive healthcare, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency virus (HIV), mental health records, drug and alcohol treatment records or sexual assault program records. *Psychotherapy notes* maintained by behavioral health providers are a subset of PHI subject to heightened confidentiality protections. Psychotherapy notes may only be used or disclosed absent the patient's authorization in very specific circumstances. Please contact UW Medicine Compliance for fact-specific questions.

Certain uses and disclosures of PHI require providing the patient with an *opportunity to agree or disagree*. Examples include: inclusion in inpatient facility directories, providing proof of immunization for students, law enforcement evidence gathering, and disclosures to family, friends or others who are involved in the patient's care.

Upon admission, patients have the opportunity to decide whether to be included in the hospitals' *facility directories*. If a patient is incapacitated at admission, the healthcare professional should exercise their best judgment on whether to list the patient in the facility directory until the patient is able to express an opinion. Hospitals may release the condition and location of patients when a requestor asks for the patient by name. With the permission of the patient, clergy of the same faith may be given directory information without asking for a patient by name. UW Medicine may also use or disclose PHI to assist in disaster relief efforts.

Provided the patient does not object, UW Medicine may disclose PHI to relatives or other persons involved in patient's care. If a patient is unable to express his or her wishes, the healthcare professional exercises professional judgment on whether or not to release any PHI. There are additional limitations on uses and disclosures where situations involve abuse or neglect, or where the information is subject to heightened confidentiality. Please contact UW Medicine Compliance for fact-specific questions.

Uses or disclosures of PHI other than those described above generally require *written patient authorization*. UW Medicine must obtain a signed valid patient authorization for a disclosure of PHI that is not for treatment, payment or healthcare operations, or otherwise permitted by law. UW Medicine may share PHI with any healthcare professional for treatment purposes without an authorization. UW Medicine may share the minimum necessary PHI with non-UW Medicine entities for payment purposes. Questions regarding the sharing of PHI for the healthcare operations of a non-UW Medicine entity should be directed to UW Medicine Compliance.

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 in limited circumstances, such as when authorized by the human subject or pursuant to an IRB-approved waiver. Research using UW facilities or patient information, and/or which includes providing healthcare to UW patients, must comply with UW, UW Medicine Compliance and UW Medicine Information Security

UW Medicine

policies. For more information on conducting research, please review the [UW Human Subjects Division web page](#).

Healthcare professionals may communicate face-to-face with their patients about health-related products or services that UW Medicine provides. Healthcare professionals may also communicate with their patients about alternative treatments, coordination of care, or specialty care.

UW Medicine must obtain the patient's authorization for any use or disclosure of PHI for non-face-to-face marketing unless it is a promotional gift of nominal value.

Federal law allows UW Medicine to use or disclose a "limited data set" for research, public health or healthcare operations. A "limited data set" is PHI that excludes 16 specific identifiers of the patient or of the patient's relatives, employers or household members. UW Medicine obtains satisfactory assurances through "data use agreements" from the entity requesting a limited data set prior to allowing the use or disclosure. If PHI is de-identified through removal of 18 specific identifiers, the data is no longer subject to state or federal privacy laws and regulations.

Members of the public may make *requests for information* from the University through the UW Office of Public Records. UW Medicine shall comply with state and federal patient privacy laws when responding to such requests.

Except for TPO purposes, most PHI disclosures made without patient authorization must be documented in the *Accounting of Disclosures* database. UW Medicine workforce members shall document such disclosures in accordance with the requirements outlined in COMP.104.

COMP.104: Patient Rights Related to Protected Health Information (PHI)

UW Medicine protects the rights of patients with respect to PHI in the designated record set, in accordance with all State and Federal laws and regulations. These rights include: Notice of Privacy Practices, request for additional privacy protections, access inspect or request a copy of PHI, request an amendment to PHI, and an accounting of disclosures of PHI.

UW Medicine provides all patients (except prisoner patients) a copy of its Notice of Privacy Practices, which outlines a patient's rights and describes how a patient's PHI will be used or disclosed.

A patient has the right to access, inspect or request a copy of PHI contained in the UW Medicine designated record set, unless an exemption applies (for example, psychotherapy notes and information compiled for risk management purposes).

A patient also has the right to direct UW Medicine to send their records to a designated person and/or company. Requests to access, inspect or photocopy PHI should be referred to the release of information service area for the entity in which services were provided. UW Medicine workforce members may access their own PHI through their entity-based approved process. UW Medicine workforce members may not use this access to view the records of their family members or friends.

Individuals treated at UW Medicine facilities have a right to request additional privacy protections, restrictions and alternative communications regarding their PHI. UW Medicine may not be required to agree to a requested restriction. UW Medicine will not grant restrictions if continuity of patient care would be impeded. If UW Medicine does agree to a restriction, then it will follow the agreed-upon restrictions. All agreed-upon restrictions must be documented in the patient's record. When a patient pays out-of-pocket in

UW Medicine

full for healthcare items or services prior to the service, the patient has the right to restrict UW Medicine from disclosing the healthcare item(s) or service(s) to their health plan.

A patient may ask a healthcare professional to correct or amend their healthcare record. Requests must be in writing and state a reason for the requested change. UW Medicine has ten days from receipt of the request to respond in writing. If a healthcare professional receives a request for amendment they must immediately contact UW Medicine Compliance.

A patient has the right to request UW Medicine to provide an accounting of all disclosures from the patient's designated record set, excluding those uses or disclosures for which an accounting is not required (for example, treatment, payment or healthcare operations; uses or disclosures made with patient authorization; or uses or disclosures incidental to an authorized use or disclosure). If you receive a request for an accounting, please contact the UW Medicine Compliance.

COMP.105: Breach Notification

All UW Medicine workforce members must report breaches of patient information to the IT Services Help Desk or UW Medicine Compliance. This policy outlines the process UW Medicine follows to notify a patient when their unsecured PHI has been inappropriately access or disclosed. The department in which the breach occurs must cooperate with the investigation, assist in remediating identified issues and may be responsible for funding the response and notification of affected patients.

COMP.106: Use and Disclosure of Protected Health Information by Business Associates

A business associate (BA) is an outside entity or individual that performs a service or activity for or on behalf of the University of Washington or UW Medicine and involves the use or disclosure of PHI. UW Medicine may disclose PHI to a BA only after a *Business Associate Agreement* (BAA) is executed which establishes the permitted and required uses and disclosures of PHI and obtains satisfactory assurances that the Business Associate will safeguard the information. The BAA must include terms and conditions that require compliance with applicable health information security and privacy laws and UW rules or policies. The BA may only create, receive, maintain or transmit PHI for or on behalf of the University of Washington or UW Medicine, not for independent use by the BA. Relationships between healthcare providers regarding the treatment of a patient do not have the same requirements and are therefore not business associate relationships. Please contact UW Medicine Compliance if you have questions about whether a business associate relationship exists in a specific situation.

COMP.107: Information Security Policy

UW Medicine protects the confidentiality, integrity and availability of electronic PHI (ePHI) through the implementation of administrative, physical and technical safeguards. The Chief Information Security Officer (CISO) is UW Medicine's assigned information security official who serves as the focal point for the information security compliance-related activities and responsibilities. UW Medicine differentiates information security accountability by workforce members, managers of workforce members, information technology (IT) administrators, system owners/department IT, and enterprise IT.