Purpose

The purpose of this policy is to support and enhance healthcare, research, and education at UW Medicine, to protect patient privacy, and to ensure the security of patient-identifiable information in accordance with federal and state laws and regulations, and institutional policies and standards regarding the security of protected health information (PHI).

Definitions

- **Authorization** – A written document that gives UW Medicine permission to disclose specific PHI for purposes other than treatment, payment, healthcare operations (TPO); or when required by law, to disclose PHI to a third party identified by the individual.

- **Disclose/Disclosure** - The release, transfer, provision of access to, or divulging in any other manner PHI outside UW Medicine.

- **Protected Health Information (PHI)** - Individually identifiable information that relates to the past, present, or future physical or mental health of an individual, the provision of healthcare to an individual, or the payment for the provision of healthcare to an individual. This includes (but is not limited to) information such as name, address, date of birth, admission, discharge or death, telephone number, fax number, social security number, medical record number, or account number. Identifiers may include facial photographs, distinctive birth marks or other images that combined with other available information could identify the patient.

- **Workforce** - Faculty, employees, trainees, students, volunteers, and other entities or persons who perform work for UW Medicine through employment, academic or service agreements or contracts.
**Policy**

The use of photography, video/audio recordings, digital imaging, etc., in the clinical setting is often necessary for patient care, research, and education. Whenever possible, UW Medicine equipment is to be used to create patient images or recordings. UW Medicine workforce members are responsible for ensuring the security of PHI when using and disclosing these records (regardless of format). Patient images and recordings are to be stored and shared according to UW Medicine Information Security Policies: [https://security.uwmedicine.org/guidance/policy/default.asp](https://security.uwmedicine.org/guidance/policy/default.asp).

Recording or imaging for clinical use is included in the Care Agreement form. Sharing recordings or images with a payer is included in the Financial Agreement form. Procedure images and recordings (e.g., colonoscopy) are considered part of treatment and do not require separate consent.

A signed Authorization Form: [http://depts.washington.edu/comply/docs/PP_08_G.pdf](http://depts.washington.edu/comply/docs/PP_08_G.pdf) is required if identifiable recordings or images are to be used outside of the clinical setting (e.g., professional presentations, publications).

Use and disclosure of identifiable patient images and recordings for research purposes must be authorized using UW approved guidelines and the IRB Consent Form: [http://www.washington.edu/research/hsd/docs/555](http://www.washington.edu/research/hsd/docs/555).

Workforce members who share or otherwise transmit recordings and images outside UW Medicine and through the Internet must meet UW Medicine Information Security requirements for confidential electronic data in transit, and encrypt or otherwise physically secure the information in a manner that prevents theft or inappropriate use.

See:
- Electronic Data Policy: [https://security.uwmedicine.org/guidance/policy/electronic_data/default.asp](https://security.uwmedicine.org/guidance/policy/electronic_data/default.asp);
- Encryption Standard: [https://security.uwmedicine.org/guidance/standards/encryption/default.asp](https://security.uwmedicine.org/guidance/standards/encryption/default.asp); and
- Technical Guidance regarding encryption: [https://security.uwmedicine.org/guidance/technical/encryption/default.asp](https://security.uwmedicine.org/guidance/technical/encryption/default.asp)

Healthcare professionals who create and maintain clinical audio/video recording, photographs, or digital images must coordinate with Health Information Management to ensure compliant maintenance, storage, and access of these records.

**Cross References**

- HMC Admin P&P 30.2 UW Medicine Marketing and Communications
- UW Medicine Media Policies
- UW Medicine Policy 5-19: Guidelines for Audio/Visual Recording by Patient/Family
• UW Medicine Policy 100.7: Definition, Retention and Disclosure of the Legal Health Record

UW Medicine Information Security Policies, Standards and Guidance

• SP-01: Electronic Data Policy: https://security.uwmedicine.org/guidance/policy/electronic_data/default.asp
• SP-03: Workforce Member Policy: https://security.uwmedicine.org/guidance/policy/workforce_member/default.asp
• IT Services Security training materials about information security best practices: https://security.uwmedicine.org/training/dept_materials/default.asp
• APS 2.4: Information Security and Privacy Roles, Responsibilities, and Definitions: http://www.washington.edu/admin/rules/policies/APS/02.04.html

UW Medicine Compliance: Privacy Policies


IRB Consent Form Template

• http://www.washington.edu/research/hsd/docs/555

Approvals

____________________  ____________________
UW Privacy Official  Date
Johnese M. Spisso, Chief Health System Officer, UW Medicine & Vice President for Medical Affairs, UW
Related Procedures

A. Patient care

1. Clinical use of recordings and images is included in the Care Agreement form signed by the patient. The Care Agreement form identifies and informs the patient who creates and accesses patient records, including recordings and images: "... Photographs, videotapes, or other images of you may be used to keep a record of your care and treatment (including surgery). These images may become part of the medical record."

2. If the patient, personal representative, or legally authorized surrogate decision-maker objects to the taking or use of images or recordings for purposes other than diagnosis or treatment, the healthcare professional must honor the objection and may not use the images for any other purpose.

3. Video and audio recordings, photographs, and digital images used for clinical care are considered medical records and will be retained and released (when specifically requested) in accordance with applicable HIM and UW Medicine Compliance policies.

4. Documenting images and recordings as medical records:
   a. Images and recordings for patient care should contain appropriate identification and be stored in the clinical information system producing the recordings or images, uploaded into the EMR, or moved to secure departmental storage.

   b. However, many image and recording files are too large for incorporation in the EMR or clinical information system. Recordings and images should not be loaded into the EMR (including transcription or the clinical information system) without the approval of Health Information Management (HIM).

   c. Healthcare professionals should record the following in the medical record:
      i. Areas of the patient’s body that were imaged.
      ii. The identity of the healthcare professional responsible for the recording or image.
      iii. Date and time of creation.

5. Images created by family members:
   Photography or recordings in a patient care setting is not allowed unless healthcare professionals, staff and anyone else present during the event gives their agreement (verbally or in writing).
B. Use and disclosure of recordings and images

1. Except for the purposes of treatment, payment or healthcare operations, recordings or images contain any features that would permit identification of the patient, cannot be released to outside requestors without specific written authorization from the patient, personal representative, or legally authorized surrogate decision-maker.

2. The authorization should state that the patient agrees to have the images or recordings released to the requestor and the purpose for which they will be used.

3. If images or recordings must be de-identified prior to use, de-identify, redact, or mask any or all of the following:
   - facial features;
   - distinctive birth marks or identifying tattoos;
   - other areas that alone or combined with narrative or text might identify the patient;
   - direct identifiers (e.g., patient name, MRN).

   It is important to ensure that the de-identification, redaction, or masking cannot be undone by the receiver of the record.

4. Any use of identifiable images or recordings for marketing, advertising or by the news media, requires specific authorization by the patient, personal representative, or legally authorized surrogate decision maker. (See Patient Authorization for UW Medicine to Use or Disclose PHI for Publicity:
   http://depts.washington.edu/comply/docs/PP_08_I.pdf.)

5. Recordings or images that do not include any identifiable patient features (e.g., close-up of a non-identifiable lesion, images of internal organs) do not require specific authorization to be included in presentations or publication, unless otherwise required by the event sponsor or publisher.

C. Research

1. De-identified patient images or recordings may be used or disclosed for research purposes without prior authorization by the patient, personal representative, or legally authorized surrogate decision maker.

2. The use or disclosure of identifiable images or recordings requires documented IRB approval of a waiver of authorization or an authorization signed by the patient. (UW Human Subjects Review (IRB) http://www.washington.edu/research/hsd/ )
D. Education

As noted in the Care Agreement, de-identified patient images or recordings may be disclosed for teaching activities involving residents, students, trainees, and practitioners in UW Medicine’s training and education programs without prior authorization by the patient, personal representative, or legally authorized surrogate decision maker.

E. Storage

1. The equipment, recordings, or images must be secured in a locked cabinet or room, until the recordings or images are uploaded into the EMR.

2. Do not store recordings and images with PHI on local hard drives.

3. Personally-owned equipment must comply with UW and UW Medicine security policies when used for storing patient-identifiable recordings or images short-term.
   a. Patient-identifiable recordings or images must be removed (uploaded into the EMR or otherwise securely managed and stored within the department), and cannot be retained on personal equipment.

4. Procedures must be in place for:
   a. Printing or developing recordings or images;
   b. Storing recordings and digital images with PHI outside of the EMR;
   c. Identification, management, and access to recordings and images by clinical services and HIM.

Related Guidelines


Additional Contacts

UW Medicine Compliance
206-543-3098
comply@uw.edu