UW Medicine

Use and Disclosure of Protected Health Information (PHI) in Patient Audio/Video Recordings, Photographs, & Digital Images

The use of photography, video/audio recordings, digital imaging, etc., in the clinical setting is often necessary for patient care, research, and education. Patient information captured in such images or recordings is Protected Health Information (PHI) and must be used, disclosed, and stored securely, in accordance with all applicable UW Medicine Policies. This document synthesizes the various policy requirements and guidance that apply to these types of PHI. It is recommended that departments that create or handle patient images and/or recordings maintain operational procedures for developing, printing, storing, accessing and disclosing these patient records.

Security of Patient Images and Recordings

1. Whenever possible, UW Medicine equipment should be used to create patient images or recordings. Patient images and recordings are to be stored and shared according to UW Medicine Patient Information Security Policies: http://depts.washington.edu/comply/comp_107.

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

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

4. Do not store recordings and images with PHI on local hard drives or on unencrypted devices.

5. 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: http://depts.washington.edu/comply/comp_107
    - Encryption Standard: https://depts.washington.edu/uwmedsec/restricted/standards/encryption-standard/ (VMC, see VMC IT Security page.)
    - Technical Guidance regarding encryption: https://depts.washington.edu/uwmedsec/restricted/guidance/encryption/ (VMC, see VMC IT Security page.)

Patient Images and Recordings in the Clinical Care Setting

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." Procedure images and recordings (e.g., colonoscopy) are considered part of treatment and do not require separate consent.

2. Sharing recordings or images with a payer is included in the Financial Agreement form.

3. 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.

4. If patients or their family members wish to take photographs or create audio/visual recordings in the clinical setting, healthcare professionals, staff and anyone else that will be part of the photograph or recording must be given the opportunity to agree or object (verbally or in writing); if anyone objects, the activity should not be allowed to occur.

5. 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. 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.

6. 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.

Use of Patient Images and Recordings for Research and Education Activities

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

2. De-identified patient images or recordings may also 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.

3. To de-identify images or recordings, redact or mask 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, address, birthdate)

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

4. 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.*

5. The use or disclosure of identifiable images or recordings for research 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/)

6. A signed patient authorization form is required if identifiable recordings or images are to be used or disclosed outside of the clinical setting (e.g., professional presentations, publications).

Patient Authorization for Use or Disclosure of Images and Recordings

1. Except for the purposes of treatment, payment or healthcare operations, recordings or images containing any features that would permit identification of the patient may not be released to outside requestors without specific written authorization from the patient, personal representative, or legally authorized surrogate decision-maker. This includes any use of identifiable images or recordings for marketing, advertising or by the news media.

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. See COMP.103 Uses and Disclosures of PHI, Sections (III) and (V) for additional information.

Resources

- COMP.103 Uses and Disclosures of PHI
- UW Medicine Entity Specific Audio/Video/Photography/Media Policies

- UW Medicine Policy 100.7: Definition, Retention and Disclosure of the Legal Medical Record (See also *NWH Legal Medical Record Definition, Retention, Disclosure & Designated Record Set*, *VMC Medical Record Policy*)
- IRB Consent Form Template: http://www.washington.edu/research/hsd/docs/555
- SP-01: Electronic Data Policy: http://depts.washington.edu/comply/comp_107.
- SP-02: Computing Device and System Security Policy: http://depts.washington.edu/comply/comp_107.
- SP-03: Workforce Member Policy: http://depts.washington.edu/comply/comp_107.
- IT Services Security training materials about information security best practices: https://depts.washington.edu/uwmedsec/restricted/about-its-security/ (VMC, see VMC IT Security page.)
- APS 2.4: Information Security and Privacy Roles, Responsibilities, and Definitions: http://www.washington.edu/admin/rules/policies/APS/02.04.html