

FREQUENTLY ASKED QUESTIONS

DIGITAL AND AUDIOVISUAL RECORDING IN THE UW MEDICINE CLINICAL SETTING

The following FAQs are intended to help UW Medicine workforce members, including UW researchers, navigate the applicable laws, policies and rules governing the creation and use of digital images (photography or video recording) and audio recordings (collectively “recordings”) in the UW Medicine clinical setting.

1. What questions should I consider before starting a project involving the creation or use of recordings in the clinical setting?

A. Do I need operational approval to undertake the proposed activities?

Official business activities undertaken in the UW Medicine clinical environment must be approved in advance by an appropriate level of operational management, including the creation or use of recordings. The below table summarizes the approval process depending on the purpose of the recording activity or project and whether the project includes an audio recording component:

Purpose of Recording Activity	Audio recording?	Approval Process
Treatment, Payment, or Healthcare Operations Purposes (excluding QA/QI)	Either: Yes and No	Routine operational approval processes. Examples of such activities include photographs taken to diagnose health conditions, recordings capturing patients or the clinical environment for media relations purposes, or audio recordings capturing call center patient interactions for quality assurance purposes.
Research, Education, or QA/QI Purposes	No	Routine operational approval processes
Research, Education, or QA/QI Purposes	Yes	<ul style="list-style-type: none"> • If the audio recording will occur in a UW Medicine clinical setting where direct patient care is delivered (UW Medical Center, Harborview Medical Center, Valley Medical Center and UW Primary Care), obtain approval from the applicable UW Medicine entity’s Chief Executive Officer (CEO) or Executive Director (ED) using form “Request for Approval for use of Audio Recordings for Research, Education or Quality Improvement Purposes” (per policy COMP.304) • QA/QI Activities: Contact entity’s quality improvement leader to determine if project may be part of entity’s or UW Medicine’s Coordinated Quality Improvement Plan before seeking approval from CEO/ED

B. Who will be captured in the audiovisual recording?

The use of audiovisual recording devices may result in the capture of unintended subjects in the recording. For instance, your project may seek to evaluate the communication behavior of physicians, but incidentally may capture other members of the care team, the patient or patient visitors. Washington state law requires that consent be obtained from anyone whose private conversations are being recorded (see below). Note that this consent under Washington state law differs from the informed consent standard used in human subjects research. Consider the feasibility of your project by tailoring it to the intended subjects of the recording and evaluating what steps may be necessary when other individuals are also captured.

C. How will you obtain consent to record private communications or conversations?

Washington state law requires that all parties provide consent when an electronic device is used to capture private communications or conversations (see RCW 9.73.030). Under this law, verbal consent (including announcing that the conversation is being recorded and allowing the individual to object) is sufficient if the consent is recorded. Consent must consider the individuals' languages, literacy and whether individuals being recorded can perform their job duties if they decline to be recorded. Because legal interpretations may vary regarding what constitutes a "private communication or conversation" we recommend that you contact UW Medicine Compliance at 206.543.3098 or comply@uw.edu who will work with the Attorney General's Office to evaluate whether such consent is required for your proposal and the appropriate method to obtain and document it before requesting approval from your entity's CEO or Executive Director.

D. Will your project's recordings become public records subject to public inspection and will you have to retain them?

Because certain components of UW Medicine and many UW research records may be subject to the Public Records Act (RCW 42.56), you should consider how this law may apply to your proposal, whether your proposal may be subject to an exception to disclosure (i.e., documents created specifically for, and collected or maintained by a quality improvement committee) and how to manage the retention of such records under the [UW Medicine Records Retention Schedule](#) or the [UW Records Retention Schedule for Research \(consult with Enterprise Records and Health Information\)](#). Some research may qualify for a federal Certificate of Confidentiality to protect research records (consult with the UW Human Subjects Division (HSD)).

2. **What are some additional considerations about the creation of recordings for non-clinical purposes in the clinical care setting?**

- A. If the patient, personal representative or legally authorized surrogate decision-maker objects to the taking or use of recordings for purposes other than diagnosis or treatment, the healthcare professional must honor the objection and may not use the recordings for any other purpose.
- B. If patients, their family members, other healthcare professionals or researchers wish to create and use recordings involving UW Workforce or other individuals (e.g., patient's family or friends etc.), those individuals must be given the opportunity to agree or object (verbally or in writing); if anyone objects, the activity should not occur. Please note that under Washington state law, consent is required to record any private conversation (see Section 1 C above).

- C. Patient recordings de-identified pursuant to UW Medicine Compliance policy may be used or disclosed for research purposes without prior authorization by the patient, personal representative or legally authorized surrogate decision maker. Researchers must obtain patient recordings maintained by UW Medicine through a UW Medicine-approved honest broker and may be required to execute a Data Sharing Agreement negotiated by the business office of the researcher's UW school or college in order to share the data with commercial entities.
- D. De-identified 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. To de-identify recordings, redact, mask, or filter the following:
- Facial features
 - Distinctive birth marks or identifying tattoos
 - Other areas that alone or combined with narrative or text might identify the patient
 - Voice
 - Direct identifiers (e.g., patient name, MRN, address, birthdate)

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

- E. Recordings that are de-identified do not require specific patient authorization to be included in presentations or publication *unless otherwise required by the event sponsor or publisher*.
- F. The creation, use or disclosure of identifiable recordings made in the clinical setting for research purposes requires HSD/IRB review and, when protected health information (PHI) will be recorded, documented IRB approval waiving the authorization requirement or a HIPAA authorization signed by the patient ([University of Washington Human Subjects Division](#)).
- G. A signed patient authorization form is required if identifiable recordings containing PHI are to be used or disclosed outside of the clinical setting (e.g., professional presentations, publications).

3. How do I appropriately secure the storage of patient recordings?

- A. Patient recordings must be stored and shared according to [UW Medicine Patient Information Security Policies](#). Recordings made solely for research purposes must comply with the requirements of the IRB-approved Data Security Plan.
- B. Whenever possible, UW Medicine equipment should be used to create patient recordings. Equipment that does not belong to UW Medicine (i.e., personally owned equipment, or equipment purchased by a grant or an academic department) must comply with UW and UW Medicine security policies when used for storing patient-identifiable recordings temporarily. Patient-identifiable recordings must be removed (uploaded into the electronic medical record (EMR) or otherwise securely managed and stored within the department) and may not be retained on personal equipment unless they were made solely for research purposes and the personal equipment meets the conditions of the IRB-approved Data Security Plan.

- C. Do not store recordings with PHI on local hard drives or on unencrypted devices.
- D. Workforce members who share or otherwise electronically transmit recordings outside UW Medicine 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](#)
 - [Minimum Computing Device Standard](#)
 - [Technical Guidance regarding encryption](#)

4. What are some common examples of circumstances that give rise to these FAQs?

A. Example #1 Photographing Skin Conditions for Treatment Purposes

An outpatient clinic would like to photograph a patient's skin condition to obtain an e-consult from a dermatologist. The clinic anticipates that the photographs will be taken by a camera purchased by the clinic and the photos will be uploaded into the patient's medical record.

Because the photography will occur for direct treatment purposes no special approval is required beyond routine operational and clinical approval processes. Additionally, no special patient consent or authorization is required to take the photographs because the UW Medicine Care Agreement informs patients of the possibility that the care team will take photographs or videotapes to keep track of the patient's treatment ([Form UH0051](#)). The clinic's management team should also consider the following:

- i. The preference that the device used to take photographs be owned by UW/UW Medicine rather than a clinician's personal device;
- ii. Whether the camera and its storage device are encrypted;
- iii. How the photographs are securely transferred from the device to the clinic's secure network drive and the electronic health record; and
- iv. How the data is deleted from the camera's storage once the images are no longer needed on the device.

B. Example #2 Remote Monitoring of Patient Rooms for Patient Safety

A hospital clinician would like to introduce a pilot program to observe patients who pose a fall-risk through real-time remote monitoring. The clinician proposes to place cameras and speaker devices in patient rooms that livestream (i.e., no recording) to a centralized hub. A healthcare provider will remotely monitor several patient rooms simultaneously to provide verbal direction to patients and alert the patient's care team when intervention is needed.

If the proposed remote monitoring activity does not introduce an audiovisual recording component, then no special operational approval is required from the hospital's executive leadership team. Even though no special consent form is required for this activity, the care team should follow their entity's fall prevention procedures, such as informing the patient about the monitoring program, honor the patient's refusal of fall risk interventions, and documenting this information in the appropriate systems. Other considerations may include:

- v. Working with the appropriate IT Security team to ensure the security of the livestreaming activity.
- vi. Discussing the proposed project with the hospital's quality improvement administrative leader if the activity is undertaken as a QA/QI initiative.
- vii. [Consulting with the UW HSD if the proposed activity meets the definition of human subjects research](#)
- viii. Obtain hospital leadership approval if the proposed activity is undertaken for QA/QI or research purposes and the activity will result in recordings that capture patient or employee voices.

C. Example #3 Audiovisual Recording in the Clinical Setting for a Research Study

A UW researcher is planning a research study that includes capturing audiovisual recordings of a certain area of the hospital to evaluate the communication style of clinicians while delivering clinical care.

Because the activity includes an audio recording component, the researcher must submit the form "*Request for Approval for Use of Audio Recordings for Research, Education or Quality Improvement Purposes*" to the hospital's Chief Executive Officer or Executive Director for approval before any recording occurs. To undertake this following research activity in the hospital, the researcher should consider the following before initiating audiovisual recording in the facility:

- ix. [Obtaining HSD/IRB review if the activity constitutes human subjects research](#)
- x. Obtaining the research subjects' informed consent and HIPAA authorization (or IRB waiver), if required.
- xi. Whether the audio recording activity will capture any individuals who have not consented into the research protocol (i.e., other members of the care team, hospital visitors, or patients) and consult with UW Medicine Compliance to determine if additional consent is required pursuant to RCW 9.73.030.
- xii. Ensure the files containing the recordings are protected according to the IRB-approved Data Security Plan.

REFERENCES

- [COMP.103 Uses and Disclosures of PHI](#)
- [COMP.107 Information Security Policy](#)
- [COMP.304 Audio Recordings in the Clinical Setting for Research, Education or Quality Improvement Purposes](#)
- [UW Medicine Information Security Standards](#)

- 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 [VMC Medical Record Policy](#))
- [IRB Consent Form Template](#)
- [IT Services Security training materials about information security best practices \(VMC, see VMC IT Security page\)](#)
- [APS 2.4: Information Security and Privacy Roles, Responsibilities, and Definitions](#)