I. 11.1.4 Photography, Video or Audio Recording, and Other Imaging of Patients

Chapter 11 - Patient Privacy	Original Effective Date: April 2003
Section: 11.1 General and Oversight Policies	Date Last Reviewed: August 2026
Responsible Entity: Chief Compliance and Privacy Officer	Date Last Revised: August 2026

II. Purpose

The purpose of this policy is to safeguard the privacy, dignity, and confidentiality of patients, visitors, and workforce members at UT Health San Antonio (UTHSA) by regulating the capture, use, and disclosure of photographs, video recordings, audio recordings, and other forms of imaging. Whether for clinical care, research, education, or other purposes, these activities must be conducted only by authorized individuals, under approved circumstances, and in compliance with institutional policies and applicable privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA). This policy ensures imaging practices support patient care while upholding legal, ethical, and professional standards.

III. Scope

This policy applies to all Workforce Members—including faculty, staff, students, healthcare providers, contractors, and researchers—who have direct or indirect access to Protected Health Information (PHI). This includes all PHI maintained by UT Health San Antonio and its controlled affiliates, such as clinics, hospitals, and research facilities.

IV. Policy

A. Patient Consent

1. Patient consent is required prior to any form of photography, video recording, audio recording, or imaging.
2. The *General Consent for Treatment* form authorizes UTHSA to obtain clinical images for purposes including documentation, treatment, healthcare operations, education, research, or patient identification, in accordance with the institution's privacy policies, IHOP 11.2.4 Uses and Disclosures of Protected Health Information for Treatment, Payment and Health Care Operations, and the Notice of Privacy Practices (NPP).
3. Marketing Images

a. Photographs, recorded images, and audio recordings taken for marketing purposes- including use in printed materials, billboards, audiovisual content, news media, online galleries, or similar formats- require a signed authorization release form.

i. Patients must complete the *Patient Authorization Release* form (available in English or Spanish) in accordance with IHOP 11.2.7 Uses and Disclosures of Protected Health Information for Marketing and IHOP 11.2.15 Uses and Disclosures of Protected Health Information for Publications.

ii. Visitors and non-patients must sign the *Model Authorization Release* form (available in English or Spanish).

b. Marketing-related images should not be stored in the patient's Electronic Health Record (EHR).

4. Research Photographs, Images, and Recordings

a. Photographs, video, audio recordings, and images collected as part of a research protocol must receive prior approval from the Institutional Review Board (IRB). Authorization must be included in the research informed consent form, in accordance with IHOP 11.2.12 Uses and Disclosures of Protected Health Information for Research.

b. Images or recordings taken solely for research are not considered part of the patient's designated medical record.

c. Requests to use PHI for non-IRB research purposes must be reviewed by the Institutional Compliance and Privacy Office. If approved, the information must either be de-identified in accordance with IHOP 11.2.9 Deidentification of Protected Health Information or supported by the patient's written consent.

B. Clinical Photographs and Recorded Images

1. Clinical photographs and recordings captured by authorized Workforce Members for patient care are considered part of the patient's EHR and must comply with all applicable policies on EHR security, access, use, and disclosure.

2. Before taking any clinical photographs or recordings, Workforce Members must:

a. Inform the patient that the images will become part of the patient's medical record.

b. Confirm the patient's identity using two forms of identification. Patient-identifying information does not need to be included on the image itself.

3. Acceptable devices for capturing clinical images include:

a. UTHSA-issued camera or electronic device; or

b. Personal mobile computing device approved by Information Management and Services (IMS) in accordance with IHOP 5.8.12 Mobile Device and Personally Owned Computing Policy and that is equipped with an Epic-supported application (e.g., Haiku, Canto, or Rover).

4. Clinical photographs or recordings must be uploaded into the patient's EHR within 24 hours.
    a. Images captured through Epic-supported mobile applications must be uploaded immediately.
    b. All images must be deleted from mobile devices after uploading to the EHR.
    c. Images submitted by patients via MyChart are automatically integrated into the EHR and treated as clinical images.

C. Images for Clinical Education

1. PHI, including identifiable photographs, video or audio recordings, or other images used in non-research publications, manuscripts, conference materials, training presentations, or public forums (e.g., LinkedIn, social media platforms, etc.) require a signed patient authorization.
    a. Research related publications and educational materials must comply with IRB approvals and IHOP 11.2.12 Uses and Disclosures of Protected Health Information for Research.
2. Patients must complete the a Patient Authorization for Release of Health Records to External Parties form to use or disclose any identifiable photographs, video, audio recordings, or other images for clinical education purposes as outlined above.
3. Requests to use identifiable patient images for educational activities must be submitted to the Institutional Compliance and Privacy Office for review and approval.

D. Patients and Visitors Photographs and Recordings

1. Patients and visitors may record or photograph during care only if:
    a. Both the clinician and patient (or their representative) agree; and
    b. The activity is not disruptive or inconsistent with the delivery of patient care.
2. Patients and visitors are prohibited from using personal devices to record or photograph other patients or Workforce Members without explicit verbal or written permission.
3. If unauthorized or prohibited recording occurs, Workforce Members must ask the individual to stop and escalate the issue to a manager or supervisor.
4. Patients may not record their own or others' medical records or PHI. Such requests must be made through MyChart or formally submitted to the Health Information Management (HIM) Office.

E. Emerging Technologies Capable of Recording, Monitoring, or Biometric Identification

Workforce members are prohibited from wearing or operating personal technologies that have active recording, livestreaming, facial recognition, biometric identification, or automated monitoring capabilities while performing duties in patient care, research, clinical, or other restricted areas unless expressly authorized for institutional business

purposes and approved by the Chief Compliance and Privacy Officer in accordance with applicable policies, procedures, and regulatory requirements.

V. Definitions

Terms used in this document have the meaning set forth in the Patient Privacy Policies Glossary unless a different meaning is required by context.

Mobile Computing Device- defined as smartphones, tablets, and any device utilizing an operating system explicitly developed for mobile computing. See IHOP 5.8.12.

VI. Related References

UT Health San Antonio Institutional Handbook of Operating Policies (IHOP)

5.8.12 Mobile Device and Personally Owned Computing Policy

5.8.22 Data Protection

11.2.4 Uses and Disclosures of Protected Health Information for Treatment, Payment and Health Care Operations

11.2.7 Uses and Disclosures of Protected Health Information for Marketing

11.2.9 De-identification of Protected Health Information

11.2.12 Uses and Disclosures of Protected Health Information for Research

11.2.15 Uses and Disclosures of Protected Health Information for Publications

For questions regarding this policy, contact the Institutional Compliance and Privacy Office at 210-567-2014 or compliance@uthscsa.edu.

VII. Review and Approval History

The approving authority of this policy is the University Executive Committee.

Effective Date	Action Taken	Approved By	Approval Date
04/2003	Policy Origination		
04/2010	Policy Revision		
03/2013	Policy Revision		
01/2023	Policy Review	ICPO	01/18/2023
04/2025	Policy Revision	Executive Committee	04/15/2025
08/2026	Policy Revision	Executive Committee	08/31/2026