

## **HIPAA Guidance on Photos, Video and Audio Recording in Clinical Areas**

Photography, video, and audio recordings (collectively recordings) have the potential to violate patient privacy and interfere with patient care. Recordings must be taken, used, and/or disclosed in compliance with state and federal law. This guidance sets out rules for the recording of protected health information (PHI) and the recording of individuals (visitors, employees, or patients) in a University clinical setting.

### **Consent vs. Authorization**

In this document, “authorization” refers to the permission that HIPAA requires for use or release of PHI. Under HIPAA, authorization must be in writing and there are specific statements that must be included for the authorization to be valid. <https://hipaa.yale.edu/sites/default/files/files/5031-FR.pdf> ).

“Consent” refers to the process of obtaining permission from a patient to make a recording in circumstances where a HIPAA authorization is not required. The requirements for consent vary based on the context.

### **Allowable Photo/Video Recording for Business Purposes**

#### **1. Patient Consent for Recording a Patient/Individual**

The Joint Commission requires that consent be obtained prior to recording a patient for purposes unrelated to diagnosis, treatment, or identification of the patient, such as quality improvement, training, or other internal organizational activities. Consent requirements apply regardless of whether the resulting recording of the patient identifies the patient (e.g., consent is required for photographing a rash on a patient’s arm, even if the patient’s face is not visible).

#### **Instances In Which Recording a Patient Does Not Require Consent:**

- To document abuse or neglect
- For safety or security of patients, workforce, or visitors
- For identification of the patient
- For patient care and treatment activities including patient safety, care coordination, and treatment planning. In such cases, recordings should be integrated into the medical record.
- To monitor clinical conditions via video surveillance
- For recording done by the patient’s family members or friends when a) the recording does not interfere with patient care or capture other patients or PHI and b) permission is obtained from any workforce member being recorded.

#### **2. Patient Authorization for Use or Disclosure of a Recording**

Patient authorization is governed by HIPAA. Recordings that identify a patient or otherwise include PHI such as full face photos, photos of unique identifying marks, or photos of patients that are date stamped (reflecting a date of service) are subject to HIPAA. If a recording identifies a patient or contains PHI, and if the purpose for which the recording will be used or disclosed is unrelated to treatment, payment or healthcare operations (TPO), then written authorization of the patient or the patient’s personal representative is required.

#### **Instances in Which Patient Authorization is Not Required to Use or Disclose a Recording**

- For internal educational or teaching purposes in cases where the image has been completely stripped of direct identifiers

- When required by law
- When authorization of a patient or a patient's authorized representative is required but cannot be obtained in advance (e.g., recordings of trauma care in the Emergency Department taken by a covered entity for internal purposes). In cases such as these, recordings may be made, but authorization is required prior to use of the recordings.
- Photographs that do not contain any personally identifiable information or any associated personally identifiable text may be published in textbooks, journals articles, other externally distributed publications, or digital media without authorization.

### **3. Important Examples of Circumstances in Which Patient Consent and/or Authorization is Required**

#### **Marketing/Publicity/Public Relations**

Public relations initiatives conducted on behalf of the University and coordinated by the Office of Public Affairs require both consent and authorization. Recordings that will be used for marketing purposes have additional HIPAA marketing-specific authorization requirements. These recordings must also protect the privacy of bystanders; if bystanders' consent has not been obtained, then they must be given the opportunity to relocate to be out of scope of the recording/photograph.

#### **Research**

Recordings to be made for research purposes must be approved by the Institutional Review Board (IRB) and included in the consent/authorization document(s).

#### **Behavioral Health**

Recordings associated with mental health treatment are subject to additional state and federal regulation and may only be used and disclosed with specific patient consent.

#### **Patient Groups/Patient Meetings**

Participants in patient groups and patient meetings must at a minimum be informed of the potential for recordings to be made of the meeting. Posted signs, announcements, or handouts may be used for this purpose. Depending on the use of the recordings, additional consent or authorization may be necessary. For example, recording a patient meeting for marketing purposes requires that all participants sign a valid marketing authorization.

#### **Academic and Training Uses**

Recordings taken for either internal student/staff training or external presentations (such as at conferences, academic presentations, etc.) require prior consent, even if those recordings do not identify the patient or contain PHI (e.g., skin rash on the arm). Recordings of a patient that identify the patient or contain PHI require HIPAA authorization or de-identification before they can be used for academic purposes (such as at conferences, academic presentations, etc.) or for training of individuals not part of the institution's workforce.

#### **Quality Improvement/Quality Assessment (QI/QA)**

Recordings taken for the purpose of quality assessment or improvement require prior consent of the patient but do not require patient authorization under HIPAA. The consent requirement may be met through incorporation into the treatment consent signed by patients at time of service. However, these recordings should not contain information beyond that which is needed for the planned QI/QA activity.

## Law Enforcement

Requests from law enforcement officials should be reviewed by the Office of the General Counsel. The following are some important examples of law enforcement recording issues:

- Disclosure for identification purposes: Recordings may be released in response to a request by law enforcement for the purposes of identifying or locating a suspect, fugitive, material witness, or missing person.
- Disclosure as evidence of a crime:
  - Recordings may be released to law enforcement when a staff member has been the victim of a crime and the images are of the suspected perpetrator of the criminal act.
  - Recordings may be released to law enforcement when the images are believed in good faith to constitute evidence of criminal conduct that occurred on the premises.
- Mandated reports of suspected abuse or neglect: Recordings may be provided to law enforcement as required by law or in compliance with and as limited by a valid court order or court-ordered warrant; a subpoena or summons issued by a judicial officer; a grand jury subpoena or an administrative request, including an administrative subpoena or summons; a civil or an authorized investigative demand; or a similar process authorized under law, provided that: i) the information sought is relevant and material to a legitimate law enforcement inquiry, ii) the request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, and iii) de-identified information could not reasonably be used.
- Body Cameras: Body cameras used by institutional police/security as well as local law enforcement must be turned off when entering patient treatment areas, except when required under local law enforcement practices in the course of arresting an individual.

## Identification of Individuals in Emergency and Disaster Relief Situations

Recordings may be released to public or private entities authorized by law or charter to assist in disaster relief efforts for notification purposes.

## Telemedicine

Patient consent should be obtained prior to recording a patient through telemedicine technology. Recordings made during a telemedicine encounter may be used and disclosed for treatment, payment, or healthcare operations, without a patient's authorization. However, any use of a telemedicine recording outside of these HIPAA-permitted uses requires the patient's authorization, if the image is identifiable or if state law requires authorization for such use (e.g., if the recording is related to mental health). In-person processes for general consent for treatment and explanation of patient rights also apply to telemedicine.

## Live Stream

Live stream may be used for purposes that are permitted under University policy. For example, live stream of surgical procedures for internal training purposes using institutionally secured devices and transmissions may be performed with prior consent or authorization. Academic streaming to external viewers (e.g., academic conferences) and non-academic streaming (e.g., Periscope) may only be performed with institutional approval and both patient consent and authorization.

## Social Media

Members of the institution's workforce may not post recordings that contain PHI to their personal social media accounts. Workforce members are cautioned to consider not only whether a visual

recording shows patients but also whether any PHI is visible in the background. University sponsored social media use, such as departmental Facebook pages, must comply with the requirements described above under marketing/publicity/public relations.

### **Fundraising**

Recordings of patients made for use in fundraising or development may be taken, used, and disclosed only with patient consent and authorization. See HIPAA policy on Fundraising.

### **Commercial Uses**

Recordings made by third parties for commercial use must be approved by appropriate institutional authorities and with the prior consent and authorization of the patient. Proposed commercial uses should be referred to the Office of the General Counsel.

## **4. Rules regarding Recording Devices**

### **Institutionally-owned Devices**

Institutionally owned and secured devices may be used for recordings otherwise allowed under University policy. Whenever possible, applications associated with the EMR for use with photos, audio recordings, or video recordings should transfer this media directly to the medical record so that it is not stored on the device.

### **Workforce-owned Devices for Recordings of Patients for Clinical or Other Business Purposes**

Workforce use of personally owned devices is permitted only when the devices are secured in accordance with University security standards for mobile devices, including encryption, limitations on the quantity of PHI that can be stored, timely and secure removal of PHI, and secure transfer of recordings to the medical record.

### **Use of Patient or Visitor Devices**

- Patients and visitors may use their own devices (i) to record conversations about treatment instructions, with the consent of the treatment provider who is discussing the patient's care; and (ii) for personal use by the patient or the patient's family and friends, so long as the recording party has obtained the prior consent of the patient or their legally authorized representative and any workforce members or others who are to be included in the recording.

Recordings by patients or visitors must be obtained in such a way as to avoid capturing information related to other patients (e.g., information on white boards or the identities of individuals in waiting rooms). In no case may recordings be obtained when doing so may interfere with the provision of care or otherwise create an unsafe environment. Care providers are authorized to notify patients or visitors to stop recording when the activity is unsafe or interferes with patient care.

## **5. Use of Outsourced Recording Services on Premises**

Contractors that record in clinical areas on behalf of the University must have a signed contract addressing the following:

- Description of the activities to be performed on site
- Description of the institution's requirements for outsourced workforce's activities while on premises, including:
  - Need for an escort while on site
  - Required training prior to arrival on site

- Need for confidentiality agreements by the contractor's workforce
- Need for vendor registration, including background/sanctions checks and immunization as applicable
- Storage of raw photos and videos
- QA process for final recordings to verify de-identification of patients or existence of valid consent and authorization
- Ownership and use of the recordings
- Insurance and indemnification for activities on premises
- Business Associate terms and conditions, if the vendor will have access to and/or retain PHI
- Requirements for consent and/or authorization by patients based on the purpose of a recording and any additional requirements for consent, such as in the case of live feeds of procedures or surgeries
- Physical and technical security
- If the vendor is permitted to create a third-party reecording, the agreement must also specify the following:
  - The purpose of the recording and its subsequent use and whether further use must be constrained
  - Authorization requirements related to planned use (e.g., requirements for use in marketing vs. educational use)
  - Whether institutional prior approval of the final recording is required
  - Whether a clinician or staff member will be paid for their participation and, if so, if such payment requires further review under policies on conflict of interest or sale of PHI