San Francisco Department of Public Health

*Policy & Procedure Detail**

Policy & Procedure Title: PATIENTS, VISITORS, AND STAFF PHOTO/AUDIO/VIDEO RECORDING DEPARTMENT OF PUBLIC HEALTH/SAN FRANCISCO HEALTH NETWORK	
Category: Privacy	
Effective Date: 8/3/2019	**Last Reissue/Revision Date:** Click here to enter a date.
DPH Unit of Origin: HEALTH INFORMATION MANAGEMENT	
Policy Contact - Employee Name and Title; and/or DPH Division: DIANE LOVKO-PREMEAU	
Contact Phone Number(s): Click here to enter text.	
Distribution: DPH-wide ☒	**If not DPH-wide, other distribution:**

All sections in table required. Updated 3/2014

1. Purpose of Policy

The purpose of this policy is to protect the privacy of patients, clients, residents, and staff, to minimize interference with a employee's ability to perform his or her job and to align with SFDPH's policy on patients, visitors, clients and staff recording.

2. Policy

a. Photographing, videotaping and audio recording by patients, clients, residents, visitors and staff is prohibited anywhere, including inside facilities unless prior administrative approval is granted. DPH/SFCHN takes the rights and privacy of its patients and staff seriously. DPH/SFCHN must comply with the Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA), 45C.F.R. Parts 160 and 164, Subparts A and E and all state and federal confidentiality laws and regulations.

b. All individuals in the recorded area, including staff, must give their verbal or written consent prior to being recorded. Per California Penal Code Section 632, it is illegal for anyone to intentionally and without the consent of all parties to record a confidential communication by means of any electronic amplifying or recording device.

c. Patients, or their support person, with the agreement of their treatment provider may record care and/or medication instructions to aid in remembering those instructions.

d. It is policy that only secure mobile devices may be used by Staff to view, record, transmit, or store PHI.

This policy does not apply to public media authorizations that are made through Communications Office. Please refer to Administrative Policy Number 13.01, Media/Press Guidelines for ZSFG.

3. Definitions

For purposes of this policy, the following definitions apply:

A. Photo/Audio/Video Recording: Recording shall refer to any photograph, digital image, scan, motion picture, videotape, computer feed or electronic or audio recording.

B. Patient/Client/Resident: An individual receiving services. Visitor: An individual who is visiting ZSFG

C. Staff: An individual employed by, contracted by, or volunteering.

D. Providers: medical professionals credentialed to practice.

E. Authorization: Permission from the patient to use or disclose Protected Health Information to an individual or entity for purposes other than treatment, payment, healthcare operations or other uses allowed by law.

F. Dedicated camera(s): A camera (or cameras) acquired by a Department or Clinical Service which is accessible to designated staff for a defined clinical or forensic purpose and which is physically stored in a secure area when not in use.

G. Protected Health Information (PHI): Any information, including electronic PHI, whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual, and (ii) that identifies the individual, or which provides a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including, but not limited to 45 CFR § 160.103.

H. Secure mobile device: a small electronic device, such as a cell phone, that has activated encryption and authentication controls.

I. Flash drive: a small electronic device containing flash memory that is used for storing data or transferring it to or from a computer, digital camera, etc. Also known under various names such a thumb drive, jump drive, pen drive or USB key chain drive

J. Secure network: "Secure network" means the data is stored in compliance with DPH and UCSF HIPAA/HITECH standards, including but not limited to, access control, auditing and logging, data protection, data encryption, and network security.

4. Procedures

A. Photographs of a Patient for the Purpose of Treatment, Reimbursement, Hospital Operations and Patient-Care Related Identification

1. Consent. When the patient signs the Terms and Conditions of Admission, he or she consents to be photographed for purposes of treatment, reimbursement, hospital operations, including quality improvement education and training, and patient-care related identification.

2. Storage. Photographs taken for diagnosis and treatment purposes and identification may be printed and included in the patient's medical record or downloaded to a computer file on the secure network, provided the images are retained for a period of time consistent with medical record retention policies. Photographs for quality improvement, education and training may be downloaded to a computer file within the secure network. Images cannot be stored on a personal computer or other personal device.

3. Downloading Images. In collaboration with DPH or UCSF Information Technology staff, the leadership of each Clinical Service and Department must define the process of how images will be moved from the mobile devices, which its Providers and Staff employ, to a secure hard drive to ensure that images are not transferred through an unsecure medium or device. Images cannot be downloaded to unsecure e-mail accounts or unencrypted thumb/ flash drives. Flash drives must be encrypted and acquired in a manner consistent with DPH or UCSF policies. TEXT MESSAGING IS NOT SECURE AND IMAGES CONTAINING PROTECTED HEALTH INFORMATION (PHI) SHOULD NEVER BE SENT BY TEXT.
4. Trauma Resuscitations. There are additional considerations for the use and retention of videotapes of trauma resuscitations taken in the ZSFG Emergency Department for quality improvement purposes which are detailed in ZSFG Policy No, 22.05 Videotaping Trauma Resuscitations in the Emergency Department.

B. Photographs and other Reproductions for Legally Mandated Reports and other Forensic Purposes

1. Consent. No consent is required for photographs that are taken for purposes of documenting possible child abuse, domestic violence or elder or dependent adult abuse.

2. Storage. Photographs that are taken for purposes of documenting possible child abuse, domestic violence or elder or dependent adult abuse are appended to one copy of the reporting form and included in the patient's medical record. For forensic and related purposes, the images may also be downloaded to a computer file on the secure network, provided the images are retained for a period of time consistent with DPH medical record retention policies.

3. Downloading Images. In collaboration with DPH or UCSF/ Information Technology staff, the leadership of each Clinical Service and Department must define the process of how images will be moved from the mobile devices its Providers and Staff use to a secure hard drive to ensure that images are not transferred through an unsecure medium/ device. Images cannot be downloaded to unsecure e-mail accounts or unencrypted flash drives. Flash drives must be encrypted and acquired in a manner consistent with DPH or UCSF/ZSFG policies. TEXT MESSAGING IS NOT SECURE AND IMAGES CONTAINING PROTECTED HEALTH INFORMATION (PHI) SHOULD NEVER BE SENT BY TEXT.

4. Use and Dissemination. Photographs that are taken for purposes of documenting possible child abuse, domestic violence or elder or dependent adult abuse are appended to one copy of the reporting form and sent to the designated law enforcement or investigative agency.

C. Identification of Patients in the Nursery and Behavioral Health Units

1. Consent. For provision of care and security reasons, Providers and staff may photograph infants in the Nursery and adults in the Behavioral Health units. The patient or surrogate does not need to sign a specific consent and authorization form, but staff will honor a patient or surrogate's refusal to be photographed.

2. Storage. Photographs that are taken for identification purposes are placed in the patient's medical record.

3. Downloading Images. In collaboration with DPH or UCSF Information Technology staff, the leadership of each Clinical Service and Department must define the process of how images will be moved from the mobile devices its Providers and

staff use to a secure hard drive to ensure that images are not transferred through an unsecure medium/ device. Images cannot be downloaded to unsecure e-mail accounts or unencrypted flash drives. Flash drives must be encrypted and acquired in a manner consistent with DPH or UCSF/ZSFG policies. TEXT MESSAGING IS NOT SECURE AND IMAGES CONTAINING PROTECTED HEALTH INFORMATION (PHI) SHOULD NEVER BE SENT BY TEXT.

D. Photographs and other Reproductions taken for Research, Publication, External Education and related Purposes

1. Authorization and Consent. Photographs that are taken for research, external teaching activities (e.g. lectures, grand rounds) or publication in scholarly journals require a signed authorization and consent by the patient, or his/her surrogate on the Authorization and Consent to Photograph / Interview /Videotape form. There may be exceptional situations when the Committee on Human Research has granted a waiver of consent.

2. Storage. Photographs that are taken for research, external teaching or publication in scholarly journals do not become part of the patient's medical record. To the greatest extent possible, these photographs should be de-identified. Storage, retention and scope of use and dissemination should be clearly defined in the Authorization and Consent form signed by the patient.

E. Photographs and other Reproductions by the Media

Requests by the media to photograph or record a patient must be referred to the Chief Communications Officer at at 206-3170. This is discussed more completely in ZSFG Policy 13.1 Media/Press Guidelines for San Francisco General Hospital Medical Center.

F. Photographs / Interviews By Law Enforcement

If law enforcement requests to photograph, videotape, interview or record a patient to establish evidence of the patient's physical condition and circumstances relating to the injury, the attending physician, or designee, may make reasonable objections to the timing of the photographing or interview if the patient is unstable and it will interfere with the delivery of patient care.

G. Identification of Patients in the Custody of Law Enforcement

Law enforcement officers may photograph patients who are under their legal custody for identification and security purposes. The taking and use of these photographs are governed by the policies and procedures of that law enforcement agency. Providers and staff may raise reasonable objections to the timing of the photographing if it will interfere with the delivery of patient care.

5. References/Attachments

APPENDICES
Appendix A: Photographing Patients in the Hospital and Clinics
Appendix B: Authorization and Consent to Photograph/Interview/Videotape

Cross References
SFDPH Policies and Procedures

Patients, Visitors and Staff Recording in SFDPH Facilities

ZSFG Administrative Policies and Procedures:

- 13.01 Media/Press Guidelines for ZSFG
- 22.05 Digital Recording of Trauma Resuscitations in the Emergency Department
- 1.01 Victims of Dependent Adult/Elder Abuse, Child Abuse, Assaultive and Abusive Conduct, and Rape/Sexual Assault
- 8.7 HIPAA Compliance: Retention, Storage, and Destruction of Protected Health Information