Photographing Patients

When photographing patients, follow these procedures and guidelines to protect patient privacy:

Consider the Purpose for Photography

Patient Care and Internal Healthcare Operations
(quality improvement, patient safety, internal education)

→ Consent obtained via **Terms and Conditions of Service Form**
**Verify patient signed the form during*

External Education / **Publication**

→ Obtain consent via the **Consent for Photography / Authorization**

→ Scan signed form into the Medical Record

Media, Promotional, or Marketing

→ Consult with the UCSF University Relations Office before Proceeding**

→ Store photos in the medical record or save to a secure network or encrypted device. DO NOT store on an unencrypted device.

→ Immediately delete photos from the camera

Photography Guidelines

1. ****IMPORTANT!!**** **Do not post patient photographs or any patient information on social media without the patient's written authorization.** UCSF social media guidelines can be found at http://www.ucsf.edu/about/social-media-overview/social-media-guidelines.
2. **Minimize personal identifiable information in images.** Where possible, avoid including the patient's name or personal information (e.g., MRN, DOB, SSN) in the image. Note that facial images are identifiable in and of themselves.
3. **Use a hospital-owned or clinic-owned camera to photograph patients.** Do not take photographs using a personal camera or phone, unless using Haiku.
4. **Minimize risk when using cameras with memory cards.** Ensure the camera is physically secured at all times. Remove the memory card at the end of every clinic or inpatient consult, download its contents to a secure server, erase the memory card, and lock the camera in a secure location. Consider the use of a camera log for shared cameras.
5. **Do not allow photographs to be published in syllabi or made available online**, unless you have a signed patient consent for this purpose. If you use clinical photographs in a lecture, it is your responsibility to inform the course director or CME provider that the photographs cannot be reprinted in any syllabus, and that the photographs must be removed if your lecture will be made available to the audience in any format (i.e., printed or electronic). Note: CME courses frequently post PowerPoint slides online for attendees to review; it is your responsibility to ensure the photographs are removed, or have all required consents documented and retained by the department for 6 years.
6. **Use secure mechanisms to communicate with healthcare providers.** When sending patient photographs for consultation to other providers, use only approved technology. For example, before piloting or implementing a new system to share clinical images, it must be reviewed/approved by UCSF IT Security to ensure the system meets UCSF's security standards. For a list of UCSF-approved system to store/share images, contact the IT Service Desk at (415) 514-4100.

Updated May 2014