Patient Privacy For Continuing Medical Education (CME)
PROTECTED HEALTH INFORMATION

Protected Health Information (PHI)
Individually identifiable health information transmitted or maintained by an organization covered by the HIPAA regulations, regardless of form.

Types of PHI
any subset of health information, including demographic information collected from an individual, that:
- Identifies the individual (18 identifiers - see next slide); OR
- Has a reasonable basis to believe that the information can be used to identify the individual

PHI Formats
- Oral communications, paper copies, video and audio recordings, digital images, other electronic formats

Patient/representative authorization is generally REQUIRED for certain uses or disclosures of PHI
HIPAA HEALTH INFORMATION IDENTIFIERS

1) Names
2) Geographic subdivisions smaller than a state (e.g., street address, city, county, etc.)
3) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and all ages over 89
4) Telephone numbers
5) Fax numbers
6) Electronic mail addresses.
7) Social Security numbers
8) Medical record numbers
9) Health plan beneficiary numbers
10) Account numbers
11) Certificate/license numbers
12) Vehicle identifiers and serial numbers, including license plate numbers
13) Device identifiers and serial numbers
14) Web URLs
15) Biometric identifiers, including finger or voice prints
16) Full face photographic images and any comparable images
17) Internet Protocol address numbers
18) Any other unique identifying number, characteristic or code

Stanford University
OCR’s POSITION: PHOTOS & PHI

Comments: Some comments noted that identifiers that accompany photographic images are often needed to interpret the image and that it would be difficult to use the image alone to identify the individual.

Response: We agree that our proposed requirement to remove all photographic images was more than necessary. Many photographs of lesions, for example, which cannot usually be used alone to identify an individual, are included in health records. In this final rule, the only absolute requirement is the removal of full-face photographs, and we depend on the “catch-all” of “any other unique characteristic” to pick up the unusual case where another type of photographic image might be used to identify an individual.

Source: Final Privacy Rule, 65 CFR 82712 (Dec. 28, 2000)

What constitutes “any other unique identifying characteristic”? Anything that distinguishes an individual and allows for identification. For example, a unique identifying characteristic could be the occupation of a patient, for instance, “current President of State University”

Source: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#supress
Baby photos are a type of PHI
- Posting pictures of baby pictures on hospital office walls without a signed HIPAA authorization violates the federal HIPAA regulations (even if parent voluntarily sends them in)

**OCR’s Official Statement**
“A patient’s photograph that identifies him/her cannot be posted in public areas” unless there is “specific authorization from the patient or personal representative”

PHOTO EXAMPLE: GETTING UNDER YOUR SKIN

January 1, 2012

*Using post-procedure photos for ads can constitute a HIPAA violation*

- Patient had cosmetic procedure and gave consent to perform procedure
- Practice used pre-treatment and post-treatment photos in local advertisement (without authorization)
- Patient sued alleging HIPAA violation

**HIPAA Requirement**

- Written patient authorization to publish identifiable patient images for commercial or educational purposes

December 19, 2013

Physician Accused of Posting Patient Photos on Social Media

- Intoxicated patient admitted to hospital and contacted her Facebook “friend,” a physician at the hospital
- The non-treating physician accessed the patient’s records, and took and posted photos (and mocking commentary) of the patient on Facebook and Instagram without consent
- Patient sued her “friend” for damages and filed HIPAA complaint on basis that her “friend” had accessed her medical records in violation of hospital policy

Source: http://journal.ahima.org/2013/12/19/physician-accused-of-posting-patient-photos-on-social-media/
STANDARD ADMISSION CONSENT – SUFFICIENT?

- "I understand that photographs, videotapes, digital, or other images may be recorded to document my care, and I consent to this. I understand that (physician's name) will retain the ownership rights to these photographs, videotapes, digital, or other images, but that I will be allowed access to view them or obtain copies. I understand that these images will be stored in a secure manner that will protect my privacy and that they will be kept for the time period required by law or outlined in (physician/hospital's name)'s policy. Images that identify me will be released and/or used outside the office only upon written authorization from me or my legal representative.”

NO

- Sample patient consent for photos found in most treatment informed consent documents signed upon admission to a clinic or hospital is insufficient for educational presentations
- These consents typically only authorize the use of photos for treatment purposes – and do not authorize the use of images for other purposes like medical education seminars or medical journal publication
Milton Wolf, a Kansas radiologist vying for the Republican nomination to U.S. Senate, posted gruesome X-ray images of gunshot fatalities and medical injuries to his Facebook page, accompanied by inappropriate commentary (e.g., drawing comparison to Terminator 2).

Wolf claimed that his usage on Facebook “didn’t reveal an individual’s identity didn’t require prior authorization” claiming it was “an educational thing for people”.

“De-identified health care images are often used for education and other purposes,” however Wolf’s use was not a “legitimate educational purpose”.

The images are patient information, identifiable in any way and Wolf’s actions were “inappropriate” and suggest violation of professional conduct.
EXCEPTION: “DE-IDENTIFIED” PHOTOS

- De-identified patient images may be used without patient authorization.
- All identifiers must be removed or redacted/block out, including but not limited to: patient name, MRN, DOB, full face photographic images and any comparable images.
- If facial images will be used, they should be cropped so the entire face is not shown, *the patient’s eyes and nose are blocked out*, to the extent “reasonably possible” for purposes of de-identification of the patient.
- Images of internal body part(s) taken during procedures using specialized equipment - arthroscopy, endoscopy, colonoscopy, bronchoscopy, laparoscopy, etc. - are typically de-identified, provided there is no reasonable basis to believe that it could be used to identify the person.
- MRI images of the head may provide information comparable to that of photographic images since a patient may be recognized via rendering of the skin surface.
HIPAA COMPLIANT AUTHORIZATION FOR PHOTOS

- HIPAA regulations require patient authorization for the release of PHI, which includes patient photos for purposes beyond treatment, payment and healthcare operations
- Written authorization should specify usage for medical education, staff teaching, or other publicity purposes
- The patient or his/her legal representative should sign and date the authorization form
- Anyone other than the patient who has the legal authority to sign should indicate his or her relationship to the patient
- Explain patient’s right to refuse to sign authorization
- Explain patient’s right to revoke authorization at any time; however, specify that revocation is inapplicable to information already released under the authorization
WHERE TO GO FOR MORE INFORMATION

Privacy Office: https://privacy.stanford.edu

Telephone: (650) 725-1828

Email: privacy@stanford.edu

Address: 127 Encina Commons, 615 Crothers Way