

Privacy & Social Media

"If you wouldn't post it in an elevator, don't post it online."

1. Know our responsibilities and obligations under HIPAA:

- a. Patients and human subjects have expectations that we will protect and secure their private information.
- b. University of Arizona Health Care Components (e.g. departments, clinics and individuals who conduct standard, electronic, transactions, such as billing insurance for treatment or those who perform services on behalf of covered entities under a Business Associate Agreement) have HIPAA obligations.
- c. Investigators must comply with HIPAA when their study involves the use or disclosure of medical information about patients.

2. Know what qualifies as protected health information (PHI) or personally-identifiable information (PII):

- a. Names and addresses;
- b. Email Addresses;
- c. Social Security numbers;
- d. Medical record numbers;
- e. Dates of birth, death, admission and discharge;
- f. Full-face photos and comparable images;
- g. Biometric identifiers (including finger, voice prints); and
- h. Many other identifiers (see <http://ocr.arizona.edu/sites/ocr.arizona.edu/files/IS%20IT%20PHI.pdf>).

3. Know Best Practices:

- a. Always think twice before posting! Don't post information about patients or research subjects, even in general terms, without their consent.
- b. When in doubt, always obtain a valid Authorization from the patient/subject before posting information online. Even if HIPAA does not apply to your particular situation, you should make all reasonable attempts to protect an individual's privacy and verify that he/she consents to the release of information. Until further guidance is released, please contact the HIPAA Privacy Program (see contact information on page 2 (5(b)) of this document) for a copy of an Authorization form.
- c. Use extreme caution when taking photos of your work environment. Your photograph might contain PHI or an individual's private information, even if you don't notice it (e.g. Who is in the background? What is on your desk/computer monitor?).
- d. Do monitor and moderate your official account (see information below about responding to patient posts).
- e. Use passwords on computers (including screensavers) and mobile devices, including your personal phones and tablets.

- f. Use an abundance of caution on your individual/personal accounts as well. Review the UA Division of Human Resources *Social Media Guidelines*:
http://www.hr.arizona.edu/social_media_guidelines
- g. Do talk about research! See *Promoting Clinical Trials on Social Media* for tips about how do this responsibly: http://www.hr.arizona.edu/social_media_guidelines

4. Respond appropriately if a patient or research subject *self-discloses* PHI or PII:

- a. Ensure that your accounts have the AHSC User Guidelines posted to proactively remind users that what they post on social media is not necessarily private. See: <http://uanow.org/participate>
- b. If the post contains a complaint about your unit's services or a question related to their personal health:
 - i. Do not immediately delete the post, even if it is a publically viewable comment. Instead, respond by asking the person to contact the appropriate person via a more private and secure channel, such as phone or email. Provide contact information. Take a screenshot of the post and your response.
 - ii. Once you are in contact with the person via a more secure channel, remind them that their post may be viewable by others and suggest that they may wish to delete it if they do not want their personal information disclosed.
- c. If the post is directed at your unit and contains positive material (such as a compliment on your unit's services):
 - i. You may acknowledge the post with a like or favorite or to make a nonspecific, encouraging comment that does not disclose any further information about the person.
 - ii. Do not repost, retweet or otherwise share the post unless you obtain their express permission (see 3(b) above).
- d. If the post discloses the PHI or PII of an individual other than the poster him or herself, take a screenshot and immediately take steps to remove or report the post. This will vary by platform and how the post was originally made.

5. Know how to report a compliance issue or who to ask if you have questions:

- a. Human Subjects Protection Program (for issues or questions related to human subjects research): VPR-IRB@email.arizona.edu
- b. HIPAA Privacy Program (for issues or questions related to privacy and security of patient and human subject research information): privacyoffice@email.arizona.edu or (520) 621-1465.
- c. Information Security Office (for issues or questions related to information security):
<http://security.arizona.edu/report-incident>
- d. Ethics and Compliance Hotline (if you would like to submit an anonymous report): (866) 364-1908
- e. The AHSC Social Media Coordinator (for other issues or questions):
bchoekenga@email.arizona.edu