Invited Commentary

Using personal mobile devices to record patient's medical information – Doing the right thing in the wrong way?

Merril A. Pauls, MD, MHSc*†

Using personal mobile devices to record patient's medical information – doing the right thing in the wrong way?

A survey published in this month's *CJEM* confirms what many of us see on a daily basis – the use of personal mobile devices (PMDs) to record a patient's confidential medical information.[1] We should support and promote practices that improve patient care, but this cannot occur at the expense of our fundamental ethical duty to safeguard patient confidentiality and privacy.

Capturing and transmitting images for the purpose of patient care

A physician does not need explicit consent to share personal health information with others in the circle of care.[2] Examples may include a plastic surgery resident sending a picture of a complex laceration to their attending or a physician sending a picture of a rash to a dermatologist.

However, the use of PMDs to take these pictures raises issues of how this information is stored and transmitted. Most PMDs will not meet the security standards required by provincial and federal legislation for the storage of personal health information. Most people save their photos to cloud storage and are unaware of where that information is stored. While the sharing of clinical information in these contexts is acceptable, the way most physicians are doing it is not.

Many health authorities are building the capacity to share and transmit patient photos in a secure manner, and there are PMD applications that are compliant with Canadian privacy legislation.[3] In addition to these technical solutions, physicians who wish to use their PMD to capture and transmit clinical information should consider the following:

- Obtain and document the patient's consent when possible. If the patient is unable to consent, document why consent could not be obtained and why sending the image is in the patient's interest.
- De-identify the image as much as possible. Try to keep facial features and other identifiable marks out of the picture. Blackout names, health card numbers, and other identifying demographic data.
- Do not send images that are potentially sensitive (such as breasts or genitalia) unless it is crucial to patient care and no feasible alternative exists.
- Change the setting on your phone so clinical images will not be uploaded to cloud storage.
- Send the image on a secure network. Some institutions and health authorities have specific rules regarding how this can/should be done.
- Delete the picture from your phone once it has been received and ask the receiver to do the same once they have reviewed it.

Even though physicians can share personal health information amongst the circle of care without explicit permission, patients can request their information not

From *Department of Emergency Medicine, Max Rady College of Medicine, University of Manitoba; and the †Emergency Physician, Health Sciences Centre.

Correspondence to: Dr. Merril Pauls, Department of Emergency Medicine, Max Rady College of Medicine, Medical Services Bldg., S203–750 McDermot Avenue, Winnipeg, MB R3E 0W2; Email: merril.pauls@umanitoba.ca

CJEM 2019;21(4):449–451 DOI 10.1017/cem.2019.352

be shared.[4] If a patient requests that a photo not be taken, this must be respected.

Capturing images for learning and teaching

The Canadian Medical Protective Association (CMPA) states that a patient's express consent is needed when their personal information is captured or shared for purposes other than health care.[5] The consent discussion should be comprehensive and include the reasons for taking the photo, what will be recorded, whether the patient will be identifiable, possible uses of the photo, who may be authorized to access the photo and in what context, and the patient's right to refuse. The CMPA website has a sample consent form.[6]

The use of PMDs to take pictures of interesting electrocardiograms (EKGs), computed tomography (CT) scans, or rashes and the casual sharing of this information with learners and other physicians is a practice that should stop. Every province has laws concerning how patient information should be stored and protected, and the native programs of most PMDs will not meet these requirements. If a physician's PMD or their cloud storage were accessed by another individual, and this type of clinical information was discovered, there could be significant legal and professional ramifications.

Physicians should consider other ways to build and maintain a teaching file, including using secure storage that is part of their clinical environment or images from free open-access medical education (FOAMed) sources (ensuring they have been collected appropriately, patient consent obtained, and the source cited). When a unique clinical image presents itself, physicians must obtain written informed consent if they intend to submit it for publication or use it as part of a teaching session.

A number of "private" social media networks exist for health care providers that claim to provide a secure environment for sharing clinical information.[7] If patient consent has not been obtained, these networks still represent a grey zone. They may meet legal requirements for privacy, and the educational focus offers some justification, but these posts can still be shared with others outside the network, and a complaint to a regulatory authority could result in discipline, if the content or tone is seen as unprofessional.

Capturing and sharing images for other reasons

We are accustomed to posting every aspect of our lives. Some physicians see no difference between a meal they posted on Instagram yesterday and a CT scan they are looking at today. Posting clinical images on personal social media should be avoided. It can be difficult to completely de-identify these images and easy for a patient or family to identify themselves.[8] A Rhode Island emergency physician discovered this the hard way when she was fired for sharing information about a trauma case on social media.[9] We have a fiduciary duty to our patients. As professionals, we are responsible to preserve the trust relationship between society and medicine. Patients will not feel comfortable disclosing personal information or allowing clinical photos to be taken, if they believe their doctor might post them on Facebook.

PMDs can help us care for patients, but the risks are significant. We must act in the best interests of our patients, adopt practices that comply with privacy laws, and minimize the risks of breaching confidentiality. This includes obtaining and documenting consent, de-identifying images, using secure platforms, and deleting photos when they are no longer needed. We must avoid the casual collection and sharing of "interesting" clinical images and avoid posting clinical information or photos on social media. Getting a few more likes is never worth the loss of trust and the risk of professional repercussions.

Keywords: Clinical photos, confidentiality, personal mobile device, privacy

Competing interests: None.

REFERENCES

1. Walker KE, Migneault D, Lindsay HC, Abu-Laban RB. Use of personal mobile devices to record patient data by Canadian emergency physicians and residents. *CJEM* 2019;21(4):455–9.
2. Canadian Medical Protective Association. Good Practices Guide – Circle of Care. Ottawa: Canadian Medical Protective Association. Available at: https://www.cmpa-acpm.ca/serve/docs/ela/goodpracticesguide/pages/communication/Privacy_and_Confidentiality/circle_care-e.html (accessed February 14, 2019).
3. Yeung J. ShareSmart featured in Canadian Health Network! Toronto: MD Consultants; 2016. Available at: https://mdconsultants.ca/sharesmart-featured-in-canadian-health-network/ (accessed February 14, 2019).

https://doi.org/10.1017/cem.2019.352 Published online by Cambridge University Press

4. Canadian Medical Protective Association. Did you know? Patients can restrict access to their health information. Ottawa: Canadian Medical Protective Association; 2017. https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2017/did-you-know-patients-can-restrict-access-to-their-health-information (accessed February 14, 2019).
5. Canadian Medical Protective Association. Using clinical photography and video for educational purposes. Ottawa: Canadian Medical Protective Association; 2011. https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2011/using-clinical-photography-and-video-for-educational-purposes (accessed February 14, 2019).
6. Canadian Medical Protective Association. Photo and Video Consent Form. Ottawa: Canadian Medical Protective Association. Available at: https://www.cmpa-acpm.ca/static-assets/pdf/advice-and-publications/risk-management-toolbox/com_photo_and_video_consent_form-e.pdf (accessed February 14, 2019).
7. Ventola CL. Social media and health care professionals: benefits, risks, and best practices. *P T* 2014;39(7):491–20.
8. Lagu T, Kaufman EJ, Asch DA, Armstrong K. Content of weblogs written by health professionals. *J Gen Intern Med* 2008;23(10):1642–6.
9. Conaboy C. For doctors, social media a tricky case. Boston Globe; 2011 Apr 20. Available at: http://archive.boston.com/lifestyle/health/articles/2011/04/20/for_doctors_social_media_a_tricky_case/?page=full (accessed February 14, 2019).

https://doi.org/10.1017/cem.2019.352 Published online by Cambridge University Press