


Sharing clinical photographs: Patient rights, professional ethics, and institutional responsibilities

by Jacquelyn M. Means, MD;
Ira J. Kodner, MD, FACS;
Douglas Brown, PhD;
and Shuddhadeb Ray, MD, MPHS

| 17





Arguments that clinical photos are part of the private medical record also raise the question of who owns the photos: the hospital, physician, or patient?

This article addresses a common ethical dilemma in modern surgical practice: sharing clinical photographs via mobile devices. To help surgeons and surgeons in training better understand and address the ethical considerations surrounding the exchange of clinical photographs with colleagues, the authors examine the following: the level of consent physicians should seek in these scenarios, how photographs may infringe upon patient rights to privacy and confidentiality, physician responsibility to uphold patient privacy, and security issues associated with the clinical use of mobile devices.

This article describes a common scenario in which a resident is seeking the advice of an on-call surgeon to consult on a patient case and is asked to share a photograph of the patient's injury. Possible approaches to this dilemma are described, as are the ethical issues that need to be considered in choosing one option over another.

The case and alternative approaches

Consider the following example: A fifth-year surgical resident working in the clinic evaluates an adult male construction worker with moderate hand trauma. The resident believes a consultation with a plastic and reconstructive surgeon (PRS) is necessary and contacts the on-call surgeon in that department. The resident gives the on-call PRS the history and physical exam details over the phone. The PRS consultant then asks the resident to send him a photo of the hand trauma via text message to get a better understanding of the extent of the injury, the underlying damage, and the urgency of the case. This institution has no guidelines or policies in place regarding transmission of patient photography via a personal mobile device.

Some possible responses to this situation include the following:

- **Option 1:** The resident takes several photos of the hand injury with a personal mobile device and sends the photos via text message to the PRS.
- **Option 2:** The resident obtains informed consent from the patient and continues to carry out the steps outlined in Option 1.
- **Option 3:** The resident obtains informed consent, takes several photos with a personal mobile device, and e-mails the photos to the PRS using a secure hospital e-mail address.
- **Option 4:** The resident tells the PRS that he is uncertain regarding the risks associated with photographing the patient and does not want to cause any unintended harm to the patient, hospital, or himself.

A closer look at the options

Option 1: The resident takes several photos of the hand injury with his personal mobile device and sends the photos via photo text message to the PRS.

The primary issue in Option 1 is whether the resident should obtain consent to take and share the clinical photographs that the consulting surgeon has requested. In current clinical practice, the spectrum of patient consent ranges from patients being completely unaware of the care decisions their treating physician is making to participating in shared decision making. Between these alternatives are several variations. For example, the physician might make the patient aware of the plan of care, offering limited but sufficient information, and/or an opportunity to object or ask questions.¹ No single variation on the spectrum is inherently or categorically more correct than another.

Physicians acting at any point along the spectrum may be practicing ethical medicine, but their actions must be justified by the clinical context. For example, a number of everyday tasks, such as ordering a complete blood count, often are performed without much patient discussion. These types of clinical tasks are typically low-risk, routine hospital orders. On the other hand, when several management alternatives could



be implemented, each with its own risks and benefits (for example, selecting a cancer treatment), a lengthy discussion with the patient to obtain informed consent is required.

Where should medical photography fall on the spectrum? What are the current and future roles of these images? Are patient photographs most comparable to a procedure, treatment, physical exam element, or diagnostic tool? In the case presented, if the images are intended solely to give the consulting PRS a better understanding of the degree of damage, the photographs arguably are being used both as a diagnostic tool—similar to an X ray—and as a physical exam component.

If a health care professional accepts this analogy, then consider the type of consent typically obtained for these actions. The patient is informed of the physician's orders, is given justification, and is provided with an opportunity to object or to ask questions. If the patient consents, the physician continues with the proposed action. If clinical photographs are analogous to diagnostics and physical exams, should the physician take the same approach to patient consent?


Although clinical photography may have functional similarities to physical exams and diagnostics, it could be argued that sharing clinical photography poses a greater risk of breaching patient privacy, the deleterious consequences of which outweigh the benefit of expedited medical care. The concern is that, as technology advances and increased connectivity facilitates the exchange of digital images, the creation of such digital photos may threaten a patient's right to privacy and confidentiality. With such a risk in mind, the consent process detailed earlier in this article may seem less appropriate. The patient is informed neither of the intended use(s) of the photographs nor of the possible endangerment of his confidentiality.

But is this patient's confidentiality truly at risk? In clinical photography, personal identifiable information (PII) is defined as any physical feature that might easily distinguish a patient, such as facial features, birthmarks, and tattoos. Under the Health Insurance Portability and

Accountability Act (HIPAA) Privacy Rule, "full face photos and any other comparable images" are considered "direct identifiers."² In the case presented, it is safe to assume that the resident plans to limit the photographs to the patient's injured hand, which has none of these identifiers. If these particular photos are shared, is there a risk of breaching the patient's privacy and confidentiality? To answer this question, one must determine what constitutes "other comparable images." This vague phrase leaves it up to the photographer who, in this case, is the treating physician, to determine if the physical attributes included in the image reveal PII.

One could argue that the definition of PII ought to be extended to include all potentially unique physical features, including limbs, digits, joints, skin color, and unique injuries. On the other hand, another physician may believe PII is strictly limited to unique markings and the face. A similar argument would be that the "full-face photos and any other comparable images" reference in the HIPAA Privacy Rule is part of a limited data set that excludes other identifiers, such as name, address, and birth date. Depending on what one concludes is PII or "other comparable photos," clinical photographs may be considered part of the private medical record and, therefore, should be protected like any other personal health information.

Arguments that clinical photos are part of the private medical record also raise the question of who owns the photos: the hospital, physician, or patient? Typically, patients have ownership over their medical record and control third-party access to their private health information. If clinical images are considered part of the patient's medical record, it follows that the patient should have ownership over any clinical photographs.^{3,4} Ownership in this discussion should be differentiated from copyright laws and instead focused on the ethical dilemma as to which party has the most at stake. The clinical photographs are valuable to all involved but are arguably most important to the patient, who has the most to lose if the photographs are released to the public.^{3,5} Therefore, upholding the ethical principle of justice supports the view that the



Physicians must use these devices prudently and remain informed of the technological shortcomings.

patient should have ownership of the photographs and control their distribution.

So, how should clinical images be shared with a larger audience, if at all? Clinical photographs have become a widely used educational tool and routinely appear in presentations as well as in hard copy and electronic publications. However, when clinical photographs are intended solely for educational purposes, they no longer provide a direct benefit to the patient. The benefit has now shifted to a societal impact; that is, to educate others in the hope of providing improved patient care in the future.³ But once the benefit shifts away from the patient, that individual is left with a risk to confidentiality. The consent issue is no longer simply whether a clinical photograph may be created but now includes permission to use the photograph.⁵

Sharing digital images with a large audience reduces that ability to control the distribution of sensitive photos. Web-based presentations and the wide availability of electronic publications makes controlling access to patient photographs a challenge. With this concern in mind, even though a physician may be passionate about education, his or her duty to uphold the patient's right to privacy and confidentiality is still of the utmost importance; therefore, the physician must exercise great care when using sensitive photos for nonpatient care-related activities.

Option 2: The resident obtains informed consent from the patient and continues to carry out the steps outlined in Option 1.

The actions associated with Option 1 remain relevant to this option. However, two important concepts require more careful attention. In health care, informed consent is integral to shared decision making and is based on respect for patient autonomy.⁶ Informed consent provides patients with an opportunity to participate in their own medical care and aims to avoid deceit and coercion.^{7,8} When obtaining informed consent, a physician typically details the risks, benefits, and limitations of all available options.

Based on this understanding of informed consent, would obtaining anything less than informed consent for clinical photography infringe upon a patient's right to autonomy? If the physician sees a significant risk of breaching patient confidentiality and believes, for example, that all patient photographs should be considered personal health information, then obtaining informed consent would be the safest action, from an ethical perspective, on the consent spectrum. If the physician concludes informed consent is necessary, then a decision between verbal versus written consent must be made. In the case presented, verbal consent would certainly be quicker, easier, and less obtrusive. This approach also upholds the ethical principle of non-maleficence by aiming to minimize patient suffering. However, from a legal standpoint, written consent may be the recommended option to protect the physician and hospital from future liability.⁹

To help guide residents and other physicians through the process of making an ethically complex decision, as in the case presented in this article, it is recommended that health care institutions have standards and policies in place that cover this issue. Unfortunately, even when these policies exist, they rarely address the specific issue of clinical photography. Institutions need to facilitate this process by making policies available and compatible with current technology.

Option 3: The resident obtains informed consent, takes several photos with his personal mobile device, and e-mails the photos to the PRS using a secure hospital e-mail address.

The resident's decision in Option 3 highlights an understanding of mobile device security issues and the increasing need to develop secure modes of transmitting and sharing clinical photographs.

Text messaging through a mobile device should always be viewed as a vulnerable mode of transmitting sensitive data. When a text message is sent, the text is stored on a central server that is not compliant



with HIPAA, as well as on the sending and receiving devices.¹⁰ Many hospital employees may be cognizant of this vulnerability and consequently avoid sending text messages containing traditional personal health information, such as patient name and date of birth. However, sending photographs via text is a newer issue, one with more associated uncertainties. When reviewing Option 3, the discussion detailed in Option 1—what constitutes PII—should be carefully considered. If a physician's definition of PII is limited to the face, tattoos, or birthmarks in clinical photographs, the risk may be determined as minimal when sending unidentifiable clinical photographs over less secure modes of transmission. Conversely, if a physician has a broader definition of PII, they may be obligated to send clinical photos through a more secure hospital e-mail address to better protect the data.

Although a protected e-mail account does provide added security, personal mobile devices have their own inherent security issues. Personal mobile devices have become increasingly prominent in the medical workplace and are popular due to their ease of use and portability. However, their portability means they can easily be lost or stolen.¹¹ An unauthorized user may then access the device's stored data (including saved photographs and text messages). Many phones lack the technology to encrypt data, a necessary step that allows the user to securely transmit sensitive patient information.¹² Even if a device has encryption capabilities, its secured digital memory card may be unable to encrypt the device's stored, and potentially sensitive, data.

Modern personal mobile devices, particularly smartphones, have virtually the same capabilities as a desktop computer. Most of these mobile devices lack the security measures that are standard on all hospital computers. Personal mobile devices are protected by weak numerical passwords, do not offer firewall protection or antivirus software, and have the option to transmit data through non-secure wireless networks.¹¹ In contrast, hospital desktop computers operate solely through an institution's server and its secure network.

An institution's information technology (IT) department makes multiple efforts to protect personal health information, including setting computer lock-out times, changing passwords, overseeing and limiting user access to certain files, detecting changes made to stored data, and monitoring secure wireless and wired networks.¹³ IT departments have far less access to and control over employees' personal devices. The variety of brands, operating systems, and service providers for mobile devices creates an even greater challenge in developing standard security measures.

Much work still needs to be done in terms of securing and regulating mobile devices for clinical use. For the foreseeable future, the owner of the device is trusted to safeguard patients' sensitive health information, including clinical photographs. Physicians must use these devices prudently and remain informed of the technological shortcomings.

Option 4: The resident tells the PRS that he or she is uncertain regarding the risks associated with photographing the patient and does not want to cause any unintended harm to the patient, hospital, or himself.

The resident who follows Option 4 understands the technology concerns discussed in Option 3 and decides to err on the side of caution. The physician recognizes the limitations of a personal mobile device and decides that the potential harm to the patient's privacy and confidentiality overrides other considerations.

Option 4 leads to a possible knowledge discrepancy and a conflict between two physicians. Imagine that the consulting PRS is an older physician who is less familiar with smartphone technology than the fifth-year resident. Given this disparity, who should be responsible for protecting the patient's privacy and confidentiality? Is it an equally shared responsibility, or is the resident more accountable because of his or her advanced acumen with smartphone technology?

To explore this issue, consider the everyday hospital practice of ordering a consult. Consults are often

requested to ensure that a more experienced, knowledgeable physician is involved in managing a patient. The consulting physician does not make the final clinical decisions but still has an ethical responsibility to provide the requesting physician with the best information and advice possible. Similarly, the resident may be obligated to provide the PRS with the technological knowledge necessary to provide the best care for the patient. Even though the PRS may have a weaker understanding of the potential risks involved, HIPAA guidelines must continue to be followed to protect personal health information, including clinical photographs.

Conclusion

With increasing technological capabilities and the large number of personal mobile devices used in the workplace, snapping a photo of a patient for both clinical and educational purposes can present ethical conundrums. These ethical issues—which include consent, respect for autonomy, photographic ownership, photographs as personal health information, and physician responsibility to uphold patient confidentiality—are further complicated by the security concerns associated specifically with mobile devices.

An ethical case can be made for several courses of action in the clinical scenario presented in this article. This breadth of possibilities is evidenced by the many variations and differences found in hospital policies regarding clinical photography. The issue that will most likely divide physicians is how to define PII and to recognize the validity of obtaining consent when warranted, specifically when there is a potential risk to the patient's privacy and confidentiality. Furthermore, increased security on mobile devices is necessary and the institution must play a role in addressing these security measures. ♦

REFERENCES

1. Brown D. A toolkit for practical medical ethics. *Virtual Mentor*. 2009;11(11):909-914.
2. U.S. Department of Health and Human Services. Modifications to the HIPAA Privacy Rule—Final Rule. *Federal Register*. Volume 67, Number 157. August 14, 2002. Available at: www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/privrule.txt. Accessed August 17, 2015.
3. Hood CA, Hope T, Dove P. Videos, photographs, and patient consent. *BMJ*. 1998;316(7136):1009-1011.
4. Segal J, Sacopulos MJ. Photography consent and related legal issues. *Facial Plast Surg Clin North Am*. 2010;18(2):237-244.
5. Berle I. Clinical photography and patient rights: The need for orthopraxy. *J Med Ethics*. 2008;34(2):89-92.
6. Tay CSK. Recent developments in informed consent: The basis of modern medical ethics. *APLAR J Rheumatol*. 2005;8(3):165-170.
7. National Center for Ethics in Health Care. Informed consent do's and don'ts for best practice. *InFocus: Topics in Health Care Ethics*. August 2006. Available at: www.ethics.va.gov/docs/infocus/InFocus_20060801_Informed_Consent_Dos_and_Donts.pdf. Accessed August 17, 2015.
8. O'Neill O. Some limits of informed consent. *J Med Ethics*. 2003;29(1):4-7.
9. AHC Media LLC. Could photographing an ED patient get you sued? Available at: www.dgslaw.com/images/materials/Eiselein_ED_photo.pdf. Accessed August 17, 2015.
10. U.S. Department of Health and Human Services. HIPAA Security Guidance. December 28, 2006. Available at: www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteseu.pdf. Accessed August 17, 2015.
11. Houlding D. Healthcare information at risk: The consumerization of mobile devices. Solution Brief: Privacy and Data Security for Healthcare. Intel Corporation. November 3, 2011. Available at: www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/securing-mobile-devices-in-healthcare-solution-brief.pdf. Accessed August 17, 2015.
12. Heikkila FM. Encryption: Security considerations for portable media devices. Institute of Electrical and Electronics Engineers (IEEE) Security & Privacy. July/Aug 2007. Available at: www.pivotgroup.net/collaterals/Encryption_Considerations_%20Portable_Removable_Media_Devices.pdf. Accessed August 17, 2015.
13. Palm Inc. Smartphone and handheld security for mobile business. 2005. Available at: webobjects.cdw.com/webobjects/docs/PDFs/Palm-Security-WP.pdf. Accessed August 31, 2015.