Arthroplasty Today 5 (2019) 57–60

Contents lists available at ScienceDirect

Arthroplasty Today

journal homepage: http://www.arthroplastytoday.org/

Office tip

Patients, pictures, and privacy: managing clinical photographs in the smartphone era

John F. Nettrour, MD [a, *], M. Benjamin Burch, MD, MS [a], B. Sonny Bal, MD, PhD, JD, MBA [b]

[a] Department of Orthopaedic Surgery, University of Missouri, Missouri Orthopaedic Institute, Columbia, MI, USA
[b] Amedica Corporation, Salt Lake City, UT, USA

ARTICLE INFO

Article history:
Received 19 September 2018
Received in revised form
1 October 2018
Accepted 2 October 2018
Available online 12 November 2018

Keywords:
Photograph
Smartphone
Privacy
Health Insurance Portability and Accountability Act
Deidentification

ABSTRACT

It is easy to capture and share clinical photographs and x-ray images using modern smartphones. This technology affords health-care providers the ability to rapidly collaborate and facilitate care for their patients. This improvement, however, has increased concerns regarding patient privacy and the safeguarding of protected health information. Health-care providers should understand the deidentification process for patient photographs because this process fundamentally changes the expectations and requirements for how providers are to handle this information. Properly deidentified patient photographs (and other data) are no longer considered identifiable protected health information and are not subject to the handling requirements mandated by the Health Insurance Portability and Accountability Act. This article addresses patient privacy concerns attendant to the acquisition, transmission, and sharing of clinical photographs among health-care providers. It provides guidelines for providers seeking to minimize the risk of noncompliance with privacy requirements as they adopt these new technologies into their practices.

Introduction

Health-care providers, today, can readily communicate and share patient information electronically. Specifically, the modern smartphone has integrated 2 key technologies: (1) high-speed wireless data connections and (2) high-quality digital cameras. This enhanced ability to obtain and share patient photographs raises questions as to how the information should be used responsibly, especially in light of societal concerns related to patient privacy and safeguarding health information. This review addresses patient privacy and related concerns attendant to the acquisition and transmittal of photographs among health-care providers and provides useful guidelines to comply with health-care privacy laws in protecting patient information, while leveraging the modern communications technology toward clinical care.

Office tip

With this article, we aim to offer a practical guide to acquiring and sharing clinical photographs using new smartphone technologies. We seek to reconcile the technological advances with current health-care privacy law and provide practitioners with useful tips regarding how to ensure the privacy of health information when using these tools to collaborate and improve patient care.

Discussion

The extent of the problem

Photographs of clinical conditions and x-ray images are obtained easily and shared using smartphones. Text messaging of patient information is now widespread among health-care providers; over half of physicians now use text messages and digital image transmission when communicating with patients and other providers regarding patient care [1-6]. In 2006, text messages surpassed telephone calls as the most prevalent form of telecommunication, and digital photography now provides almost all photographic image captures worldwide [7,8]. Information sharing via short messaging system (SMS) has been shown to facilitate patient care and interventions [9,10].

No author associated with this paper has disclosed any potential or pertinent conflicts which may be perceived to have impending conflict with this work. For full disclosure statements refer to https://doi.org/10.1016/j.artd.2018.10.001.

* Corresponding author. Department of Orthopaedic Surgery, University of Missouri, 1100 Virginia Avenue, Columbia, MI 65216, USA. Tel.: +1 573 882 2663.
E-mail address: nettrourj@health.missouri.edu

https://doi.org/10.1016/j.artd.2018.10.001

In a 2014 survey of the Canadian Society of Plastic Surgeons, 89% of the respondents transmitted clinical photographs using smartphones; the figure rose to 100% for resident physicians [11]. In the same study, 57% of the surgeons had stored patient photographs on their smartphones, and 10% did not use password protection on the devices. These findings have been corroborated by other authors, who have reported increasing use of digital photography and smartphones in other medical specialties [12-14]. Despite the advantages, adoption of digital technology in this manner may run counter to patient privacy concerns and related legislation.

Safeguarding health information

In 1996, the Health Insurance Portability and Accountability Act (HIPAA) was implemented to enhance the portability and continuity of health insurance coverage in the United States. The HIPAA also contained a mandate for protecting the privacy of medical records. A section of the HIPAA called "Subtitle F-Administrative Simplification" offers the definitions of "protected health information" (PHI) and "individually identifiable health information" [15]. The Secretary of Health and Human Services (HHS) was tasked with the promulgation of the final regulations to accomplish the goals outlined in the HIPAA. In the years that followed, the HIPAA "Privacy Rule" and the "Security Rule" were formulated by the HHS to establish the standards by which health-care providers are held accountable.

The Final Privacy Rule set forth the concept of "deidentification" of health information (including medical photographs) for exemption from the HIPAA requirements. The distinction between "deidentified" patient information and identifiable PHI is important because each is handled differently. For identifiable PHI, health-care providers must follow the requirements of the HIPAA and its supporting legislation. In contrast, with "deidentification," patient data are no longer considered identifiable PHI, such that the mandates and requirements of the HIPAA are not applicable. The following section will review this difference in light of the use of clinical photographic images.

Deidentification: its importance and how to do it

Section 164.514 of the Final Privacy Rule acknowledges the inherent difficulties in deidentifying health information and photographs. It states that "there is always some probability or risk that any information about an individual can be attributed to that individual." [16]. This rule proposes 2 methods to remove identifying information from records and photographs to "render the information 'deidentified' and thus not subject to this (the Privacy) rule" [16,17]. These 2 methods are illustrated in Figure 1; the first deidentification method is the "expert determination method." This envisions data being analyzed and reviewed by an expert in statistics, with sufficient encryption to make it effectively "deidentified" to prevent individual recognition [16,17]. The second means for deidentification is the Safe Harbor Method [16,17]. In this method, 18 specific identifiers are removed from the records or photographs, and the information is then deemed "deidentified" and no longer considered identifiable PHI that can be linked to a specific individual (Table 1). Of the criteria, #17 specifically addresses patient photographs (ie, "full-face photographs and any comparable images" are to be removed for information to be "deidentified").

Patient photography was carefully weighed by the authors of the Privacy Rule, and their opinions are captured in the Final Privacy Rule of 2000 [16,18]. In the antecedent Proposed Privacy Rule (1999), all photographic images were considered direct patient identifiers and therefore could not be "deidentified" [18]. In contrast, the Final Rule (2000) was more lenient and allowed patient photographs to be included in the "deidentification" process. Authors of the rule commented that "We agree that our proposed requirement to remove all photographic images was more than necessary … in this final rule the only absolute requirement is the removal of full-face photographs … 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," (emphasis included as per original legislation) [16].

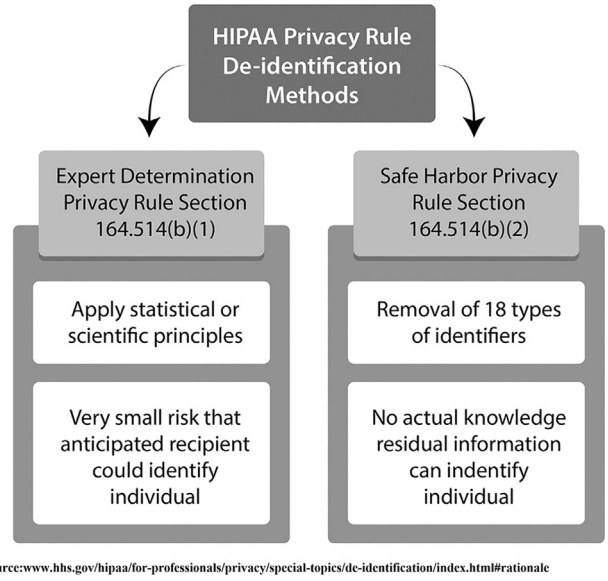

Figure 1. Two methods of deidentification.

Table 1
Eighteen identifiers to be removed for deidentification.

1. Names	10. Account numbers
2. All geographic subdivisions smaller then a state	11. Certificate/license numbers
3. All elements of dates (except year) for dates directly related to the individual (date of birth, date of admission, date of discharge, date of death). Also, all ages over 89 years or elements of dates indicative of such age.	12. Vehicle identification or serial numbers including license plate numbers
4. Telephone numbers	13. Device identification or serial numbers
5. Fax numbers	14. Web Universal Resource Locators (URLs)
6. Email addresses	15. Internet Protocol (IP) addresses
7. Social security numbers	16. Biometric identifiers including finger and voice prints
8. Medical record numbers	17. Full-face photographs and any comparable images
9. Health plan beneficiary numbers	18. Any other unique identifying number, characteristic or code

Deidentified health information created after this method is no longer protected by the Privacy Rule because it does not fall within the definition of PHI (protected health information).
Source: www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification. Accessed: August 30, 2018.

Table 2
Potential identifiers with clinical photos.

1. Intrinsic to the patient:
Anatomic anomalies, birthmarks, scars
2. On the patient:
Unique clothing, jewelry, piercings, tattoos
3. Around the patient:
Unique setting, surroundings, or location
4. Any facial photography

As the Final Privacy Rule allows photographs as long as they are deidentified, what is the unique "characteristic" whereby such a photograph may still identify an individual? The HHS "Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability (HIPAA) Privacy Rule (2012)" offers insights into this question. This instructive document is derived from the American Recovery and Reinvestment Act of 2009, which required the HHS to offer guidance in meeting the requirements of the Privacy Rule. An indicative example of an "identifying characteristic" would be "the current President of State University," a highly specific example illustrating the intent of the legislation [19].

Removing visible and concealed identifiers for photos

Neither HIPAA nor the Privacy Rule specifies exactly which patient characteristics should be removed when deidentifying patient photographs. In accordance with legislative intent to remove features or characteristics, which can reasonably identify an individual, we recommend that the items listed in Table 2 should be redacted from clinical photographs. Thus, patient tattoos, birthmarks, surgical scars, clothing, body piercings, facial photography, and the surroundings of the photograph should be considered and removed as necessary to deidentify the image.

In addition to obvious identifiers, digital images and smartphones embed so-called technical metadata into the image files. Exchangeable image file format (EXIF) data are a type of metadata pertaining to photographic images; these data are created and stored with the image when the photo is taken. Common EXIF data can include camera make, serial number, shutter speed, focal length, compression mode, and aperture settings [20,21]. Figure 2 provides an example of typical EXIF data contained within a digital photograph. EXIF data may also include the specific date, time, and location data pertaining to the photograph. Time-stamping of the photograph in terms of the day and time—along with location recording with Global Positioning System coordinates (ie, "geotagging")—can create very specific patient identifiers [22]. The Safe Harbor Method for deidentification specifically calls for time and location data removal. To accomplish this, we recommend turning off the smartphone Global Positioning System locating feature to prevent geotagging and the use of a commercially available smartphone EXIF data removal application.

Handling identifiable PHI

Electronic media such as email, SMS, or multimedia messaging service (MMS) facilitate rapid communication and can improve health-care delivery [3,23]. With these expanded care delivery tools, health-care professionals must be mindful of the HIPAA regulations and requirements for handling identifiable PHI. Standard SMS and MMS texting of identifiable PHI data do not satisfy HIPAA requirements because these media are not encrypted, and many smartphones cannot encrypt data [24]. Even with smartphones equipped to encrypt data, standard SMS texting does not offer secure (encrypted) data transmission; the data may be stored in central servers that are not HIPAA compliant.

The Joint Commission and the Centers for Medicare and Medicaid Services have recommended that health-care organizations have policies prohibiting SMS and MMS texting of identifiable information and photographs from personal mobile devices [25,26]. Although the Centers for Medicare and Medicaid Services later allowed texting of identifiable patient information with secure (encrypted) platforms, the texting of patient care orders is still prohibited, regardless of the platform being used [27]. Proprietary messaging services are now available, with secure platforms and servers that are HIPAA compliant for managing identifiable PHI [28,29]. Even so, there are as yet no accepted standards or regulations to guide the evolution of these services [28].

Unlike standard SMS and MMS messaging, electronic medical record (EMR) systems provide an excellent means to store and share identifiable PHI. These systems are HIPAA compliant, use frequently changing passwords for security, and are frequently backed-up to protected servers. The EMR offers a secure, intra-system sharing platform; several vendors now offer applications for

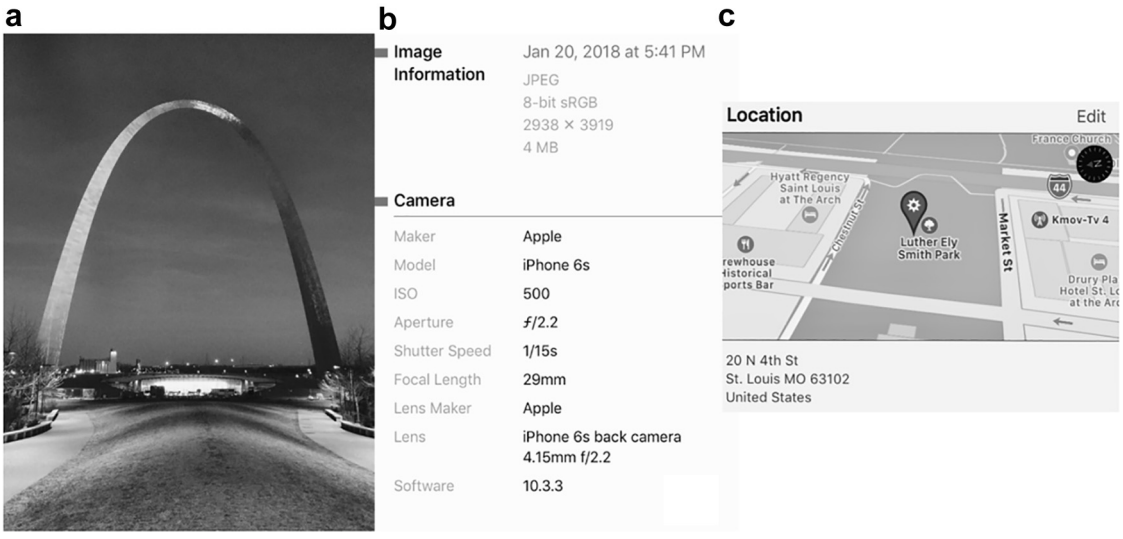

Figure 2. Captured photographic image (a), EXIF data and timestamp embedded within photograph's file (b), and EXIF geotagging location data embedded in photograph's file (c).

the upload of clinical photographs into EMRs [2]. EMR systems are not easily accessed by outside computers and smartphones, however, thereby limiting their use in data transmission among providers [30]. In addition, EMR systems are susceptible to attacks by computer hackers [30]. Similar to EMR systems, intrasystem email platforms are another tool within many health-care systems that while encrypted, usually lack the convenience and streamlined use of smartphone texting.

Is consent needed for treatment photographs?

Traditional informed consent refers to patient autonomy in considering the risks, benefits, and alternatives of available treatment options [31]. Section 164.506 of the Privacy Rule distinguishes between "verbal agreements," "consents (written)," and "authorizations (written)." "Consent" is defined as written permission to use and disclose identifiable PHI for treatment, payment, and health-care operations. "Authorization" is the written permission required for all other uses and disclosures of identifiable information [16]. Both consent and authorization are written, in contrast to simple "verbal agreements" that can accommodate situations where it is impractical to obtain written permission to share a patient's information [16].

With regard to identifiable PHI and photographs, the Final Privacy Rule states that "we require covered health care providers who have a direct treatment relationship with an individual to obtain a general 'consent' from the individual in order to use or disclose identifiable PHI about the individual for treatment" [16]. Consents for medical treatment and billing routinely obtained by hospitals and offices generally address the acquisition, sharing, and recording of identifiable PHI for patient treatment; this will include clinical photographs that are used for medical treatment. If patient photographs which contain identifiable PHI are used for purposes other than treatment of the individual (ie, education, research, and publication), then a separate written authorization from the patient is required. In contrast, photographs which have undergone the deidentification process are no longer considered identifiable PHI and, as such, are not subject to the handling requirements of HIPAA [16,17].

Summary

Photographs that can be linked to a patient are considered identifiable PHI, and therefore, their handling, sharing, and storage are subject to HIPAA requirements. Clinical photographs that have been deidentified in accordance with HIPAA/Privacy Rule guidelines are harder to link to an individual patient and are therefore not considered PHI and escape HIPAA requirements. An understanding of this difference is important to practitioners who want to facilitate clinical care using patient photographs, while respecting patient privacy and minimizing noncompliance risk.

References

[1] Reardon M. Text messaging explodes in America. CBS News. CNET. https://www.cbsnews.com/news/text-messaging-explodes-in-america/; 2008. [Accessed 9 September 2018].

[2] Harting MT, DeWees JM, Vela KM, Khirallah RT. Medical photography: current technology, evolving issues and legal perspectives. Int J Clin Pract 2015;69:401.

[3] Fjeldsoe BS, Marshall AL, Miller YD. Behavior change interventions delivered by mobile telephone short-message service. Am J Prev Med 2009;36:165.

[4] Chow CK, Redfern J, Hillis GS, et al. Effect of lifestyle-focused text messaging on risk modification in patients with coronary artery disease: a randomized clinical trial. JAMA 2015;314:1255.

[5] Shah DR, Galante JM, Bold RJ, Canter RJ, Martinez SR. Text messaging among residents and faculty in a university general surgery residency program: prevalence, purpose, and patient care. J Surg Educ 2013;70:826.

[6] Frizzell JD, Ahmed B. Text messaging versus paging: new technology for the next generation. J AM Coll Cardiol 2014;64:2703.

[7] Goldfarb J, Kayssi A, Devon K, Rossos PG, Cil TD. Smartphones and patient care: exploring the use of text-based messaging for patient-related communication. Surg Innov 2016;23:305.

[8] McKnight R, Franko O. HIPAA compliance with mobile devices among ACGME programs. J Med Syst 2016;40:129.

[9] Drolet BC, Marwaha JS, Hyatt B, Blazar PE, Lifchez SD. Electronic communication of protected health information: privacy, security and HIPAA compliance. J Hand Surg Am 2017;42:411.

[10] Pryzybylo JA, Wang A, Loftus P, Evans KH, Chu I, Shieh L. Smarter hospital communication: secure smartphone text messaging improves provider satisfaction and perception of efficacy, workflow. J Hosp Med 2014;9:573.

[11] Chan C, Charette J, Dumestre DO, Fraulin FO. Should 'smart phones' be used for patient photography? Plast Surg (Oakv) 2016;24:32.

[12] Rimoin L, Haberle S, Aspey LD, Grant-Kels JM, Stoff B. Informed consent, use, and storage of digital photography among Mohs surgeons in the United States. Dermatol Surg 2016;42:305.

[13] Accetta P, Accetta J, Kostecki J. The use of digital cameras by US dermatologists. J Am Acad Dermatol 2013;69:837.

[14] Milam EC, Leger MC. Use of medical photography among dermatologists: a nationwide online survey study. J Eur Acad Dermatol Venereol 2018;32:1804.

[15] Health insurance portability and accountability Act of 1996, public law 104-191. https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf; 1996. [Accessed 9 August 2018].

[16] Final privacy rule, federal register, vol. 65, No. 250; 45 code of federal regulations parts 160 and 164: standards for privacy of individually identifiable health information; final rule. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf?language=es; 2000. [Accessed 9 August 2018].

[17] HHS.gov. HIPAA for professionals. Workshop on the HIPAA privacy rule's de-identification standard. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/2010-de-identification-workshop/index.html. [Accessed 9 August 2018].

[18] Proposed privacy rule, federal register, vol. 64, No. 212; 45 code of federal regulations parts 160 and 164: standards for privacy of individually identifiable health information; proposed rule. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/privacyrule/1999nprm.pdf?language=es; 1999. [Accessed 9 August 2018].

[19] Guidance regarding methods for de-identification of protected health information in accordance with the health insurance portability and accountability Act (HIPAA) privacy rule. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf; 2012. [Accessed 9 August 2018].

[20] Meta resources: a guide to metadata standards and best practices for image creators, distributors, users, and developers. http://photometadata.org/META-Resources. [Accessed 2 September 2018].

[21] PhotographyVox. EXIF data explained- what is EXIF data?. http://www.photographyvox.com/a/exif-data-explained/. [Accessed 2 September 2018].

[22] Mikkelson R. Fact check: smartphone pictures pose privacy risks. https://www.snopes.com/fact-check/smartphone-pictures-pose-privacy-risks/. [Accessed 2 September 2018].

[23] Koivunen M, Niemi A, Hupli M. The use of electronic devices for communication with colleagues and other healthcare professionals- nursing professionals' perspectives. J Adv Nurs 2015;71:620.

[24] Toth C. Five ways to ensure secure text messaging in your medical practice. Physicians Practice. http://www.physicianspractice.com/mobile/five-ways-ensure-secure-text-messaging-your-medical-practice. [Accessed 9 September 2018].

[25] Clarification: use of secure text messaging for patient care is not acceptable. The Joint Commission Perspectives. https://www.jointcommission.org/assets/1/6/Clarification_Use_of_Secure_Text_Messaging.pdf; 2016. [Accessed 11 August 2018].

[26] Security standards: technical safeguards. HIPAA security series. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf?language=es. [Accessed 9 September 2018].

[27] Texting of patient information among healthcare providers. CMS center for clinical standards and quality/survey & certification group (ref: S&C 18-10-ALL). https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertificationGenInfo/Downloads/Survey-and-Cert-Letter-18-10.pdf; 2017. [Accessed 30 July 2017].

[28] Samora JB, Blazar PE, Lifchez SD, Bal BS, Drolet BC. Mobile messaging communication in health care: rules, regulations, penalties, and safety of provider use. JBJS Rev 2018;6:e4.

[29] Landman A, Emani S, Carlile N, et al. A mobile app for securely capturing and transferring clinical images to the electronic health record: description and preliminary usability study. JMIR Mhealth Uhealth 2015;3:e1.

[30] Thomas VA, Rugeley PB, Lau FH. Digital photograph security: what plastic surgeons need to know. Plast Reconstr Surg 2015;136:1120.

[31] Hall MA, Orentlicher D. Health care law and ethics in a nut shell. Minnesota: Thomson Reuters; 2011.