Volume 21 Number
September 2015

Review

Review of digital image security in Dermatology

Colton Nielson BS, Cameron West MD, Ikue Shimizu MD

Dermatology Online Journal 21 (10): 1

Texas Tech University Health Sciences Center, Department of Dermatology

Correspondence:

Cameron West, M.D.
Phone: (806) 743-1842
Fax: (806) 743-2933
Cameron.west@ttuhsc.edu

Abstract

The inherently visual nature of dermatology naturally lends itself to photography. As technology has evolved, smartphone cameras have become ubiquitous and have the potential to improve education and patient care in dermatology. Although patients and physicians may agree that photography can improve patient care, there are certain risks involved with smartphone photography in the medical field. Perhaps most concerning is the number of dermatologists using smartphones to take unsecured images in their daily practice. A recent study revealed that 22% of surveyed dermatologists used smartphone cameras multiple times per day in their practice. Dermatologists may also overestimate patient comfort with smartphone use in clinical photography. We present a review of the use of smartphones in dermatology and address the potential lack of security and accompanying ethical dilemmas.

Keywords: Smartphone, iPhone, digital image

Introduction

Improvements in digital photography have enhanced efficiency in taking photographs and the resolution of medical images [1, 2]. It has become an invaluable asset in many fields, but especially in dermatology. Many say it has become the ‘standard of care’ offering the most efficient method to observe dermatologic lesions over time and assess outcomes [1, 2]. Yet, the nature of digital technology allows images to be easily copied and transferred. Uncontrolled distribution of digital images provides opportunities for unauthorized individuals to access protected patient information in the form of clinical images [2].

Smartphones and Digital Images in Dermatology

Secure storage of digital images is necessary to protect patient privacy. In the experience of the authors, many smartphones are also connected to one or more cloud storage servers. Although this facilitates sharing of images and can act as backup storage for any critical images, the security of images stored on smartphones and through cloud computing is, in general, insufficient to protect patient photographs. In 2012, the New York Times reported that once an Apple iPhone®, iPod Touch®, or iPad ® owner grants permission for an application to access location information from their device, the application can potentially copy their photo library [2]. In several high profile examples, celebrity photos have been leaked onto the Internet after their phones were hacked [3]. Apple has since fixed the security gap that allowed the attacks to occur, yet opportunities for security breaches remain [4].

Recent results from a study published in the Journal of the American Academy of Dermatology showed 89% of dermatologists surveyed agreed that photography improved patient care [5]. Moreover, a study in Australia revealed that 100% of dermatologists surveyed utilize their personal smartphones for patient photography [6]. Eighty-five percent of these physicians had stored over 100 patient photographs on their smartphones, whereas 62% had stored 200 or more [6].

Kunde et al. found the main reasons provided by practicing dermatologists for clinical photography was treatment and disease monitoring and to gain advice from their peers or consultants [6]. Accetta et al. reported forty-four percent of clinicians used digital images to confirm biopsy sites [5]. Of those surveyed by Kunde et al., 92% reported texting or e-mailing images to colleagues for advice or opinion, whereas only 54% reported routinely disclosing to the patient the identity of the third party [6]. Similarly, Anyanwu found 74% of surveyed dermatologists reported receiving photographs from colleagues through texts and 80% through e-mail or other methods not properly secured and encrypted [7]. Hubbard et al. discovered that 21% of dermatologists used the patient's name to identify an image, either to send via email or for storage purposes [2].

Risks with Smartphone Digital Imaging

The practices described above can expose physicians to the potential for Health Insurance Portability and Accountability Act (HIPAA) violations, which carry heavy fines and penalties and could jeopardize an otherwise successful practice. Many providers may not recognize HIPAA applies to the storage and transfer of clinical photographs [7]. In addition, standard cloud storage options are not necessarily encrypted to HIPAA standards. Secure cloud storage options that adhere to HIPAA currently exist, but may not be accessible owing to costs or lack of knowledge regarding available resources [8].

A recent survey study by Accetta et al. revealed ninety-one percent of surveyed dermatologists report owning a digital camera for personal use [5]. Smartphones are usually more portable than a standalone digital camera, and may help minimize these barriers to digital photography. This may be a reason that over 90% of surveyed dermatologists under the age of 40 reported using some form of photography in general practice, as opposed to 76% of dermatologists 60 years and older [5]. The available data suggests younger dermatologists appear to be most responsible for the 'smartphone era' in dermatology [5]. Perhaps most concerning, neither patient safety nor fear of HIPAA violations were cited as reasons for refraining from the use of any form of digital imaging in daily practice. Rather, responses included time consuming (54%), complexity (21%), and cost (18%) [5].

Unlike most digital cameras, however, the transmission capabilities of smartphones make them uniquely vulnerable to potential privacy breaches. A standalone digital camera can be locked away at the end of the clinic day; a smartphone will generally accompany its owner home, since it cannot serve its main function of a communication device otherwise. There is both a potential of physical loss of device as well as issues of transmission security. Although many modern smartphones now come equipped with a remote wipe feature, this does not address wider security issues such as non-encrypted communications, cloud security breaches, and phone hacks. Once an image is transmitted, the sender has no control over security measures at the receiving device, making the data vulnerable while in transit and once received by another party.

Another significant issue is that dermatologists tend to overestimate patient comfort with their physician using a personal phone for use in clinical photography. Anyanwu et al. reported 61% of dermatologists surveyed believed that patients were comfortable with the use of a physician's smartphone for clinical photographs, whereas a survey conducted by Leger, et al showed that only 32% of patients were comfortable with this practice [7, 9]. Furthermore, a survey of 300 patients by Hsieh et al. shows the majority of patients preferred a hospital-owned camera (97.7%) over the use of personal photographing equipment (27.5%) or a physician's smartphone camera (27.2%) [9].

Discussion

In conclusion, dermatologists often use clinical images to assist with diagnosis and disease monitoring and also for teaching purposes [11, 12]. With the evolution and convenience of smartphones, many dermatologists now resort to smartphones to capture these images. Cameras on current smartphones are able to capture images that are relatively equivalent in quality to standard point-and-shoot digital cameras and smartphones are by nature more available moment by moment. However, smartphones are not necessarily secure and the data stored on them is also possibly unsecure. Many devices have automatic cloud upload options, in which a majority of images are automatically uploaded and shared through cloud technology. As well-publicized breaches in security demonstrate, such cloud storage of patient images have a potential to breach HIPAA regulations. Even without cloud storage backup, loss of a device remains a potential breach of security. Furthermore, studies have revealed inconsistent consent of patients for photography within clinics [1, 2, 7].

Until these problems are more widely recognized, the practice of capturing, storing, and sending photographs will continue to create gaps in the maintenance of patient privacy. As imaging and technology continue to improve, physician education on how to safely utilize technology in a manner that maintains the privacy of patients will become increasingly important. Furthermore, we must evaluate available resources to facilitate data storage practices and to maintain sufficient security.

At minimum, consent for medical photography should be a universal requirement to appropriately inform and protect the patient [11, 12]. If consent is only required for patient-identifying images, the definition of identifiable becomes subjective [1, 11]. These consents should detail the lack of security and protection currently provided by most forms of online technology, including smartphones and their storage mechanisms, if such technology is used. Consents should also address the potential sharing of images with a third party, identify potential third parties, and method of communication.

Moreover, physicians should be aware that a failure to use secure communications can result in a HIPPAA violation [15]. Each unsecured communication is considered a violation and may result in a fine of up to $50,000 [15]. Multiple violations can add up to the maximum penalty of $1.5 million in fines for identical violations each year [15].

Potential long-term solutions include HIPAA-compliant text messages and storage cloud servers, EHR systems, and even specialized social media websites [7, 8, 15]. Utilization of secure smartphone applications, which allow secure transfer of photographs between smartphones, may facilitate a balance between the convenience of technology and commitment to patient confidentiality [7]. Przybylo et al. concluded from a prospective, cluster-randomized controlled trial at Stanford Hospital that smartphone based, HIPAA-compliant group messaging applications improved provider perception of communication, while providing the information security that paging and commercial cellular networks do not [13].

Another secure method by which health care providers can send information to both patients and other providers involves the messaging features within the EHR system [15]. Providers can communicate with patients through the patient portal and send orders to other providers via computerized physician order entry (CPOE) [14]. In addition, providers can share information with other medical providers by participating in a Health Information Exchange [14]. Several examples of technology that facilitate HIPAA compliant communication are included (Table 1).

Table 1. Sampling of several HIPPA compliant storage and communication systems

HIPPA Compliant Technology	Company	System Description	Website
Imprivata Cortext®	Imprivata	HIPAA-compliant communications platform	http://www.imprivata.com/secure-communications[14]
Firehost Secure Cloud Hosting®	FireHost Inc.	HIPAA-compliant cloud storage	http://www.firehost.com/[15]
CareCloud®	CareCloud	HIPAA-compliant cloud storage	http://www.carecloud.com/[16]
qliqSoft®	qliqSOFT	HIPAA compliant text messaging	https://qliqsoft.com/[17]
Medigram®	Medigram, Inc.	HIPAA-compliant group messaging (HCGM)	https://medigram.com/[18]
HippaChat®	Everbridge	HIPAA-compliant text messaging and video calls like FaceTime or Skype	http://www.hipaachat.com/[19]
FotoFinder Handyscope®	FotoFinder Systems	HIPAA-compliant iPhone photo application	http://www.handyscope.net[20]

tKDerm Touch®	TKDERM dermatological database	HIPAA-compliant iPhone photo application	http://www.tkderm.sourceforge.net[21]

Guidelines for HIPAA-compliant, cloud-based storage are evolving and still indistinct. Caution must be taken towards all cloud service providers (CSPs) that claim to be HIPAA certified [22]. The U.S. Department of Health and Human Services (HHS), the entity responsible for HIPAA, does not require or formally recognize any HIPAA certification programs for CSPs [22]. However, certain principles should be followed in order to ensure HIPAA-compliant cloud storage (Table 2). These principles are based on broad guidelines for HIPAA compliance issued by HHS. [22, 23, 24] Should questions arise, it is advisable to contact the group or institution's privacy officer.

Table 2. Major Requirements for HIPAA-Compliant Cloud Storage

Cloud Service Providers (CSP): Maintenance of HIPAA compliance	**Description**
Undergo annual independent audits[22]	Audits of CSP data center operations and cloud infrastructure, preferably measured against the office of Civil Rights (OCR) HIPAA Audit Protocol. The protocol provides audit criteria utilized by OCR, the entity responsible for enforcing HIPAA compliance[22]
Knows and follows the HIPAA privacy and security rules[22]	**HIPAA Privacy Rule:** Requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization[22, 24] ▪ No impermissible uses or disclosures of PHI ▪ Provide breach notification to the Covered Entity ▪ Provide either the individual or the Covered Entity access to PHI ▪ Disclose PHI to the Secretary of HHS, if compelled to do so ▪ Provide an accounting of disclosures **HIPAA Security Rule:** Requires Implementation of technical security measures to guard against unauthorized access to Protected health information (PHI) transmitted over an electronic network[22, 24] ▪ Unique User Identification(required): assign a unique name or number for identifying/tracking user identity ▪ Emergency access procedure (required): establish procedures for obtaining necessary ePHI during an emergency ▪ Audit controls (required): implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI ▪ Authentication(required): Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed
Provide a business associate agreement (BAA)[22]	The BAA specifies what the supplier will do for the covered entity and that it will comply with the HIPAA requirements to secure the privacy of Protected health information[22]
Encrypt protected health information (PHI)[22]	Encryption is considered the gold standard for data security. HIPAA rules state the use of encryption is 'strongly recommended' but is not yet mandatory[22, 24] ▪ If encryption is not used by a covered entity or business associate, clear documentation of the risk analysis, the decision not to encrypt, and the specifics of an equivalent level of protection must be in place to document the efforts to protect ePHI.
HIPAA breach notification rule[22]	The breach notification rule requires healthcare providers to notify

	patients when there is a breach of unsecured PHI and also prompt notification of U.S. Department of Health and Human Services (HHS) in breaches of unsecured PHI.[22]

In conclusion, there are numerous options available to communicate using a HIPAA-compliant platform. Efforts must be made to initiate change and educate both dermatologists and patients on the risks involved with images taken by smartphones. This review aims to provide insight to assist physicians, specifically dermatologists, to develop a HIPAA compliant system when using smartphones and digital imaging in daily practice.

References

1. Lakdawala, Nikita, Demian Fontanella, and Jane M. Grant-Kels. "Ethical Considerations in Dermatologic Photography." Clinics in Dermatology 30.5 (2012): 486-91. [PMID: 22902218]
2. Hubbard, V. G., D. J. Goddard, and S. L. Walker. "An Online Survey of the Use of Digital Cameras by Members of the British Association of Dermatologists." Clinical and Experimental Dermatology 34.4 (2009): 492-94. [PMID: 19175618]
3. "Is Your Smartphone Photo Library Secure? - ACSN Security." ACSN Security. https://www.acsn.co.uk/whos-looking-at-your-photos/, Accessed 11 Apr. 2015.
4. "Apple Toughens iCloud Security after Celebrity Breach." http://www.bbc.com/news/technology-29237469, 17 Sept. 2014. Accessed11 Apr. 2015.
5. Accetta, Peter, Julia Accetta, and James Kostecki. "The Use of Digital Cameras by US Dermatologists." Journal of the American Academy of Dermatology 69.5 (2013): 837-38. [PMID: 24124827]
6. Kunde, Lauren, Erin Mcmeniman, and Malcolm Parker. "Clinical Photography in Dermatology: Ethical and Medico-legal Considerations in the Age of Digital and Smartphone Technology." Australasian Journal of Dermatology 54.3 (2013): 192-97. [PMID: 23713892]
7. Anyanwu, Cynthia O., and Jules B. Lipoff. "Smartphones, Photography, and Security in Dermatology." Journal of the American Academy of Dermatology 72.1 (2015): 193-95. [PMID: 25497925]
8. Gerard, Perry, Neil Kapadia, Patricia T. Chang, Jay Acharya, Michael Seiler, and Zvi Lefkovitz. "Extended Outlook: Description, Utilization, and Daily Applications of Cloud Technology in Radiology." American Journal of Roentgenology 201.6 (2013): W809-811. [PMID: 24261387]
9. Leger, MC, T. Wu, A. Haimovic, R. Kaplan, M. Sanchez, D. Cohen, EA Leger, and JA Stein. "Patient Perspectives on Medical Photography in Dermatology." Dermatologic Surgery (2014): 1028-037. [PMID: 25099296]
10. Hsieh, C., D. Yun, AC Bhatia, and JT Hsu. "Patient Perception on the Usage of Smartphones for Medical Photography and for Reference in Dermatology." Dermatologic Surgery (2015): 149-54. [PMID: 25533160]
11. Berle, I. "Clinical Photography and Patient Rights: The Need for Orthopraxy." Journal of Medical Ethics 34.2 (2008): 89-92. [PMID: 18234945]
12. "Informed Consent for Medical Photographs." Genetics in Medicine 2.6 (2000): 353-55. [PMID: 11339658]
13. Przybylo, JA. "Smarter Hospital Communication: Secure Smartphone Text Messaging Improves Provider Satisfaction and Perception of Efficacy, Workflow." Journal of Hospital Medicine. (2014): 573-78.[PMID: 11339658]
14. "Imprivata." Secure Communications for Healthcare. http://www.imprivata.com/secure-communications. Accessed 21 April. 2015.
15. "Managed Hosting." Secure Cloud Hosting. http://www.firehost.com. Accessed 17 April. 2015.
16. "Healthcare Software | Medical Billing | EHR | CareCloud." http://www.carecloud.com. Accessed 21 April. 2015.
17. "HIPAA Compliant Messaging Platform for Secure Texting https://qliqsoft.com. Accessed 21 April 2015.
18. "Healthcare Communication Made Simple." https://medigram.com. Accessed 26 April2015.
19. "About - FAQ - Hipaachat." About – FAQ. http://www.hipaachat.com. Accessed 17 April 2015.
20. "Handyscope - Mobile Dermatoscope: Handyscope." www.handyscope.net. Accessed 26 April 2015.
21. "TkDerm : Dermatological Database." http://www.tkderm.sourceforge.net. Accessed 26April 2015.
22. "Five Things to Know about HIPAA-compliant Cloud Storage." http://www.peak10.com/five-things-to-know-about-hipaa-compliant-cloud-storage/. 27 Mar. 2014. Web. 25 July 2015.
23. www.hhs.gov. Web. 25 July 2015
24. “How do I become HIPPA compliant? (A checklist)” https://www.truevault.com/blog/how-do-i-become-hipaa-compliant.html