APS
Archives of Plastic Surgery

Clinical Practice and Education
Review Article

# Safe clinical photography: best practice guidelines for risk management and mitigation

Rajiv Chandawarkar[1], Prakash Nadkarni[2]

[1]*Department of Plastic Surgery, Ohio State University Wexner Medical Center, Columbus, OH;* [2]*College of Nursing, University of Iowa, Iowa City, IA, USA*

Clinical photography is an essential component of patient care in plastic surgery. The use of unsecured smartphone cameras, digital cameras, social media, instant messaging, and commercially available cloud-based storage devices threatens patients' data safety. This paper Identifies potential risks of clinical photography and heightens awareness of safe clinical photography. Specifically, we evaluated existing risk-mitigation strategies globally, comparing them to industry standards in similar settings, and formulated a framework for developing a risk-mitigation plan for avoiding data breaches by identifying the safest methods of picture taking, transfer to storage, retrieval, and use, both within and outside the organization. Since threats evolve constantly, the framework must evolve too. Based on a literature search of both PubMed and the web (via Google) with key phrases and child terms (for PubMed), the risks and consequences of data breaches in individual processes in clinical photography are identified. Current clinical-photography practices are described. Lastly, we evaluate current risk mitigation strategies for clinical photography by examining guidelines from professional organizations, governmental agencies, and non-healthcare industries. Combining lessons learned from the steps above into a comprehensive framework that could contribute to national/international guidelines on safe clinical photography, we provide recommendations for best practice guidelines. It is imperative that best practice guidelines for the simple, safe, and secure capture, transfer, storage, and retrieval of clinical photographs be co-developed through cooperative efforts between providers, hospital administrators, clinical informaticians, IT governance structures, and national professional organizations. This would significantly safeguard patient data security and provide the privacy that patients deserve and expect.

**Keywords** Data encryption / Electronic health records / Patient safety / Patient protection / Photography

**Correspondence:** Rajiv Chandawarkar
Department of Plastic Surgery, Ohio State University Wexner Medical Center, 915 Olentangy River Rd, Suite 2100 Columbus, OH 43212, USA
Tel: +1-614-293-5000
Fax: +1-614-293-1213
E-mail: chandawarkarmd@gmail.com

Received: January 13, 2021 • Revised: March 4, 2021 • Accepted: April 9, 2021
pISSN: 2234-6163 • eISSN: 2234-6171 • https://doi.org/10.5999/aps.2021.00262 • Arch Plast Surg 2021;48:295-304

## INTRODUCTION

Healthcare organizations (HCOs) have a history of suboptimal security practices, and have consequently been lucrative targets for hackers: >41 million patient records were breached in 2019 [1] and the total estimated damage from ransomware is >$20 billion [2]. In December 2020, hackers breached the records of a large private plastic surgery chain in Britain that was known for catering to celebrities, and stole 900 GB of "before vs. after" images that they threatened to release unless paid a ransom [3].

 

Patient data safety is a collective effort. However, while HCO employees in the US undergo mandatory Health Insurance Portability and Accountability Act (HIPAA) training, safe management of image data is not emphasized in either the content or the accompanying content-mastery quizzes. Consequently, relatively few US plas tic surgeons tend to be aware of the risks of routine use of cellphones to take and transmit pictures and store them on home computers. Further, while clinical photography is essential to plastic-surgery practice (Fig. 1), the literature is lacking in terms of full recognition of the risks and explorations of mitigation strategies. Finally, the US's guidelines for safe clinical photography lag behind those of the UK, Canada, Australia, and the EU. This work:

- Identifies potential risks of clinical photography and heightens awareness of safe clinical photography.
- Evaluates existing risk-mitigation strategies globally, comparing them to industry standards in similar settings.
- Formulates a framework for a risk-mitigation plan for avoiding data breaches by identifying the safest methods of picture taking, transfer storage, retrieval, and use, both within and outside the organization. We note that, since threats evolve constantly, the framework must evolve too.

Adopting this framework (or something similar to it) will strengthen the security around clinical photography in the US and help better manage digital safety concerns for patients, physicians, and institutions.

## METHODS

We searched both PubMed and the web (via Google) with the key phrases "patient safety," "'clinical photography," "photography transfer and storage," "ethics of clinical photography," "national guidelines of clinical photography," "digital security," and "digital security of clinical photography," and (for PubMed) we expanded the search to child terms and related terms. Through the search, we:

1. Identified the risks and consequences of data breaches in individual processes in clinical photography: image capture (and temporary/local storage), transmission, permanent storage, and retrieval/use.
2. Determined current, although not necessarily optimal, clinical-photography practices in the US and abroad.
3. Identified how clinicians perform safe patient photo-taking and storage.
4. Evaluated current risk mitigation strategies for clinical photography. We considered guidelines from professional organizations, governmental agencies, and non-healthcare industries.

Finally, we combined lessons learned from the steps above into a comprehensive framework that could contribute to national/international guidelines on safe clinical photography.

We did not perform our own survey of clinician practices because surveys on this subject (see the "Current Practices" sub-

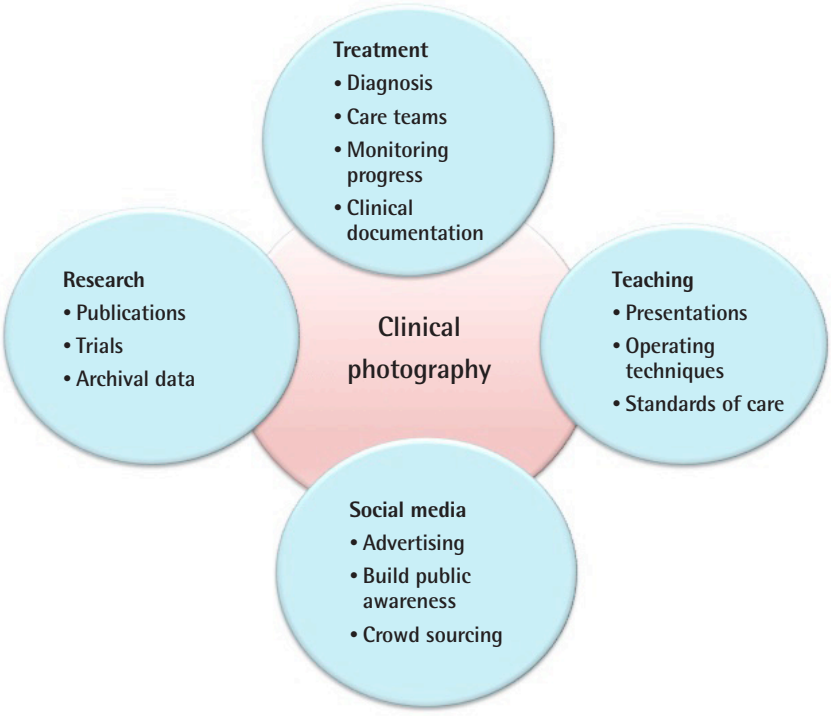


**Fig. 1.** Important functions of clinical photography.

section of Results), including clinician behavioral lapses [4-6], have already been reported.

## RESULTS

### Risk in individual clinical photography processes

Each of the four processes of clinical photography—capture, transfer, storage, and retrieval/use—poses a different type (quality) and level (quantity) of risk (Fig. 2). Understandably a data breach at the capture level would involve far fewer images (and patients) than a breach at the storage level, where the breach would also involve time-tagged data (e.g., before- and after-treatment pictures, disease-tracking, etc.). In this section, we only consider the risks of each process. These are not insurmountable, and the Discussion section considers possible solutions.

#### *What information can a digital photo disclose?*

A photo, obviously, can disclose personal health information (PHI). Photo PHI includes the patient's face, name or initials, date of birth, date of treatment, and externally visible birthmarks, moles, or tattoos. However, even without PHI, indirectly identifiable information can be disclosed that enables a motivated individual to re-identify a specific patient (e.g., a celebrity).

All digital-photography devices (including cellphones) use a format called EXIF (Exchangeable Image File), where a set of data elements is appended to the image, which itself typically employs the JPEG (Joint Photography Experts Group) format. EXIF elements include the date and time when the photo was taken, the camera manufacturer and model (sometimes even the serial number), shutter speed, camera mode, and aperture. Devices with global positioning system (GPS) capability will also record the "geotag" (i.e., the location where the photo was taken), as latitude, longitude, and elevation (all at about 100-m resolution, which would identify the caregiver's office/institution).

These terms could help identify individual patients if one knows other facts about them (e.g., that they had surgery in a particular city on a certain date). In non-PHI contexts, law enforcement agencies (including the National Security Agency) routinely attempt to harvest EXIF data to geolocate individuals of interest (either the photographer/s or the subject being photographed).

EXIF data can be removed: Facebook and Twitter do this automatically with uploaded images. Numerous free and commercial tools also give fine control over the EXIF elements to be deleted: even Windows File Explorer will let you do this one JPG file at a time. Furthermore, geotagging can be disabled on both smartphones and digital cameras: on the iPhone, this is accomplished by turning off Location Services in the Camera App.

#### *Image capture: advantages and disadvantages of different approaches*

While most academic institutions employ clinical photographers and/or provide departmental digital cameras, these have

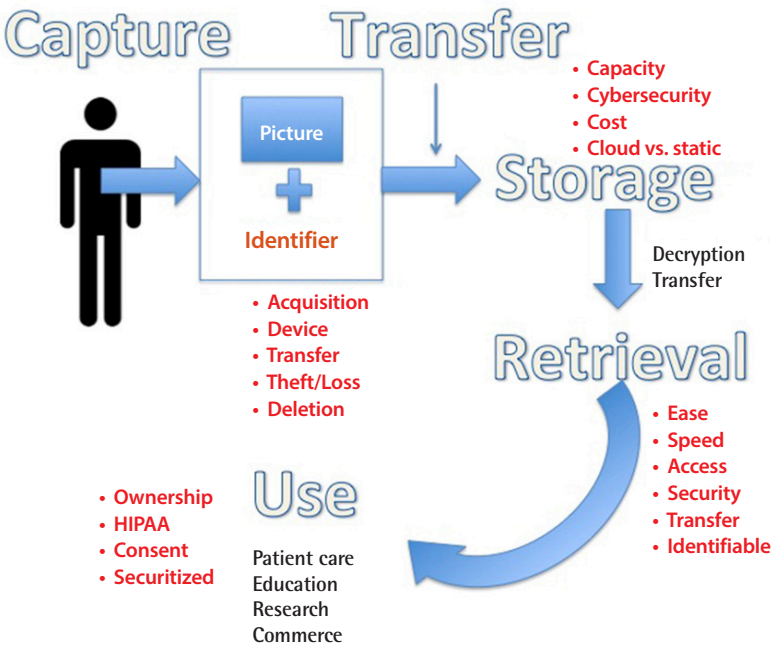


**Fig. 2.** Four main phases of clinical photography that pose unique risks for data breaches. HIPAA, Health Insurance Portability and Accountability Act.

the following drawbacks: (1) for both photographers and shared cameras, lack of availability when needed (e.g., at multiple locales simultaneously, during off-duty hours, in operating rooms, outpatient sites, or bedside) is an issue; (2) with standard digital-camera features like autofocus and automatic flash that enable "point-and-shoot," the expertise level to create quality photos has dropped drastically. Hiring dedicated photographers is consequently hard to justify financially; (3) for department cameras, loss/theft and maintenance (e.g., battery replacement) are ongoing concerns [7,8]; or (4) many modern digital cameras (e.g., the Ricoh G800) [9], have a password function. The G800 allows two passwords, for administrator and user. However, the camera is not intended for group use: shared user passwords are as good as none. At best, every user must use his or her own SD card (which must be password-protected).

While smartphones offer "on-the-spot" availability, data-loss risks due to physical loss/theft/damage are amplified because they travel with the owner. Furthermore, their default operational mode is insecure: secure use requires additional diligence and expense [10].

#### *Image-transfer risks*

Transfer based on texting is insecure by default: one needs to use software that offers end-to-end encryption. Using social media poses even a greater threat to data security [8,11], mainly because social media providers' business model is based on monetizing their users' data (paradoxically, Facebook's WhatsApp software, when used for person-to-person messaging, offers secure end-to-end encryption).

#### *Storage risks*

A low-tech solution used in small practices is to back up a digital camera on a hard drive with two-factor authentication (password + biometrics) and no internet connectivity. The obvious problems are that: (1) retrieval for any purpose (sharing, research, publication) is cumbersome, requiring a removable device, such as a USB thumb drive; (2) tagging a file with a patient's name/MRN/DOS adds risks; or (3) failure to implement off-site backup storage can increase vulnerability to theft, loss, or device malfunctions.

#### *Retrieval and use risks*

Both the JPEG and EXIF components of a digital photo can be used as part of a "spear-phishing" attack (sending someone a message/file that pretends to come from a friend/colleague) to transmit malware. The LokiBot malware, which steals data from machines where it resides, conceals its source code in the body of JPG and PNG files [12] to escape detection by antimalware software that looks for special "signatures" (patterns of bytes) in attachments. For EXIF data, one phishing message hid the malware within the camera make and model fields, which have no size limits or restrictions on what they might contain [13]. The technique of concealing one file (malware) within another (image/video) is a special case of steganography ("concealed writing"), which was first used more than 2,500 years ago: a step-by-step tutorial illustrating concealment within JPEG files is available online [14].

## Current practices in clinical photography

The literature reveals that the use of smartphones for clinical photography is widespread and increasing rapidly, but the awareness of risks is not growing commensurately.

- In a survey of 300 French plastic surgeons [15], over 81% of respondents indicated that they "could not go on with their daily practice today without their smartphone." They stored photographs on their smartphones (50%) or synced with virtual storage (25.6%). Most (80.2%) used a dedicated secured smartphone application.
- In a Canadian survey [4], over 89% of responding Canadian plastic surgery residents and attending physicians used smartphones to take clinical photographs of patients. Over half (57%) stored these photos on their phones (of these, 73% stored clinical photos among personal photos; 26% had accidentally shown a clinical photo to friends or family).
- In a US survey of members of the American Society of Plastic Surgery and plastic surgery trainees [16], 82.8% of attendings were HIPAA-noncompliant when using stand-alone digital cameras, compared with 90.2% of trainees using smartphones. Both groups also breached HIPAA rules when using other photographic management modalities.

Risk unawareness extends beyond plastic surgery. In a survey of Australian dermatologists [5], 50% of respondents sent/received images on their smartphones at least weekly, usually by multimedia message or email. Almost half (46%) stored images on smartphones with limited security measures. Consent for photograph transmission was inadequately documented. Only 22% were aware of clear workplace policies regarding smartphone use. Most desired further education on digital image management.

## Official privacy and security legislation and guidelines

#### *US federal government legislation: HIPAA*

In the US, under HIPAA, an individual's PHI (from photos or otherwise) stays protected for 50 years after the death date [17]. HIPAA provides general recommendations [18,19] rather than specific prescriptions, such as technological solutions.

Patient photos that are used solely for intra-institutional training or teaching do not need express consent. However, photos for external use (conferences, seminars) do.

Common forms of HIPAA photo violations

- Disclosing photos without proper encryption and protection
- Sharing unauthorized photos of patients on social media
- Using photos in marketing campaigns without consent
- Taking patient photos out of the practice on devices

HIPAA guidelines for data transmission and storage

The HIPAA guidelines permit the use of cloud service providers (CSPs), provided the CSP complies with HIPAA rules (e.g., Eclipsys Corporation, provides a cloud option for its electronic health record [EHR] system: this benefits smaller organizations, which can thereby operate with a skeletal information-technology staff). The contract between an HCO and a CSP can also include provision of services such as data backup and recovery, encryption. Federal guidelines for use of cloud services are available [20]. The level of service specified in the contract depends on the HCO's assessment of risk.

***US state legislation***

In response to widespread data breaches and ransomware attacks, numerous individual states in 2020 enacted legislation to protect consumers' data in both healthcare and non-healthcare contexts. The details have been summarized elsewhere [21].

***The United Kingdom***

The Caldicott Principles

The UK has adopted a bold, refreshing approach to data sharing via the Caldicott Principles [22,23], as summarized below: (1) justify the purpose for using PHI. Do not use PHI unless absolutely necessary: use the minimum necessary PHI; (2) access to PHI should be on a strict need-to-know basis. Everyone with PHI access should be aware of their responsibilities: understand and comply with the law; (3) the duty to share information, in the patient's best interests, can be as important as the duty to protect patient confidentiality.

All the principles are commonsensical, and guidelines similar to the last exist elsewhere. Thus, the US Joint Commission emphasizes that HCO staff must elicit at least two identifiers from a patient at every encounter, to ensure that the right patient is being treated: patient safety takes priority over possible privacy loss.

UK NHS guidelines for cellphone use

The UK's Human Rights Act 1998, National Health Service (NHS) Act 2006, Health and Social Care Act 2012, Data Protection Act 2018, and General Data Protection Regulation (GDPR) 2018 provide national guidelines on the use of digital data capture and instant messaging software. The NHS encourages the use of a smartphone application that enables patient confidentiality and has secure data sharing [24]. A modestly updated version of the NHS guidelines is reproduced in the Discussion section. Inherent in these directives is the patient's right to request access to, location of, amendment to, or simple erasure of their pictures [25].

Other UK guidelines and implementations

The British Orthopedic Association Standards of Trauma guideline [26] and the National Institute for Health and Care Excellence (2017) guideline NG37 [27] highlight that hospitals have a responsibility to ensure that there is a protocol in place for photography for certain clinical conditions. These national guidelines have been put in a usable form to produce a Caldicott-compliant hospital imaging protocol used for open fractures [7].

***Canada***

The Canadian health system reveals a better understanding of some aspects of clinical photography, such as photograph retention and storage. Other processes, including capture and transfer, are not well described. National and provincial colleges (healthcare governance bodies in Canada) do not have explicit and readily available instructions regarding clinical photography using a smartphone and electronic transmission of patient information [28]. A comprehensive national guideline from the Canadian Medical Association serves as a reference for the responsible use of clinical photography with a mobile device [29].

***South Korea and Japan***

There are strict rules regarding clinical photographs, all of which are directed to the EHRs or can only be captured on a secured camera or institutional network.

***Australia***

In Australia, the Privacy Act (1988, amended 2020) governs privacy and protection of health data [30]. In addition, the Privacy Impact Assessment Register records details of privacy impact assessments conducted by the Department of Health since July 1, 2018 [31]. The Privacy (Australian Government Agencies–Governance) APP Code 2017 [32] requires that all agencies, including the Department of Health, must conduct a privacy impact assessment for all high-privacy-risk projects. Non-adherence can lead to imposition of fines [30].

*European Union*

In the European Union, the GDPR regulates and safeguards healthcare data privacy and protection [33]. It fully recognizes modern-day threats, and addresses both external threats (hackers, leaks) and guidelines for users. Additionally, however, violations of the GDPR are monitored, and wrongdoers are fined, as in the case of Bounty [34]. A list of fines above 100,000 pounds has been published [35].

Secure European servers for messaging data and user information exist in several locales, such as Frankfurt, Germany, and Dublin, Ireland.

### Risk-mitigation measures: approaches in industry

We will discuss risk mitigation as it specifically applies to digital-photography processes. In general, mitigation approaches (originally developed in industry) involve the following stages:

- Identify the risk.
- Analyze the risk: quantify threat severity, and understand the routes of exposure and how these threats work.
- Mitigate the risk.
- Monitor and review the effect of mitigation measures; revise the measures as needed.

An excellent book on electronic security is by Du [36]. The goal of cybersecurity standards in industry is to improve the security of information technology (IT) systems, networks, and critical infrastructures [37]. Several government resources are available that frame cybersecurity from the standpoint of sensitive information, knowledge sharing and development of best practices [38,39]. While all employees (including those of HCOs) are routinely made to take a course in basic security principles, the content of these courses has not kept pace with malware advances, and needs to be updated regularly.

## DISCUSSION

While photographs are critical components of patient care, providing useful timely information and enabling clinicians to serially monitor patients' progress, ignoring security risks in clinical photography is no longer tenable. Alarmingly, universal recommendations to ensure data security of patient photographs are conspicuously unavailable in the US. While guidelines are indeed available in countries with nationalized health systems [1], they must be applied piecemeal to individual HCOs within the US's fragmented healthcare system, resulting in much duplicated effort.

We suggest a framework of best practice guidelines by applying the lessons learned from abroad and from data security in non-healthcare industries. Care has also been taken to ensure that these guidelines preserve the inherent ease-of-use that smartphones provide (both for capturing photos and transferring/sharing photos), while maximizing the security of this process.

### Foundations of the proposed framework

A multilevel action-plan is based on the following foundational conditions (see Fig. 3 for examples):

- Mobile-device cameras are here to stay: Smartphones are increasingly used for clinical photography as they have good resolution and Internet connectivity, which allows faster communication between the care teams. This capability has been shown to improve patient care [40-43].
- The Caldicott Principles provide an excellent guide to managing patent data, emphasizing how safe data sharing helps improve patient care, while also making safe sharing our responsibility.

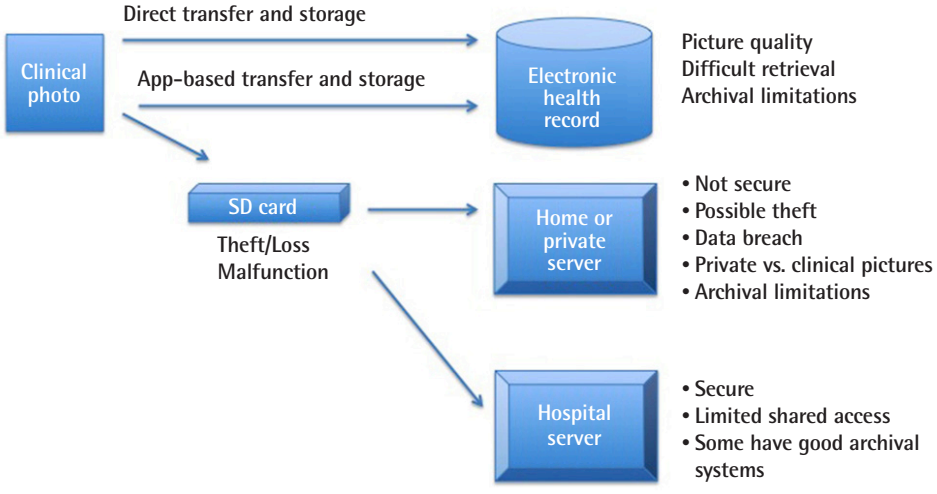


**Fig. 3.** Examples of methods to transfer and store clinical pictures.

- Robust cybersecurity measures developed in non-healthcare industries should be incorporated.
- A policy of maximizing ease and maximizing security will facilitate adoption.
- Basic risk-reduction practices should be deployed in everyday, real-time situations. This would allow us to rapidly deploy security measures right away, while a new secure system is being developed and deployed. While the system would still have vulnerabilities, these practices—which can be seen as the equivalent of wearing a mask in the coronavirus disease (COVID-19) pandemic—would at least help us avoid common mistakes.
- A system is only as strong as its weakest component. While we have considered the risks of image capture, transfer, storage, and retrieval separately earlier, any solution must address them together.

## Recommendations

A mobile app should be used to transfer image data from smartphone to archival storage: with a manual do-it-yourself approach, one or more steps may be accidentally omitted. Our recommendations are based on the UK NHS Guidelines for secure digital-photography infrastructure. These guidelines, reproduced below, specify the following requirements for the app and the accompanying infrastructure:

1. End-to-end encryption using 256-bit AES (Advanced Encryption Standard).
2. Verification of all users as medical professionals.
3. Two-factor authentication: PIN code+fingerprint and/or facial-recognition access to the app (separate from phone protection).
4. Remote wipe function. Ability to wipe all photographic data from the phone remotely in case of theft.
5. All messages are automatically deleted after 10 days.
6. Store photos on cell phones as briefly as possible, erasing them soon after transfer (Apps can be configured to do this automatically).
7. Audit trail of user data to detect fraud or intrusion (HIPAA mandates audit trails, but only for access to patient records).

To the above, we add the following recommendations:

- Smartphones must be configured for maximum security (password + biometrics, automatic EXIF removal, storage encryption, etc.) before using them for clinical photography. However, expecting non-technically adept clinicians to configure their personal smartphones is unreasonable. HCOs must provide preconfigured smartphones to clinicians whose job responsibilities include image capture (cloning software drastically reduces manual effort by allowing the configuration on one phone to be rapidly transferred automatically to other phones). HCOs must additionally provide secure image storage, either through the EHR itself (e.g., Epic Haiku/Cantor) or via secure image servers. Some EHRs limit storage, and therefore force users to save images as lower-resolution files, but as storage costs drop and capacity expands—since storage is still following Moore's Law—this technical limitation will hopefully become insignificant. Image servers could be local or cloud-based (e.g., Microsoft OneDrive). Either option incentivizes the prompt removal of image data from the smartphone. A comparative review of the latest (2020) smartphones by Google, Samsung, and Apple [44] indicates that even after configuration for maximal security (that exceeds the UK NHS's requirements above), ease of use does not suffer. While these phones are expensive, bulk-purchase costs are dwarfed by those of HIPAA-related fines or lawsuits.
- Digital cameras: Geotagging should be turned off. Clinicians should only use secured SD storage cards. (SDHC and SDXC cards support password protection.) Any SD card loss should be reported as soon as it is detected.
- Even if a patient's face or identifiable body part(s) are included, clinicians should not tag the image file name with PHI such as medical record number or patient name. If it is absolutely necessary to convey this information to a colleague, one should send a separate message or make a verbal phone call.
- If transferring images to colleagues via texting, one should only use a secure texting app with end-to-end encryption from sender to receiver.

### *Recommendations for solo practitioners, small groups, and home use*

Three modalities are commonly available, and each has its specific advantages and disadvantages. While working from home, some lines can become blurred. For instance, while working in the office, the internet connection is typically secure. However, when working remotely, we are responsible for our own Wi-Fi routers and internet connections. Most work-from-home employees probably connect to their hospital network via a virtual private network, but it is still important to secure one's home router. All clinicians using home devices should ensure that their routers consistently receive firmware updates. All cloud-based storage apps (paid or free) have access to clinical photographs, which makes them and their users easy targets. They cannot be used for clinical pictures.

When using a computer hard drive to store photos (as most

private practice providers do), the following guidelines are recommended: (1) create a routine—a regular system for taking photos off the cameras and cards and onto secure storage; (2) utilize encrypted storage by default, as well as encrypted Wi-Fi communication using a key. The most robust Wi-Fi protocol, WPA2, uses AES encryption; or (3) data-backup plans must include remote (e.g., off-site) storage of backups to ensure against physical damage to home or office. Cloud-based backup of encrypted files should also be considered.

### Reporting data breaches

Any breach should be taken seriously and should be reported and reviewed. Whenever in doubt about how to proceed with the use of clinical images, or a potential breach, the hospital administration should be contacted for advice.

### Professional organizations

We propose that professional organizations (American Society of Plastic Surgeons [ASPS], American Society for Aesthetic Plastic Surgery [ASAPS], American Council of Academic Plastic Surgeons [ACAPS]) consider creating national guidelines for each type of plastic surgical practice, applying universal rules for secure clinical photography. Ideas for such a framework were described several years ago in 2002 by Lee et al. [45]. Modifications based on different governmental regulations can be added as needed. Establishing a Commission on Safe Clinical Photography will help protect patients and physicians, define best practices, and limit damage due to breaches. A task force should be created to liaison with governmental agencies to update national guidelines for data security and risk management and create a repository of resources for clinicians who want to create a secure structure for their own clinical photography. Similar regulatory committees and resources are available for photojournalists whose work is as sensitive (Committee to Protect Journalists) (Table 1) [46].

**Table 1.** List of resources for photojournalists as an example of formatting similar resources for clinicians

| List of resources for photojournalist |
|---|
| Rory Peck Trust Digital Security Guide<br>https://rorypecktrust.org/freelance-resources/digital-security/ |
| CPJ's Emergency Response Resource Center<br>https://cpj.org/emergency-response/resource-center/ |
| CPJ's Technology Security Guide<br>https://cpj.org/wp-content/uploads/2020/05/guide.pdf |
| Reporters Without Borders' Seven digital security habits that journalists should adopt<br>https://rsf.org/en/news/seven-digital-security-habits-journalists-should-adopt |
| CPJ's links for other Digital Security guides<br>https://cpj.org/2019/09/digital-safety-diy-guides/ |
| The Freedom of the Press Foundation's Guides and Training<br>https://freedom.press/training/ |
| The NewsGuild of New York's list of Digital Security guides for journalists<br>https://www.nyguild.org/digital-security |
| Electronic Frontier Foundation's Security Education category archives<br>https://www.eff.org/issues/security-education |
| Electronic Frontier Foundation's Surveillance Self-Defense guides<br>https://ssd.eff.org/en |
| Witness's guides on Safety and Security<br>https://library.witness.org/product-tag/safety-and-security/ |
| The Guardian Project's secure apps and open-source software libraries<br>https://guardianproject.info/ |

CPJ, Committee to Protect Journalists.

## CONCLUSIONS

Developing best practice guidelines for the simple, safe, and secure capture, transfer, storage, and retrieval of clinical photographs is critical. Tools and technology to ensure security are available, while regulation and national oversight are not. This task will require heightened awareness and a cooperative effort between providers, hospital administrators, clinical-informaticians, IT governance structures, and national professional organizations. Successful implementation of these guidelines would ultimately improve patient care and keep their data safe.

## NOTES

### Conflict of interest

Rajiv Chandawarkar is an editorial board member of the journal but was not involved in the peer reviewer selection, evaluation, or decision process of this article. No other potential conflicts of interest relevant to this article were reported.

### Author contribution

Conceptualization: R Chandawarkar. Methodology: R Chandawarkar, P Nadkarni. Project administration: R Chandawarkar, P Nadkarni. Writing - original draft: R Chandawarkar, P Nadkarni. Writing - review & editing: R Chandawarkar, P Nadkarni.

### ORCID

Rajiv Chandawarkar https://orcid.org/0000-0002-7300-1640

## REFERENCES

1. Davis J. Update: the 10 biggest healthcare data breaches of 2020, so far [Internet]. Danvers, MA: Healthcare IT Securi-

ty; c2020 [cited 2020 Dec 25]. Available from: https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far.
2. Spin Inc. What is ransomware? The major cybersecurity threat explained [Internet]. Palo Alto, CA: Spin Inc.; c2019 [cited 2020 Dec 5]. Available from: https://spinbackup.com/blog/what-is-ransomware-the-major-cybersecurity-threat-explained/.
3. Tidy J. Hackers threaten to leak plastic surgery pictures [Internet]. London: BBC News; c2020 [cited 2020 Dec 26]. Available from: https://www.bbc.com/news/technology-55439190.
4. Chan N, Charette J, Dumestre DO, et al. Should 'smart phones' be used for patient photography? Plast Surg (Oakv) 2016;24:32-4.
5. Abbott LM, Magnusson RS, Gibbs E, et al. Smartphone use in dermatology for clinical photography and consultation: current practice and the law. Australas J Dermatol 2018;59:101-7.
6. Rimmer A. Doctors' use of Facebook, Twitter, and WhatsApp is the focus of 28 GMC investigations. BMJ 2017;358:j4099.
7. Houston J, Ashby L, Ogidi J, et al. A novel Caldicott-compliant hospital imaging protocol for open fracture photography. Br J Hosp Med (Lond) 2020;81:1-8.
8. Mobasheri MH, King D, Johnston M, et al. The ownership and clinical use of smartphones by doctors and nurses in the UK: a multicentre survey study. BMJ Innov 2015;1:174–81.
9. Ricoh Corporation. Ricoh G800 features: security [Internet]. Tokyo: Ricoh Corporation; c2020 [cited 2020 Dec 26]. Available from: https://industry.ricoh.com/en/dc/g/g800/features6.html.
10. Rimmer A. Hidden risks your smartphone poses to your career. BMJ 2017;359:j4896.
11. Morris C, Scott RE, Mars M. Security and other ethical concerns of instant messaging in healthcare. Stud Health Technol Inform 2018;254:77-85.
12. Osborne C. LokiBot malware now hides its source code in image files [Internet]. ZDNet; c2020 [cited 2020 Dec 25]. Available from: https://www.zdnet.com/article/lokibot-information-stealer-now-hides-malware-in-image-files/.
13. Ramaswami SS. Picture perfect: how JPG EXIF data hides malware [Internet]. San Francisco, CA: Cisco Umbrella; c2020 [cited 2020 Dec 25]. Available from: https://umbrella.cisco.com/blog/picture-perfect-how-jpg-exif-data-hides-malware.
14. Shah S. Exploit delivery via steganography and polyglots [Internet]. Stegosploit; c2015 [cited 2020 Dec 25]. Available from: https://stegosploit.info/.
15. Djian J, Lellouch AG, Botter C, et al. Clinical photography by smartphone in plastic surgery and protection of personal data: development of a secured platform and application on 979 patients. Ann Chir Plast Esthet 2019;64:33-43.
16. Lam JS, Simpson BK, Lau FH. Health insurance portability and accountability act noncompliance in patient photograph management in plastic surgery. Ann Plast Surg 2019;82:486-92.
17. US Department of Health and Human Services. Health information of deceased individuals [Internet]. Washington, D.C.: US Department of Health and Human Services; c2020 [cited 2020 Dec 9]. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/health-information-of-deceased-individuals/index.html.
18. US Department of Health and Human Services. HIPAA for professionals [Internet]. Washington, D.C.: US Department of Health and Human Services; c2020 [cited 2020 Dec 9]. Available from: https://www.hhs.gov/hipaa/for-professionals/.
19. US Department of Health and Human Services. HIPAA: guidance material for consumers [Internet]. Washington, D.C.: US Department of Health and Human Services; c2020 [cited 2020 Dec 9]. Available from: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/.
20. Badger B, Grance T, Patt-Corner R, et al. NIST SP 800-146, Cloud Computing Synopsis and Recommendations. Gaithersburg: US National Institute for Standards in Technology; 2012.
21. Spirion Corporation. New U.S. State Data Protection Laws Enforceable in 2020 [Internet]. St. Petersburg, FL: Spirion Corporation; c2020 [cited 2020 Dec 10]. Available from: https://info.spirion.com/DS2020-Q2-2020EnforcedStateLaws_LPRegistration.html.
22. Crook MA. The Caldicott report and patient confidentiality. J Clin Pathol 2003;56:426-8.
23. Caldicott DF. Information: to share or not to share. The Information Governance Review [Internet]. London: Department of Health; c2013 [cited 2020 Nov 21]. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251750/9731-2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF.
24. UK National Health Service (NHS). Information governance considerations for staff on the use of instant messaging software in acute clinical settings [Internet]. London: NHS; c2018 [cited 2020 Nov 21]. Available from: https://

digital.nhs.uk/binaries/content/assets/website-assets/data-and-information/ig-resources/information-governance-considerations-for-individuals-on-the-use-of-instant-messaging-software-in-acute-clinical-settings.pdf.
25. John B. Are you ready for general data protection regulation? BMJ 2018;360:k941.
26. British Orthopaedic Association. Open fractures [Internet]. London: British Orthopaedic Association; c2017 [cited 2020 Nov 21]. Available from: https://www.boa.ac.uk/uploads/assets/3b91ad0a-9081-4253-92f7d90e8df0fb2c/29bf80f1-1cb6-46b7-afc761119341447f/open%20fractures.pdf.
27. National Institute for Health and Care Excellence (NICE). Fractures (complex): assessment and management. NICE guideline NG 37 [Internet]. London: NICE; c2017 [cited 2020 Nov 21]. Available from: https://www.nice.org.uk/guidance/ng37.
28. Heyns M, Steve A, Dumestre DO, et al. Canadian guidelines on smartphone clinical photography. Can J Physician Leadership 2018;4:58-163.
29. Canadian Medical Association. Best practices for smartphone and smart-device clinical photo taking and sharing (CMA policy summary) [Internet]. Ottawa, ON: Canadian Medical Association; c2018 [cited 2020 Nov 21]. Available from: https://policybase.cma.ca/documents/policypdf/PD18-04.pdf.
30. Commonwealth of Australia. Federal Register of Legislation: Privacy Act 1988, Schedule 1, Part 4, Principle 11 [Internet]. Canberra: Australian Government; c1988 [cited 2020 Nov 22]. Available from: https://www.legislation.gov.au/Details/C2017C00283.
31. Commonwealth of Australia. Privacy impact assessment register [Internet]. Canberra: Australian Government; c2020 [cited 2020 Nov 22]. Available from: https://www.health.gov.au/using-our-websites/privacy/privacy-impact-assessment-register#why-we-have-the-register.
32. Commonwealth of Australia. Privacy (Australian Government Agencies – Governance) APP Code 2017 [Internet]. Canberra: Australian Government; c2020 [cited 2020 Nov 22]. Available from: https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/australian-government-agencies-privacy-code/.
33. GDPR.eu. Recital 53: Processing of sensitive data in health and social sector [Internet]. GDPR.eu; c2020 [cited 2020 Nov 21]. Available from: https://gdpr.eu/recital-53-processing-of-sensitive-data-in-health-and-social-sector/.
34. GDPR.eu. The UK Information Commissioner's Office issued a massive judgment against a company for illegal data sharing. Here's how to avoid the same fate [Internet]. GDPR.eu; c2020 [cited 2020 Nov 21]. Available from: https://gdpr.eu/data-sharing-bounty-fine/.
35. CoreView Inc. Major GDPR Fine Tracker: an ongoing, always-up-to-date list of enforcement actions [Internet]. Alpharetta, GA: CoreView Inc; c2020 [cited 2020 Nov 21]. Available from: https://www.coreview.com/blog/alpin-gdpr-fines-list/.
36. Du W. Computer & internet security: a hands-on approach. 2nd ed. Wenliang Du; 2019.
37. Scarfone K, Benigni D, Grance T. Cyber security standards [Internet]. Gaithersburg, MD: US National Institute for Standards in Technology; c2012 [cited 2020 Nov 21]. Available from: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152153.
38. European Network and Information Security Agency (ENISA). ICT Security Standards Roadmap [Internet]. Geneva: International Telecommunication Union; c2020 [cited 2020 Nov 22]. Available from: https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/default.aspx.
39. International Standards Organization. ISO/IEC JTC1/SC 27 (2008). Standing Document 6 (SD6): Glossary of IT Security Terminology, 2008-03-19 [Internet]. c2008 [cited 2020 Nov 22]. Available from: http://www.jtc1sc27.din.de/sce/SD6.
40. Allen KG, Eleftheriou P, Ferguson J. A thousand words in the palm of your hand: management of clinical photography on personal mobile devices. Med J Aust 2016;205:499-500.
41. Patel NG, Rozen WM, Marsh D, et al. Modern use of smartphone applications in the perioperative management in microsurgical breast reconstruction. Gland Surg 2016;5:150-7.
42. Gardiner S, Hartzell TL. Telemedicine and plastic surgery: a review of its applications, limitations and legal pitfalls. J Plast Reconstr Aesthet Surg 2012;65:e47-53.
43. Hunter T, Hardwicke J, Rayatt S. The smart phone: an indispensable tool for the plastic surgeon? J Plast Reconstr Aesthet Surg 2010;63:e426-7.
44. Knight J. The 4 best phones for privacy & security in 2020 [Internet]. Gadget Hacks; c2020 [cited 2020 Dec 15]. Available from: https://smartphones.gadgethacks.com/how-to/4-best-phones-for-privacy-security-2020-0176106/.
45. Lee WJ, Hwang K, Lee SI, et al. Proposal of photographic standards in plastic surgery. J Korean Soc Plast Reconstr Surg 2002;29:45-54.
46. Committee to Protect Journalists (CJP). What we do [Internet]. New York, NY: CJP; c2020 [cited 2020 Nov 21]. Available from: https://cpj.org/about.