BEST PRACTICES FOR SMARTPHONE AND SMART-DEVICE CLINICAL PHOTO TAKING AND SHARING

BACKGROUND

Clinical photography is a valuable tool for physicians. Smartphones, as well as other devices supporting network connectivity, offer a convenient, efficient method to take and share images. However, due to the private nature of the information contained in clinical photographs there are concerns as to the appropriate storage, dissemination, and documentation of clinical images. Confidentiality of image data must be considered and the dissemination of these images onto servers must respect the privacy and rights of the patient. Importantly, patient information should be considered as any information deriving from a patient, and the concepts outlined therefore apply to any media that can be collected on, or transmitted with, a smart-device.

Clinical photography can aid in documenting form and function, in tracking conditions and wound healing, in planning surgical operations, and in clinical decision-making. Additionally, clinical photographs can provide physicians with a valuable tool for patient communication and education. Due to the convenience of this type of technology it is not appropriate to expect physicians to forego their use in providing their patients with the best care available.

The technology and software required for secure transfer, communication, and storage of clinical media is presently available, but many devices have non-secure storage/dissemination options enabled and lack user-control for permanently deleting digital files. In addition, data uploaded onto server systems commonly cross legal jurisdictions. Many physicians are not comfortable with the practice, citing security, privacy, and confidentiality concerns as well as uncertainty in regards to regional regulations governing this practice.[1] Due to concern for patient privacy and confidentiality it is therefore incredibly important to limit the unsecure or undocumented acquisition or dissemination of clinical photographs.

i Heyns M†, Steve A‡, Dumestre DO‡, Fraulin FO‡, Yeung JK‡
† University of Calgary, Canada
‡ Section of Plastic Surgery, Department of Surgery, University of Calgary, Canada

To assess the current state of this topic, Heyns *et al.* have reviewed the accessibility and completeness of provincial and territorial medical regulatory college guidelines.[2] Categories identified as vital and explored in this review included: Consent; Storage; Retention; Audit; Transmission; and Breach. While each regulatory body has addressed limited aspects of the overall issue, the authors found a general lack of available information and call for a unified document outlining pertinent instructions for conducting clinical photography using a smartphone and the electronic transmission of patient information.[2]

The discussion of this topic will need to be ongoing and it is important that physicians are aware of applicable regulations, both at the federal and provincial levels, and how these regulations may impact the use of personal devices. The best practices supported here aim to provide physicians and healthcare providers with an understanding of the scope and gravity of the current environment, as well as the information needed to ensure patient privacy and confidentiality is assessed and protected while physicians utilize accessible clinical photography to advance patient care. Importantly, this document only focusses on medical use (clinical, academic, and educational) of clinical photography and, while discussing many core concepts of patient privacy and confidentiality of information, should not be perceived as a complete or binding framework. Additionally, it is recommended that physicians understand the core competencies of clinical photography, which are not described here.

The Canadian Medical Association (CMA) suggests that the following recommendations be implemented, as thoroughly as possible, to best align with the CMA policy on the Principles for the Protection of Patient Privacy (CMA Policy PD2018-02). These key recommendations represent a non-exhaustive set of best practices – physicians should seek additional information as needed to gain a thorough understanding and to stay current in this rapidly changing field.

KEY RECOMMENDATIONS

1. CONSENT

- Informed consent must be obtained, preferably prior, to photography with a mobile device. This applies for each and any such encounter and the purpose made clear (i.e. clinical, research, education, publication, etc.). Patients should also be made aware that they may request a copy of a picture or for a picture to be deleted.
- A patient's consent to use electronic transmission does not relieve a physician of their duty to protect the confidentiality of patient information. Also, a patient's consent cannot override other jurisdictionally mandated security requirements.
- All patient consents (including verbal) should be documented. The acquisition and recording of patient consent for medical photography/dissemination may be held to a high standard of accountability due to the patient privacy and confidentiality issues inherent in the use of this technology. Written and signed consent is encouraged.

- Consent should be considered as necessary for any and all photography involving a patient, whether or not that patient can be directly recognized, due to the possibility of linked information and the potential for breach of privacy. The definition of non-identifiable photos must be carefully considered. Current technologies such as face recognition and pattern matching (e.g. skin markers, physical structure, etc.), especially in combination with identifying information, have the potential to create a privacy breach.
- Unsecure text and email messaging requires explicit patient consent and should not be used unless the current gold standards of security are not accessible. For a patient-initiated unsecure transmission, consent should be clarified and not assumed.

2. TRANSMISSION

- Transmission of photos and patient information should be encrypted as per current-day gold standards (presently, end-to-end encryption (E2EE)) and use only secure servers that are subject to Canadian laws. Explicit, informed consent is required otherwise due to privacy concerns or standards for servers in other jurisdictions. Generally, free internet-based communication services and public internet access are unsecure technologies and often operate on servers outside of Canadian jurisdiction.
- Efforts should be made to use the most secure transmission method possible. For data security purposes, identifying information should never be included in the image, any frame of a video, the file name, or linked messages.
- The sender should always ensure that each recipient is intended and appropriate and, if possible, receipt of transmission should be confirmed by the recipient.

3. STORAGE

- Storing images and data on a smart-device should be limited as much as possible for data protection purposes.
- Clinical photos, as well as messages or other patient-related information, should be completely segregated from the device's personal storage. This can be accomplished by using an app that creates a secure, password-protected folder on the device.
- All information stored (on internal memory or cloud) must be strongly encrypted and password protected. The security measures must be more substantial than the general password unlock feature on mobile devices.
- Efforts should be made to dissociate identifying information from images when images are exported from a secure server. Media should not be uploaded to platforms without an option for securely deleting information without consent from the patient, and only if there are no better options. Automatic back-up of photos to unsecure cloud servers should be deactivated. Further, other back-up or syncing options that could lead to unsecure server involvement should be ascertained and the risks mitigated.

4. Cloud storage should be on a Canadian and SOCII certified server. Explicit, informed consent is required otherwise due to privacy concerns for servers in other jurisdictions.

5. AUDIT & RETENTION

- It is important to create an audit trail for the purposes of transparency and medical best practice. Key information includes patient and health information, consent type and details, pertinent information regarding the photography (date, circumstance, photographer), and any other important facts such as access granted/deletion requests.
- Access to the stored information must be by the authorized physician or health care provider and for the intended purpose, as per the consent given. Records should be stored such that it is possible to print/transfer as necessary.
- Original photos should be retained and not overwritten.
- All photos and associated messages may be considered part of the patient's clinical records and should be maintained for at least 10 years or 10 years after the age of majority, whichever is longer. When possible, patient information (including photos and message histories between health professionals) should be retained and amalgamated with a patient's medical record. Provincial regulations regarding retention of clinical records may vary and other regulations may apply to other entities – e.g. 90 years from date of birth applies to records at the federal level.
- It may not be allowable to erase a picture if it is integral to a clinical decision or provincial, federal, or other applicable regulations require their retention.

6. BREACH

- Any breach should be taken seriously and should be reviewed. All reasonable efforts must be made to prevent a breach before one occurs. A breach occurs when personal information, communication, or photos of patients are stolen, lost, or mistakenly disclosed. This includes loss or theft of one's mobile device, texting to the wrong number or emailing/messaging to the wrong person(s), or accidentally showing a clinical photo that exists in the phone's personal photo album.
- It should be noted that non-identifying information, when combined with other available information (e.g. a text message with identifiers or another image with identifiers), can lead to highly accurate re-identification.
- At present, apps downloaded to a smart-device for personal use may be capable of collecting and sharing information – the rapidly changing nature of this technology and the inherent privacy concerns requires regular attention. Use of specialized apps designed for health-information sharing that help safeguard patient information in this context is worth careful consideration.

- Having remote wipe (i.e. device reformatting) capabilities is an asset and can help contain a breach. However, inappropriate access may take place before reformatting occurs.
- If a smartphone is strongly encrypted and has no clinical photos stored locally then its loss may not be considered a breach.
- In the event of a breach any patient potentially involved must be notified as soon as possible. The CMPA, the organization/hospital, and the Provincial licensing College should also be contacted immediately. Provincial regulations regarding notification of breach may vary.

Approved by the CMA Board of Directors March 2018

References

[1] Chan N, Charette J, Dumestre DO, Fraulin FO. Should 'smart phones' be used for patient photography? *Plast Surg* (Oakv). 2016;24(1):32-4.
[2] Unpublished - Heyns M, Steve A, Dumestre DO, Fraulin FO, Yeung J. Canadian Guidelines on Smartphone Clinical Photography.