

A thousand words in the palm of your hand: management of clinical photography on personal mobile devices

Automated solutions to curb privacy risks

Ubiquitous access to high resolution photography through personal mobile devices (PMDs), such as smartphones and tablets, has forever changed how we communicate. In the clinical environment, photography has extended beyond professional photography units and into the hands of clinicians through PMDs. Opportunities to optimise patient care have been enhanced by this immediate transfer of accurate and relevant clinical images. Despite these benefits, photographic documentation of the patient's condition on PMDs creates a sensitive personal record on inherently insecure devices¹ when the patient is vulnerable.² This exposes patients to an ongoing risk of potentially serious consequences and psychological harm in the event of illicit publication.³ Health care organisations must ensure that security is a paramount concern and that their clinicians obtain consent appropriately to minimise the risk of a breach of patient confidentiality.

Clinical photography is a rapidly expanding modality for documenting illness and recording signs of disease,^{1,4} overcoming access and turnaround delays that may impede the professional photography units' effectiveness.² PMD use in the clinical environment allows rapid photographic documentation at the point of care.⁵ Immediate distribution of clinical images through multimedia messaging or email may streamline clinical consultation at the patient's bedside, expedite decision making and minimise unnecessary on-call attendances. This same immediacy, and the fact that PMDs may be easily stolen, lost or left unlocked, significantly magnifies the risks of unauthorised publication and patient harm.^{1,6} Harms may include unconsented secondary uses, identification, publication, psychological trauma and financial, occupational and reputational damage. Patient acceptability of the use of PMDs as a tool in clinical photography is thus understandably low.^{7,8} These reservations will likely remain until proper regulation is enacted; a change that health care organisations have found difficult to accomplish.²

While individual recommendations to clinicians to improve their PMD security¹ are beneficial, poor compliance with organisational policies remain.² Manually uploading and removing photos from PMDs is onerous, with doctors often retaining large databases of images on these devices,⁵ creating an unacceptable risk to patients. The capture of potentially identifiable physical features and metadata, and the unknown factor of how software developments may enable the identification of image subjects, dictate that health care organisations treat every patient image as potentially identifiable and implement automated systems that regulate the use of PMDs for clinical photography to protect patients from harm.⁹

The National Safety and Quality Health Service Standards in Australia require health care organisations

to implement mechanisms protecting the confidentiality of patients' clinical records.¹⁰ Poor compliance² is evidence of a failing system of PMD regulation. Health care organisations must scope and develop automated information management solutions that minimise arduous manual tasks and consider the role that an application (app) installed on clinicians' PMDs may play in facilitating this.

Consent procedures

Validly obtained consent must be fully informed and be given voluntarily, before the fact and with capacity.¹¹ Patients must be informed of how an image is to be used, transmitted, stored and disposed of,¹² as well as the fallibility of security mechanisms before acquiring the photograph to meet this standard. Positioning oneself in front of a clinician's PMD is commonly — and unacceptably — considered to be an appropriate consent procedure,¹³ a practice which requires censure. The sensitive nature of the image and the magnitude of the risks patients face mandate that clearly documented, explicit consent is warranted. In the absence of this, the potential for indirect coercion exists, pressuring patients to allow an image to be acquired in order for their care to continue.^{3,7}

While patients may gain some utility in diagnosis and management that is potentially more timely and accurate through the use of PMDs for photography, the benefits heavily favour time scarce clinicians, who ultimately accept little of the risk. The power imbalance in the therapeutic relationship¹⁴ renders many patients unable to express objections to clinicians who fail to adhere to appropriate consent procedures, or who focus on their own benefits without clear exploration of the patient's risk of harm.

Cultural change is required to combat poor adherence² to organisations' procedures for consenting patients when PMD photography is used.³ With this in mind, an automated app-based system allows for standardisation and automated documentation of the consent process before acquisition. This creates a stopgap that ensures components are not omitted and requires the clinician to input confirmation of specific aspects of consent to which patients have agreed. Consultation with consumer representatives and trialling of the standardised consent procedure must occur to facilitate patient understanding.

Legislative requirements

The rapid uptake of PMD photography requires health care organisations to carefully consider how to best minimise the significant risks patients face through permanent global publication.⁹ Privacy, record keeping and freedom of information legislation in all likelihood

Kieran G Allen^{1,2}

Paul Eleftheriou³

John Ferguson⁴

¹ Monash University, Melbourne, VIC.

² Queensland University of Technology, Brisbane, QLD.

³ Austin Health, Melbourne, VIC.

⁴ Sidra Medical and Research Center, Doha, Qatar.

email@kieranallen.net.au

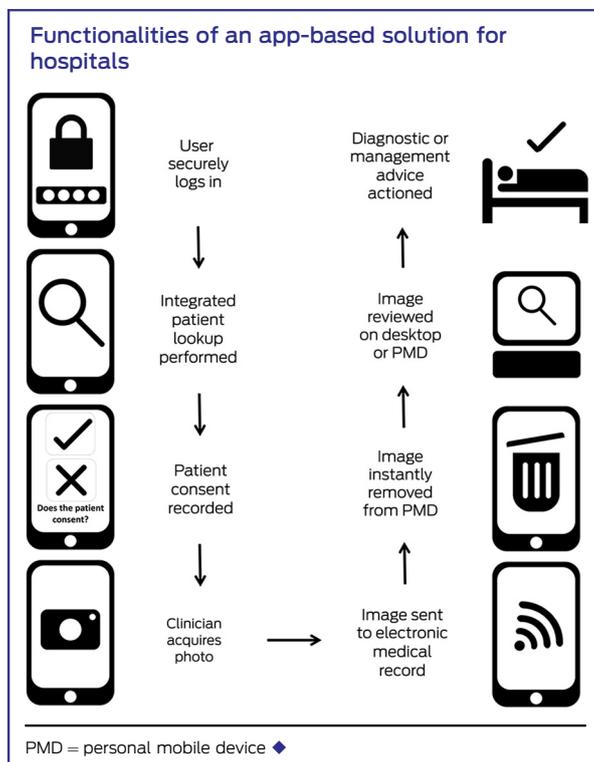
doi: 10.5694/mja16.00520

applies, despite remaining untested at law.^{6,15} Health care organisations should not underestimate the penalties that may apply under privacy legislation to protect patients from the potential risks of unauthorised publication.¹ Automated deletion of PMD records and prevention of automated upload to cloud servers¹ in unknown locations, where Australian law may not apply, is an effective mechanism to reduce this risk.

Automated solutions may also facilitate record keeping requirements for images with a clinical use (as opposed to research or educational use), which varies across jurisdictions, typically for a period of 7 years after the cessation of patient contact for adults.¹⁵ The broad definition of “health information”, as stated in the Australian *Privacy Act 1988* (Cwlth), is any information about a person’s health or disability. Given that clinical images collected on a clinician’s PMD convey information about the presence (or stage) of disease, a conservative definition is prudent, as it is likely that images are indeed a component of a patient’s medical record, irrespective of the mode of acquisition.^{6,15}

Whether legislation applies to images on a PMD itself remains unknown.¹⁵ Ideally, health care organisations would automatically transfer clinicians’ PMD images to the electronic medical record and immediately remove the PMD copy, which negates this ambiguity. Health information or freedom of information requirements, which convey a right of access to one’s medical record, necessitates such a system.

We propose to implement and evaluate an app-based solution at an Australian metropolitan tertiary hospital in the near future (Box), which has the following key functionalities:



- requires secure credentials to be entered;
- allocates a unique patient identifier — the hospital unit record;
- captures patient consent, as previously described;
- removes unnecessary metadata;
- transmits securely the uniquely identified image and consent to a data repository within or linked to the organisation’s medical record;
- deletes immediately the PMD copy once transmitted;
- enables colleagues to access the image on their PMD or computer to provide advice regarding diagnosis and management;
- records individual image access; and
- requires re-entry of credentials after a set time.

Any such system must seamlessly integrate with health information systems and PMDs to ensure immediate transmission of photographs to patient records. To prevent patient identification, photos must never use specific patient details as the filename, or embedded within the file. In the event of unauthorised access, these details permit images which may otherwise be anonymous to become identifiable. Little justification or capability exists for clinicians to retain photos on the PMD itself in this system.

Conclusion

Clinical photography plays a key role in the delivery of efficient, high quality health care. The rapid technological advances that have taken place over the past decade have seen the PMD rise to prominence as an essential clinical “tool of the trade”, bringing with it the capability and immediate availability of high resolution digital imaging and transmissibility. This has allowed for rapid access to second opinions and advice, but has inadvertently increased the risks surrounding confidentiality, security and informed consent.

Health organisations’ ability to ensure adequate development of and adherence to policies and procedures surrounding PMD use has been lacking.² The importance of implementing secure mechanisms of photographic capture, transmission and disposal from PMDs should not be underestimated as an element of quality care. Strong leadership from hospital networks, private health care organisations and professional associations will ultimately enable PMD photography to improve patient care and health outcomes. Widespread implementation of the software described and the promotion of its use will help improve the patients’ valid apprehensions⁵ toward PMD camera technology in the clinical setting, while allowing realisation of its benefits and, most importantly, improvements in the delivery of health care.

Acknowledgements: We thank Fiona McDonald for providing editorial opinion on this manuscript.

Competing interests: For the purpose of implementing the software solution described, the authors have engaged a commercial software developer, AGFA, but receive no financial or other benefits from this association.

Provenance: Not commissioned; externally peer reviewed. ■

© 2016 AMPCo Pty Ltd. Produced with Elsevier B.V. All rights reserved.

References are available online at www.mja.com.au.

- 1 Stevenson P, Finnane AR, Soyer HP. Teledermatology and clinical photography: safeguarding patient privacy and mitigating medico-legal risk. *Med J Aust* 2016; 204: 198-200. <https://www.mja.com.au/journal/2016/204/5/teledermatology-and-clinical-photography-safeguarding-patient-privacy-and>
- 2 Burns K, Belton S. Clinicians and their cameras: policy, ethics and practice in an Australian tertiary hospital. *Aust Health Rev* 2013; 37: 437-441.
- 3 Berle I. Clinical photography and patient rights: the need for orthopraxy. *J Med Ethics* 2008; 34: 89-92.
- 4 Scheinfeld N, Rothstein B. HIPAA, dermatology images, and the law. *Semin Cutan Med Surg* 2013; 32: 199-204.
- 5 Koehler N, Vujovic O, McMenamin C. Healthcare professionals' use of mobile phones and the internet in clinical practice. *J Mob Technol Med* 2013; 2: 3-13.
- 6 Kirk M, Hunter-Smith SR, Smith K, et al. The role of smartphones in the recording and dissemination of medical images. *J Mob Technol Med* 2014; 3: 40-45.
- 7 Burns K, Belton S. "Click first, care second" photography. *Med J Aust* 2012; 197: 265. <https://www.mja.com.au/journal/2012/197/5/click-first-care-second-photography>
- 8 Lau CK, Schumacher HH, Irwin MS. Patients' perception of medical photography. *J Plast Reconstr Aesthet Surg* 2010; 63: e507-511.
- 9 Jones B. "Drop 'em blossom" — Clinical photography and patient dignity. *J Audiov Media Med* 1996; 19: 85-86.
- 10 Australian Commission on Safety and Quality in Health Care. National Safety and Quality Health Service Standards, September 2011. Sydney: ACSQHC; 2011. <https://www.safetyandquality.gov.au/wp-content/uploads/2011/01/NSQHS-Standards-Sept2011.pdf> (accessed Oct 2016).
- 11 del Carmen MG, Joffe S. Informed consent for medical treatment and research: a review. *Oncologist* 2005; 10: 636-641.
- 12 Hill K. Consent, confidentiality and record keeping for the recording and usage of medical images. *J Vis Commun Med* 2006; 29: 76-79.
- 13 Scheinfeld N. Photographic images, digital imaging, and the law. *Arch Dermatol* 2004; 140: 473-476.
- 14 Goodyear-Smith F, Buetow S. Power issues in the doctor-patient relationship. *Health Care Anal* 2001; 9: 449-462.
- 15 Mahar PD, Foley PA, Sheed-Finck A, Baker CS. Legal considerations of consent and privacy in the context of clinical photography in Australian medical practice. *Med J Aust* 2013; 198: 48-49. <https://www.mja.com.au/journal/2013/198/1/legal-considerations-consent-and-privacy-context-clinical-photography-australian> ■