Clinical images and the use of personal mobile devices. Guide for medical students and doctors

Fact sheet

- Clinical images are routinely captured and used by doctors working in the Australian healthcare system.
- Clinical images are often used beneficially in the provision of patient care, particularly for capturing clinical signs, injuries and lesions, and monitoring of these over time.
- Appropriate transmission of clinical images aids professional referrals for improved diagnosis, treatment and management, particularly in regional, rural and remote settings where specialist services may be limited or not available.
- Clinical images may also be used for non-clinical purposes such as teaching, training and research.
- Research suggests that patients are supportive of clinical images being taken and shared with other specialists to improve clinical care and inter-clinician communication.¹
- While clinical imaging departments exist in many hospitals, many doctors use personal mobile devices to capture such images.
- Many doctors do not realise that an image, even if captured on a personal mobile device, forms part of a patient's medical record and is subject to the same privacy and confidentiality principles as any other element of the record.
- Significant legal and financial penalties apply for breaches in confidentiality of medical records, in addition to consideration of professional and ethical obligations.
- For example, a clinician who has a patient’s photo saved on their phone could face significant fines of up to $340,000, regardless of whether damages have been proven. This means that organisations must take such steps as are reasonable in the circumstances to protect personal information.
- The Australian Medical Association (AMA) is committed to upholding the principles of medical professionalism and has partnered with the Medical Indemnity Industry Association of Australia (MIIAA) to produce guidelines for the use of personal mobile devices when taking clinical images.
- This is the first relevant national professional guide for doctors and medical students working in the Australian healthcare system.
- The guide will help medical student and doctors to be aware of the legal, professional and ethical obligations associated with the capture and use of clinical images, particularly when captured on a personal mobile device.
- The guide outlines professionally appropriate processes of informed consent, documentation, capture, secure storage, disclosure, transmission and deletion of clinical images, including considerations of quality, de-identification and privacy legislation.
- Case reports and discussion of complex situations are included, as is a checklist for doctors.

Clinical images and the use of personal mobile devices. Guide for medical students and doctors

- The guide does not specifically cover other purposes such as teaching, training or research.
- While the guide may be useful for doctors working in other clinical settings, they are primarily intended for use by Medical Students and Doctors in an Australian Public Hospital environment.
- The guide can be found at https://ama.com.au/guidelines-clinical-images-and-use-personal-mobile-devices and should always be read subject to any relevant privacy legislation, and any requirements in employment contracts and/or hospital policies related to clinical images and the use of personal mobile devices.
- The AMA and MIIAA encourage jurisdictions to develop and promote sensible policy and procedure in this area and to provide a secure platform within health services to enable doctors and facilities to use this technology safely, efficiently and effectively.

Key messages

- **CONSENT TO COLLECTION, USE, AND DISCLOSURE OF CLINICAL IMAGES TAKEN WITH A PERSONAL MOBILE DEVICE**
  - Before taking a clinical image, consider the purpose for which you require the image and obtain appropriate consent.
  - Make sure the patient understands the reasons for taking the image, how it will be used and to whom it will be shown.
  - Document the consent process in the health record. Check what your health service/hospital requirements are for written consent.
  - Never send a clinical image to anyone else unless you have the patient’s consent to do so, or the patient would reasonably expect you to send the image for the purpose of their clinical management or you are otherwise permitted by law to do so.
  - If the clinical image is sent to the wrong person, patient privacy has been breached. In these circumstances you should seek advice from hospital management or your medical defence organisation.

- **STORAGE AND SECURITY OF CLINICAL IMAGES**
  - Find out what your health service/hospital policy is for storing clinical images, and what systems your hospital has in place to facilitate the storage of digital images.
  - Make sure clinical images do not auto upload to any social media networks or back up sites.
  - Delete any clinical image after saving it onto the health record.
  - Have controls on your mobile device to prevent unauthorised access.
Clinical images and the use of personal mobile devices. Guide for medical students and doctors

Background

• A survey of doctors and nurses in August 2010, from 17 wards in an Australian tertiary hospital, explored the prevalence of medical photography, image use, quality of consent, cameras and technology, confidentiality, and data storage and security. Of the 170 staff surveyed, 48% had taken medical photos in the past year. Most used hospital-owned cameras, but one-fifth used a personal mobile phone. Junior surgical staff noted the efficacy of taking mobile phone images to show consultants later, yet they retained the images after the cases had concluded.2

• Consent practices were more alarming, with non-compliance with hospital consent policy widespread. Of clinicians taking photos for patient files, 65% used verbal rather than written consent, and of clinicians taking them for educational purposes, 59% used only verbal consent.

• Copyright issues were generally misunderstood; only 33 out of 71 health professionals understood that clinician-taken medical photos were owned by the health department. Many believed that taking an image meant owning an image. Labelling, storage and disposal practices were irregular, with 10% of clinicians compromising the security of patient information by storing images on personal devices.

• A survey3 on the use of cameras on smartphones by doctors in the clinical setting and their understanding of published policies pertaining to clinical photography in 2013 revealed that of the doctors surveyed:
  • all had a phone, most with in-built cameras, and almost all were connected to the Internet; only 43 per cent had a lock on their phone;
  • 65 per cent of our doctors were taking clinical images but only a quarter had obtained appropriate patient consent; of those, only seven per cent had obtained written consent.
  • 23 per cent documented in the medical record that an image has been taken of their patient and many kept those clinical images for later use, with 91 per cent sharing images in insecure ways such as email and IM.
  • 40 per cent of respondents knew that there was a prevailing policy regarding clinical photography and of those who do know there was a policy, only five per cent had read it.
  • Sixty per cent incorrectly believe that they, rather than the hospital, owned the image.

2 Burns KR. Examining issues and compliance with hospital policy when clinicians take medical photographs [honours thesis]. Melbourne: RMIT University, 2011.