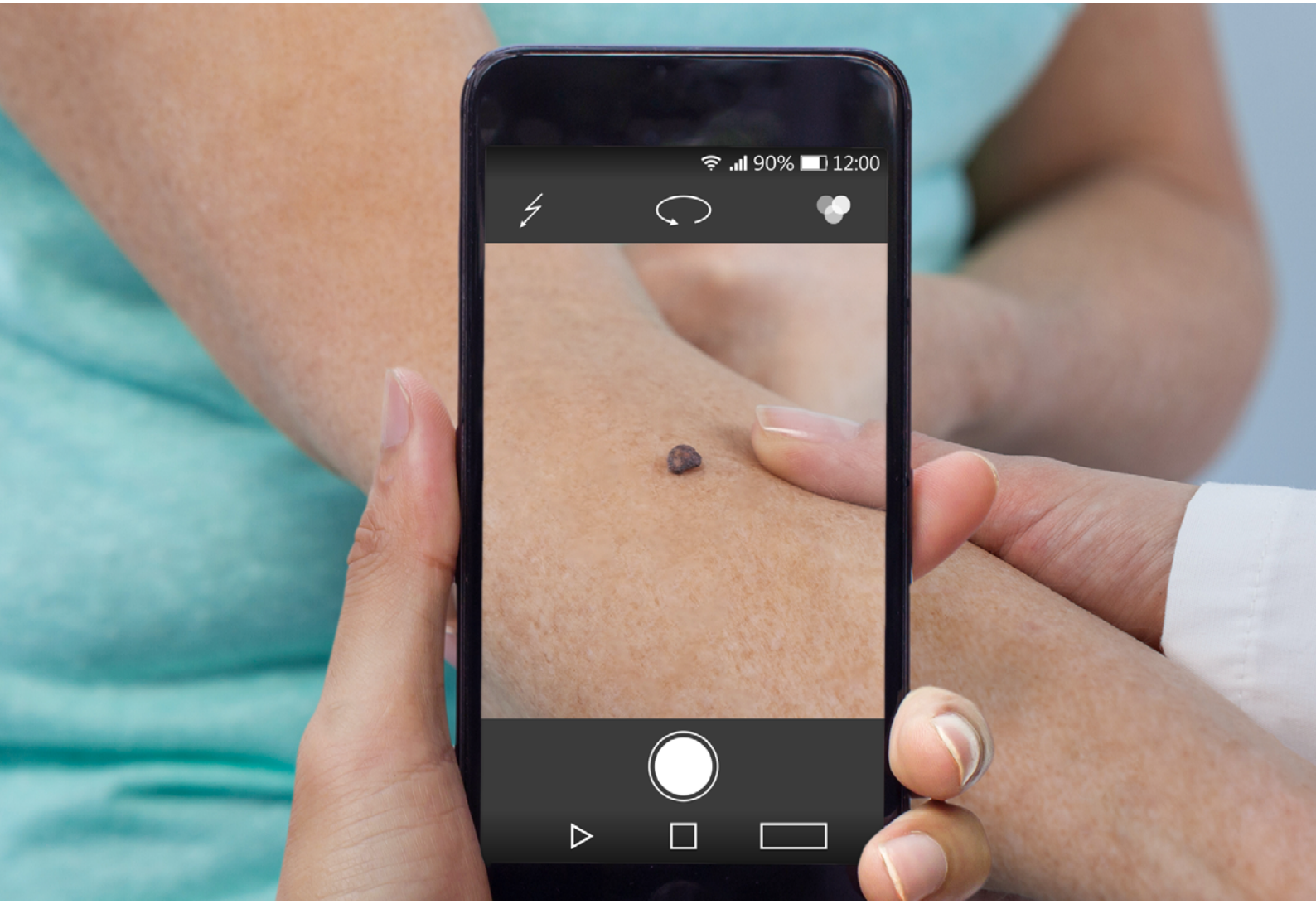
RACGP

Royal Australian College *of* General Practitioners

Using personal mobile devices for clinical photos in general practice



Medical photography has long had an important role in the assessment and management of patients in general practice. With most mobile phones and tablets equipped with high-quality cameras, significant memory capacity, and wireless technology, it is easier than ever to capture and distribute clinical photos of patients.

While clinical photos are a useful tool, care needs to be taken to ensure patient privacy, particularly when they are taken on a personal mobile device that belongs to the clinician and is used outside of the workplace.

6759

Potential hazards

A clinical photo is likely to capture details of a sensitive nature. In the digital age, a photo can be a permanent record and if it ends up in the public domain, it has the potential to cause embarrassment or psychological harm.

Photos can be sent to the wrong person by accident and there is a risk that they may be intercepted during transmission to other devices. When clinical photos are sent to another clinician for consultation or second opinion, there is no guarantee they will be stored securely on that person's device.

Clinical photos taken on a personal mobile device should be treated with particular care. A clinician's own phone or tablet might not be as secure as other devices used in the practice for storing sensitive medical information. A personal device is perhaps more likely to be lost, stolen or accessed by other people. Another hazard is that a clinician might simply forget to transfer the photos from the personal mobile device to the patient's medical record or to delete the photo from the device after the photo has been transferred.

Key points

General considerations

- Know your obligations under the law with regard to the collection, disclosure and storage of clinical photos in the jurisdiction of your practice (refer to Section 1)
- Check your practice's policy with regard to the use of personal mobile devices for clinical photos (refer to Section 2)
- Obtain informed consent from the patient prior to collecting photos (refer to Section 3)
- Report data breaches if they occur (refer to Section 4)

Collecting photos (refer to Section 5)

- Take care when using clinical photography apps
- Ensure the device has a high-resolution camera
- Capture only what is required
- Remove metadata when de-identifying photos, where applicable

Storing photos (refer to Section 6)

- Use strict privacy settings on the device
- Store photos in the patient's health record
- Always delete the photos from the device
- Avoid third-party storage options and prevent automated back-ups
- Treat photos sent by others as if you took them yourself

Disseminating photos (refer to Section 7)

- Take measures to transmit photos securely where possible
- Never share photos outside of a professional context
- Be wary of social media sharing

Clinical photos and the law

Broadly, clinical photos taken for the purposes of patient management are part of that person's health record, even if they only exist in an electronic format[1]. As such, they should be treated like any other personal health data and are subject to the same conditions for collection, disclosure and storage specified in state/territory and federal laws and regulations. They may be accessed for legal proceedings or in situations where a complaint is raised against a health practitioner. Fines may apply for breaches of privacy as a result of unauthorised disclosure[2].

GPs should act in accordance with the *Privacy Act 1988* (Privacy Act) and Australian Privacy Principles (APPs) when collecting and distributing clinical photos. Under the Privacy Act, a photo of a patient is considered 'personal information' if an individual is reasonably identifiable in the image. A photo is considered 'sensitive information' if it contains health information about the individual or is collected for the purposes of providing a health service. It attracts additional privacy protections compared to other types of personal information under the APPs.

Practice policies and procedures

General practices in which personal mobile devices are used for clinical purposes should consider developing an organisational policy for staff on the use of photos. Such a policy might include information on[3]:

- the production, reproduction, management, retention and disposal of clinical photos
- issues of consent and copyright
- how and when clinical photos should be uploaded or attached to a patient's medical file
- how clinical photos should be removed from a personal mobile device when they have been uploaded or attached to the patient's file
- whether a photography app would be used to capture the image, if relevant
- the maximum number and resolution of clinical photos to be taken and where the photos will be stored as retaining a large volume of high-resolution images in clinical information software systems can create backup issues (this can be discussed with the practice's IT consultant or software supplier).

The practice's policy can be revised as required and discussed with all new staff, including non-clinical staff, during their induction.

Practice owners should also consider purchasing a device reserved specifically for taking clinical photos, to be housed securely on site.

Consent

Obtaining consent

Consent must be sought before photographs are taken. Posing for a photo or positioning oneself in front of a device is unlikely to be considered an acceptable form of consent in a legal context[4].

Consistent with federal and state legislation, consent must be the product of a discussion between the doctor and the patient (or their designated advocate). Such a discussion might cover the following information[2]:

- why the photos are being taken
- how the photos will be used (specify each possible use)
- whether the photos will be shared with others and, if so, with whom (including whether the photos will be posted to social media for clinical opinion from peers)
- how and where the photos will be stored after they have been taken on a personal mobile device
- whether the photos will be de-identified
- how the photos will be archived and/or disposed of.

Consent that is specific to purpose

Using clinical photos for purposes beyond that for which the patient has given consent may leave health practitioners vulnerable to complaints to the Medical Board of Australia or other authorities[5]. GPs should only send a clinical photo to a third party with the patient's express consent, or in a situation where the patient would reasonably expect that the image would be sent to another person as part of their care, or are otherwise permitted by law to share the image[2].

Data breaches

If a device containing clinical photos is hacked, stolen or lost, or photos are sent to a third party without the prior consent of the patient, this might be considered a data breach under APP 11. For advice specific to your situation, contact your medical defence organisation (MDO).

Collecting photos

Take care when using clinical photography apps

There are smartphone apps that are specifically designed for capturing and managing clinical photos. Caution is advised in using apps that have been downloaded from online stores for health information, as it is difficult to tell whether they are credible and secure. It might not be possible to control the use or disclosure of a photo shared via an app. It is wise for users to review the app's privacy policy and the app's compliance with cross-border disclosure requirements[6].

Ensure the device has a high-resolution camera

Make sure the device can take clear, high-resolution images with accurate colour retention to reduce potential for misdiagnosis.

Capture only what is required

Adhere to common-sense principles for protecting patient privacy and confidentiality when taking clinical photos, regardless of the device that is being used.

- Avoid gratuitous detail irrelevant to the presentation (eg by taking a cropped image rather than a full-body shot where this is more appropriate).
- Be mindful it may be possible for a patient to be identified by their eyes and, other facial structures, race, age, scars, birthmarks, tattoos and piercings.
- When using photos for research or education purposes, remember the rarer the presentation, the more likely the patient will be able to be identified[2].

Photo-sharing apps may have a feature that allows the user to conceal parts of the image that contain potentially identifying details. With each use, it is important to consider whether the concealments sufficiently de-identify the patient before the image is distributed[6].

Remove metadata when de-identifying photos where applicable

Digital photos contain hidden information (metadata) that might identify a person, including the time and date the image was taken, the manufacturer and model of the device, and the Global Positioning System (GPS) location. When a clinical photo is to be used in research or as a teaching tool, metadata should be removed as part of the process of de-identifying the image. It is good practice for individuals to research how best to remove image metadata as the process varies depending on the device used to take the image. Many devices have a feature that allows the user to disable the automatic generation of metadata when a photo is taken.

Storing photos

Use strict privacy settings on the device

As per the RACGP's *Standards for general practices* (5th edition), general practices should take reasonable steps to ensure personal mobile devices used in the practice and the information stored or accessed on them are as secure as the practice's desktop computers and network.

It is good practice for clinicians to equip personal mobile devices used for clinical photos with a PIN, password, or other identity recognition software to protect and secure the information[6].

All mobile devices have unique identification numbers which can be retrieved in the 'settings' menu. These can be quoted to the service provider or police in the event of theft and allows the owner to lock or erase data from the device remotely.

Store photos in the patient's health record

Clinical photos taken on personal mobile devices should be stored against the patient's health record as soon as is practicable after they are taken, with a label and notes on the consultation and diagnosis[2]. Some clinical information systems allow the upload of digital picture files for easy storage. Photos can also be printed and scanned to add to patient records.

Always delete photos from the device

Clinical photos should be deleted from the personal mobile device on which they were taken or accessed when they have been stored against the patient's file.

Avoid third-party storage options and prevent automated back-ups

Online image storage options (cloud-based solutions) can be fraught with problems. There are many different companies that offer this service and their privacy policies vary.

Many apps used on personal mobile devices periodically back up their data to cloud storage as an automated task. It is wise to disable this feature in all relevant apps on devices used for clinical photos, as anything uploaded to the cloud has the potential to be accessed and distributed by others.

Apps that organise recent photos in a device for easy upload, such as Facebook, should be used with caution as this feature can lead to accidental dissemination of sensitive material.

Treat photos sent by others as if you took them yourself

Clinicians who receive a clinical photo from another person (such as a health practitioner or a patient) might be bound by the same ethical and legal requirements that would apply if they had taken the photo themselves. Ensure the photo is stored against the patient's health record and deleted from the device[2].

Disseminating photos

Take measures to transmit photos securely where possible

Clinical photos can be intercepted by a third party when they are sent from one device to another, such as when they are sent to another clinician for opinion or to a desktop computer in the practice. Where possible, set up file passwords or use data encryption software to protect clinical information during transmission.

Never share photos outside of a professional context

GPs should be mindful of their ethical, professional and legal duty to respect patient privacy and confidentiality, and always refrain from exhibiting clinical photos on a personal mobile device with others outside of a professional context.

Be wary of social media sharing

Photos posted to a social media platform can end up in the public domain, even when they are sent in a private message conversation, a 'secret' or 'closed' group, or a personal profile with strong security settings. Do not post clinical images to social media unless the patient has provided specific permission for this. If a patient has provided permission, ensure appropriate measures to de-identify the image have been taken prior to posting it to platforms such as Facebook, Twitter, or Instagram.

Additional reading from the RACGP

Guide for the use of social media in general practice: www.racgp.org.au/your-practice/ehealth/social-media/guide

Information security in general practice: www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice

mHealth in general practice – A toolkit for effective and secure use of mobile technology: www.racgp.org.au/running-a-practice/practice-resources/practice-tools/mhealth-in-general-practice

Standards for general practices (5th edition), www.racgp.org.au/your-practice/standards/standards-for-general-practices-(5th-edition)

References

1. 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(1):48-9.
2. Medical Indemnity Industry Association of Australia and Australian Medical Association. Clinical images and the use of personal mobile devices: A guide for medical students and doctors. West Perth, WA: MIIAA/AMA; 2014.
3. Burns K, Belton S. Clinicians and their cameras: policy, ethics and practice in an Australian tertiary hospital. Australian Health Review. 2013;37(4):437-41.
4. 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(11):499-500.
5. Montgomery J. Get smart: clinical images and smartphones. Sydney, NSW: Avant Mutual Group; 2017. Available at http://www.avant.org.au/news/get-smart-clinical-images/
6. Office of the Australian Information Commissioner. What should health service providers consider before taking a photo of a patient on a mobile phone? Available at https://www.oaic.gov.au/agencies-and-organisations/faqs-for-agencies-orgs/health-service-providers/what-should-health-service-providers-consider-before-taking-a-photo-of-a-patient-on-a-mobile-phone