Clinical images and the use of **personal mobile devices**

A guide for medical students and doctors

miiaa
MEDICAL INDEMNITY INDUSTRY ASSOCIATION OF AUSTRALIA

AMA

Foreword

In the interests of upholding the principles of medical professionalism, the Australian Medical Association (AMA) and the Medical Indemnity Industry Association of Australia (MIIAA) have produced this guide for the proper use of personal mobile devices when taking clinical images.

The guide outlines the key ethical and legal issues to be aware of before using a personal mobile device to take or transmit clinical images for the purpose of providing clinical care. The guide does not specifically cover other purposes such as research, teaching, or training.

While the guide may be useful for doctors working in other clinical settings, it is primarily intended for use by Medical Students and Doctors in an Australian Public Hospital environment.

This guide should always be read in conjunction with any relevant privacy legislation, and any hospital policies and contracts related to clinical images and the use of personal mobile devices.

Medico-legal input for this publication was provided through the MIIAA by experts from Avant Mutual Group and MDA National.

miiaa
MEDICAL INDEMNITY INDUSTRY ASSOCIATION OF AUSTRALIA

AMA

Key points to remember

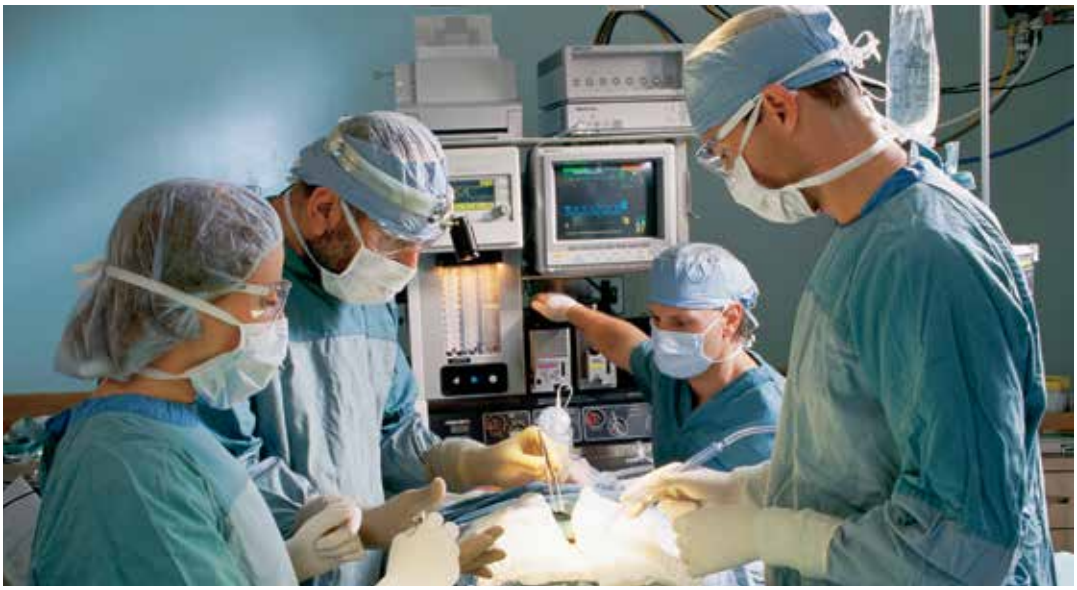
Collection, use, and disclosure of clinical images taken with a personal mobile device

- 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 if the patient would reasonably expect you to send the image for the purpose of their clinical management, or if 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.

Privacy and confidentiality



Case Study One

An elderly patient was undergoing cardiac surgery. At the conclusion of the operation, the patient arrested and CPR was commenced, including internal cardiac compressions. A medical student filmed the resuscitation on her iPhone, and posted the footage on Facebook. Although the patient was not identifiable, the student tagged the name of the hospital in her status, "Guess what happened at work today?" A colleague, who was one of the student's Facebook friends, saw the footage and reported it to management. The matter was reported to the University.

Maintaining confidentiality is an essential part of any clinical consultation. Doctors have an ethical, professional, and legal duty to respect patient rights to privacy and confidentiality regarding their personal and health information, and how it should be used.

Clinical images are "health information", and must be treated with the same privacy and confidentiality as any other health record or information. They should only be taken with appropriate consent, stored securely, and only disclosed in accordance with the consent given, or if there is a legal obligation to do so.

Using clinical images for any purpose other than that for which consent has been obtained, or sharing them in a non-professional context, is inappropriate. Breach of your obligations under privacy laws may result in a substantial fine, and you also risk being the subject of a complaint to AHPRA, health complaints entity, or an internal hospital investigation.

Decision making process for collecting, using and storing clinical images for the purposes of clinical care

Collection

At all times, follow the hospital policy/the terms of your contract.

- Would this patient's care benefit from a clinical image?
  - YES → Should I be the person taking the image?
    - YES → Am I planning to use my personal mobile device?
      - YES → Does my hospital have a policy or does my contract have a clause about using my personal mobile device?
        - YES → Follow hospital policy/terms of your contract.
        - NO → Obtain the patient's consent to take the photo for the particular purpose, and document their consent.
      - NO → Use the hospital's equipment.
    - NO → Talk to an approproate person about taking the image.
  - NO → Am I taking the image for the purpose of teaching, training, or research?
    - YES → Obtain patient's consent, and follow any relevant hospital policy.
    - NO → Don't take the image.

Take the photo, record who took it, when it was taken, and the mode of capture.

Use and disclosure

- Do I want to show the image to someone else?
  - YES → Is the image identifiable?
    - YES → Is it for a purpose related to clinical care, or for a purpose the patient would reasonably expect?
      - YES → You can send the image.
      - NO → You will need specific consent from the patient for the particular purpose.*
    - NO → Does the hospital's policy cover sending the image to someone else?
      - NO → You can send the image without specific consent (subject to privacy legislation), but when you take the image you should notify the patient that this may be done.
  - NO → See STORAGE AND SECURITY.

*Unless otherwise permitted, or required by law to disclose without consent.

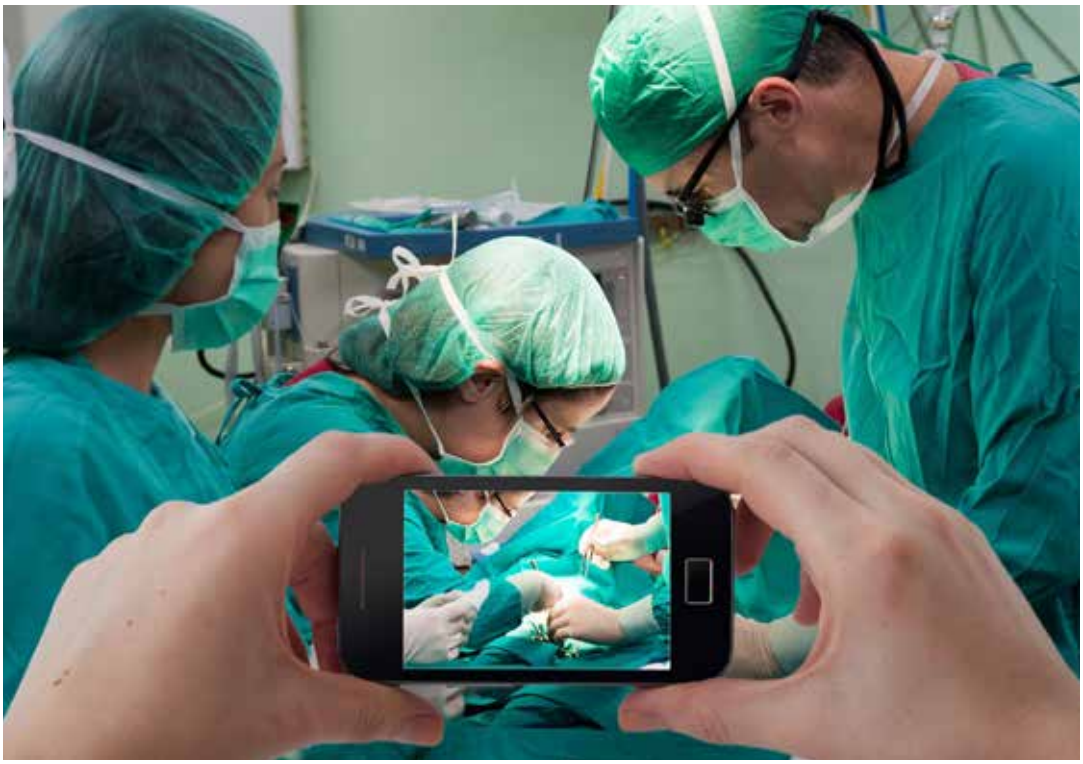
Storage and security

Clinical images taken on personal mobile devices for clinical purposes are part of the clinical record and are the property of the hospital.

- Are you aware of the hospital policy?
- Have you transferred the image to the patient's record?
- Have you recorded who took the image, when it was taken, and the mode of capture?
- Is your personal mobile device password protected and secure from unauthorised access?
- Have you made sure photos on your personal mobile device do not auto-upload?
- Have you deleted the image from your personal mobile device once it's been saved to the record?

What is a clinical image?

For the purposes of this guide, a clinical image may be a photo, video recording, or audio recording. A clinical image may be of the patient's body - such as an injury, skin lesion or body fluid - or an image of a pathology report, diagnostic image, or medication.



Benefits of clinical images

There are many benefits to taking clinical images. For example, they can capture the state of a lesion and track changes over time.

The availability of personal mobile devices, and the widespread use of digital and social media, means that a clinical image can be taken immediately and sent to a colleague in another location for advice on diagnosis, treatment, and management.

Sharing images in this way can improve clinical practice and inter-clinician communication, and improve patient access to timely clinical care, particularly where access to specialist care and advice is limited or absent. Clinical images can also be a beneficial adjunct to teaching and training.

Hospital policies and contracts

Case Study Two

Mr Lim was admitted to the ED with a large laceration to his thigh. An intern obtained Mr Lim's consent to take photographs of the laceration for the purpose of sending them to the surgeon for review and advice regarding management. The intern forwarded the images to the surgeon and to medical records, as requested. Three months later, a member of staff witnessed the images being shown by the intern on their phone to other doctors on the ward. A complaint was made to the Director of Medical Services regarding the images being present on the intern's phone. It was found that the intern had breached the hospital's clinical image policy.

While many hospitals and health departments around Australia have implemented clinical image policies, there is evidence that not all doctors are aware of or follow these policies.

It is important to ensure that all doctors working in public hospitals understand and follow the organisation's policies and contracts with respect to clinical images and the use of personal mobile devices.

Some organisations may prohibit the use of personal mobile devices to capture clinical images, in their employment contracts and/or policies.

Where a hospital does have a policy on clinical images and the use of personal mobile devices, doctors should follow this in the first instance and use this guide as further information.

Where a hospital does not have a policy on clinical images and the use of personal mobile devices, this guide will provide useful information on steps to consider when taking an image using a personal mobile device.

Consent to collection, use, and disclosure of clinical images taken with a personal mobile device

Obtaining consent to collect a clinical image

Case Study Three

Mr Jones was to undergo excision of an unusual rectal lesion. After he was anaesthetised, the surgical team pointed out key features of the lesion to an RMO, who took several photos of the lesion on his mobile phone. The RMO was subsequently asked to attend a meeting with the Director of Clinical Services, during which he was informed that a staff member had complained about him taking photos in the operating room. The RMO explained that preoperatively he had asked the patient if he could take pre- and post-operative photos of the lesion for therapeutic and teaching purposes. The RMO explained that the patient was happy for photos to be taken, but conceded that he had not recorded this in the clinical notes, or asked the patient to sign a "Consent to Photographs" form.

Patients have the right to consent to (or refuse) the collection, use, and disclosure of clinical images. Only competent patients can provide consent; however, where a patient lacks decision-making capacity, consent should be sought from the patient's substitute decision-maker (see Complex Circumstances).

You should discuss the following information with the patient (or their substitute decision-maker) to ensure they make an informed decision when consenting to (or refusing) the collection, use, and disclosure of clinical images:

- The purpose(s) of the clinical image i.e. why the clinical image is being taken.
- How the clinical image may be used e.g. an image could be used in a de-identified form for training and education purposes.
- Who will have access to the image.
- Whether it might be shared and disclosed to others, and for what purposes.
- Whether it will be de-identified.
- How and where it will be stored.

Right to refuse consent

Patients have the right to refuse a clinical image being taken. A patient's refusal to consent to clinical images should not compromise their care where there is a suitable alternative. However, they should be informed as to how clinical images may be of assistance to their doctors.

There may be exceptions to a patient's right to refuse consent, such as where a court order requires it. If this is the case, doctors should clarify the scope of the requirement with their hospital administration or medical defence organisation.

Scope and nature of consent

The scope and nature of the patient's original consent may need to be considered when later deciding to what extent the clinical image can be used and disclosed. Additional consent may be required to use the images for these purposes.

Withdrawing consent

While patients have the right to withdraw their consent for an image to be used, they should be informed when obtaining consent that, once an image has been taken and forms part of the health record, it cannot normally be deleted from the record.

When obtaining consent, any limits to removing images in the future should be explained to the patient. For example, where a patient has consented to their image being used in a publication, it may not be possible to have that image removed once it has been published.

Documenting the consent process

The consent process should be documented in the medical records, including the scope and details of the consent. For example, if an image is taken and sent to a senior colleague to obtain clinical advice, the patient should be informed and a note made in the record e.g. "photograph of wound taken on PMD and sent to Dr X for clinical advice". Some hospitals and practices also require that the patient sign a consent form, which should be placed in the medical records with the clinical image.

A patient's refusal, or withdrawal, of consent should also be documented in the health record.

Use and disclosure of clinical images

As with any health information, a doctor should only use and/or disclose clinical images in accordance with relevant privacy legislation and/or a hospital's policies. In general, this means that clinical images should only be used and/or disclosed:

- for the direct or primary purpose for which they were collected;
- for a secondary purpose closely related to the direct or primary purpose;
- in accordance with the patient's consent (if the use and disclosure is different from the direct or secondary purpose); or
- where permitted by law – that is, the use and disclosure falls within an exemption under the relevant privacy legislation.

The direct or primary purpose is the purpose (or purposes) the patient was informed about when he or she provided consent for the image to be collected. In the health context, this would normally be related to the provision of clinical care and treatment, but it could be for medical research or training if this was explained to the patient when the image was collected.

Example: on presentation to the Emergency Department a clinical image of a facial lesion is taken as a record of the patient's condition at the time. The direct purpose is to capture details of the patient's lesion.

A secondary purpose closely related to the direct or primary purpose is one where the patient has a reasonable expectation that the clinical image would be used in this way. This covers the provision of clinical care, including sharing the image with a colleague to confirm diagnosis, treatment, and management.

Example: the clinical image of the facial lesion is sent to or shared with a dermatologist for advice on the appropriate treatment for the patient.

Example of a use that would not be a secondary purpose: the clinical image of the facial lesion is stored in an identifiable form on the doctor's smartphone. It is later emailed to another doctor who posts it on Facebook as a good example of that type of unusual lesion. The patient would not have reasonably expected that his clinical image would be used in this way.

To avoid any dispute about whether the use or disclosure of an image is in the reasonable expectation of a patient, it is advisable to inform the patient as to how the image may be used when obtaining consent to take an image. This provides the patient with an opportunity to let you know if they object to such use.

Patient consent – a clinical image can be used or disclosed in a way that is different to its direct or secondary purpose where the patient consents to the clinical image being used or disclosed in this way. This consent should be documented.

Other circumstances where you may be able to use or disclose a clinical image

Circumstances may exist where you are allowed or required by law to disclose clinical images to third parties without patient consent. For example, to prevent a serious threat to the safety or health of a patient or the public. However, you should always seek advice from your hospital management and, if necessary, consult with your medical defence organisation as to when these circumstances apply.

De-identification of clinical images

Clinical images used for teaching, training, and research should be de-identified, where possible, and must comply with relevant research or ethical guidelines.

When de-identifying photographs, remember that seemingly insignificant features, such as tattoos, can still make a person identifiable to others. Even when all identifying features are removed, sometimes the clinical condition itself may provide recognition - the rarer the clinical presentation, the more likely it may be identifiable.

Also remember that digital images may contain metadata that could be used to identify an individual, despite other identifiers being removed. This may include the time/date of capture, the device that was used, and the GPS location of capture. Care should be taken to remove this data when de-identifying images.

Key Points to Remember

- 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 if the patient would reasonably expect you to send the image for the purpose of their clinical management, or if 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

Retention of clinical images

Health information has to be retained for set periods of time prescribed by legislation. This requirement extends to the retention of clinical images.

Hospitals and their staff have a duty to take reasonable steps to protect the personal information they hold, including clinical images, from misuse, loss, unauthorised access or interference, modification, and disclosure.

Storage in the health record

Clinical images taken by doctors on their personal mobile device in the course of providing clinical care are part of, and should be stored securely in, patient's health record. This means that clinical images are treated in exactly the same way as other clinical records in terms of security and decisions about disclosure. They may be accessed for use in legal proceedings or patient complaints.

If the purpose for obtaining the clinical image is to provide clinical care, the patient's details should be linked to the image to ensure proper identification. It is essential to record who took the image, when it was taken, and the mode of capture.

Copyright

Clinical images included in the health record are generally the property and responsibility of the health service/hospital, even if they have been taken on a personal mobile device.

Transferring the clinical image from a personal mobile device to the health record – reasonable steps

Some organisations have systems in place that provide a secure platform to enable doctors to transfer an image from their personal mobile device to a patient's health record safely, securely, and effectively. Find out if your hospital has a process that allows you to transfer an image from your mobile device and store it electronically.

If it doesn't, you will need to produce a hard copy/copies of the image to store in the patient record.

Securing your mobile device – reasonable steps

While the clinical images reside on your personal mobile device, you must take reasonable steps to have controls on the device to prevent unauthorised access. Make sure any clinical images do not auto-upload to any social media networks or back-up sites that might be publically available.

Your mobile device should have password protection, and you should be able to erase images remotely if your device is stolen.

Leaving clinical images on a mobile device increases the risk of unauthorised access if the device is lost or stolen, and increases the risk of the image being sent by mistake to an unauthorised third party.

Deleting clinical images from your mobile device

Once images taken for the purpose of providing clinical care are securely stored in the patient's health record, they should be immediately deleted from the mobile device.

Key Points to Remember

- 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.

Access to clinical images

Case Study Four

A patient presented to hospital late at night with injuries she reported were caused by her partner in a domestic violence incident. The doctor used his smartphone to take photos of the injuries. The patient later subpoenaed her medical record from the hospital. Neither the photos nor audio recording were produced to the court. The court required production of the photos and audio recording on the basis that they formed part of the patient's records. The doctor had kept the images on his phone.

Keep in mind that patients are entitled to request access to, and obtain a copy of, their health record, including any clinical images. These images may also need to be produced to a court for legal proceedings.

Receipt of clinical images

Case Study Five

A Registrar is at home on call. At about 11.30pm, he is woken by an intern who wants to send him a clinical image on his smartphone to obtain advice about a patient. The Registrar reviews the image and calls the intern to provide the necessary advice. He then goes back to sleep, leaving the clinical image on his phone.

If you receive a clinical image from a third party on your personal mobile device, you are bound by the same legal and ethical requirements as if you had taken the image.

You will need to consider what your obligations are regarding the acquisition, quality, use and disclosure, storage, and disposal of the clinical image. It may be necessary to discuss this with the person who sent you the image.

In most cases, the person who obtained the image has the responsibility for incorporating the clinical image in the patient's health record. Once this is done, it is not necessary for the receiver of the image to retain a copy as well, and it should be deleted from the personal mobile device.

Clinical images taken by, or provided by, patients

Case Study Six

A father presented to the Emergency Department with a photo he had taken of his son's wound when it first occurred. The wound has since become infected. It would be useful to have a copy of the father's photo for the son's medical record for future treatment purposes.

In this case, the photo is the property of the father. You can ask for a copy of the photo, explaining how it will be used, and where it will be stored. In most cases, patients or their representatives are likely to agree with such a request, but they are not obliged to provide you with a copy of their photo. You should explain that, once the photo forms part of the health record, it has to be retained along with the rest of the record. It cannot be deleted until the retention period expires.

Image quality

The quality of the clinical image is a key consideration. Think about whether the resolution of the mobile device you are using can provide the image quality you will require; accurate colour retention and image definition are vital if the image is to be used to assist diagnosis and treatment, or for research purposes. This is particularly the case when transmitting images of previously obtained diagnostic images or pathology reports.

Complex circumstances

There are some circumstances where it may be difficult to be certain that you have addressed the legal issues correctly. These include clinical images that involve:

- Children.
- Adults with impaired capacity.
- Intimate areas of the body.

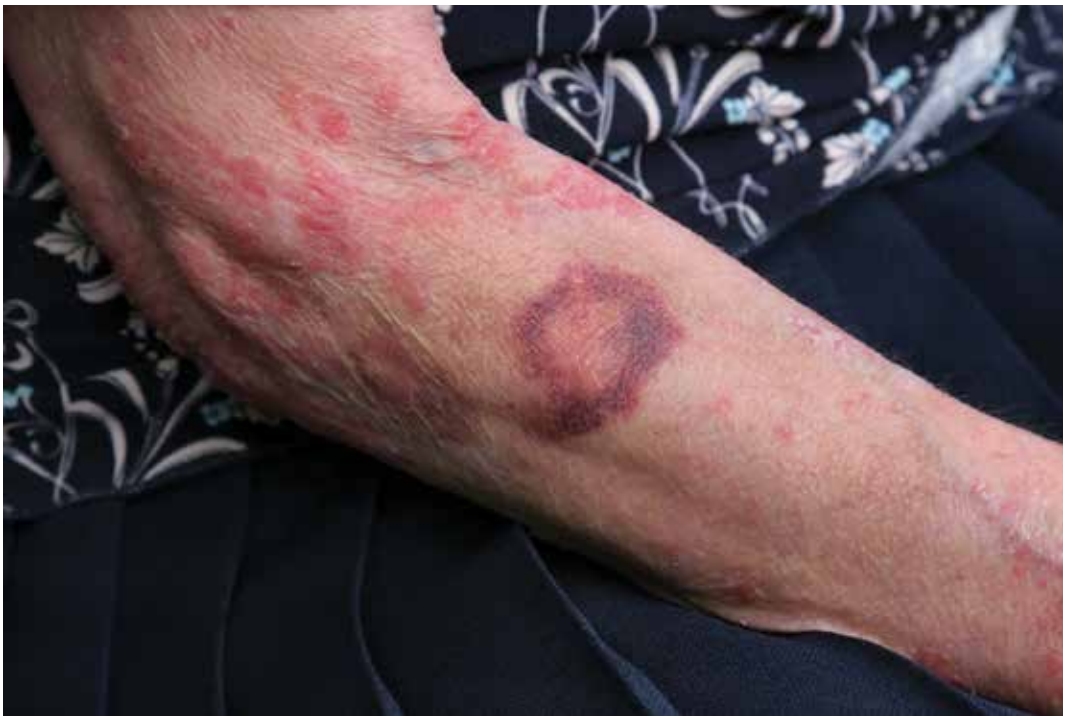
Children

Children's hospitals often have strict policies in relation to how and when clinical images can be taken.

When taking pictures of children, make absolutely certain that it is necessary to do so, and appropriate consent has been obtained and documented.

There is no defined age at which children can provide valid consent. For young children, their parents or guardians generally provide consent, and sign any consent forms. If the child appears distressed at having an image taken, you will need to reconsider your position, even if the parent or guardian has provided consent.

Older children and young people under 18 years of age will need to be assessed to determine if they have sufficient maturity to understand fully the purpose for taking the clinical images. If so, consent will need to be obtained from them, and you should encourage input from their parents.



Adults with impaired capacity

Where an adult patient lacks decision-making capacity, consent from the appropriate substitute decision-maker must be obtained. If a patient's lack of capacity is temporary or fluctuating, it may be better to wait until they regain capacity, and can make their own informed decision.

If no-one is available to provide consent, and treatment is urgent, the images can be taken in accordance with relevant laws about emergency treatment.

Intimate areas of the body

Remember that particular care should be taken where images may be considered pornographic or obscene, if taken out of context. An image risks being considered pornographic or obscene if it includes unnecessarily sensitive content that is not relevant to the clinical purpose. It should be remembered that it is a serious criminal offence to disseminate pornographic images electronically.

Ask for advice

In these circumstances, and at any time you feel uncertain about how to proceed with the use of clinical images, always contact your hospital administration or medical defence organisation for advice related to your specific situation.

Resources

State and Territory Privacy Law

- The Office of the Australian Information Commissioner (OAIC). S*tate and territory privacy law* http://www.oaic.gov.au/privacy/other-privacy-jurisdictions/state-and-territory-privacy-law

Australia

- Australian Medical Association. *Social Media and the Medical Profession: A guide to online professionalism for medical practitioners and medical students*. https://ama.com.au/social-media-and-medical-profession
- Australian Medical Association. *AMA Code of Ethics. 2004 (Editorially Revised 2006).* https://ama.com.au/codeofethics
- Australian Medical Association. *Medical practitioner responsibilities with electronic communication of clinical information.* 2013. https://ama.com.au/position-statement/medical-practitioner-responsibilities-electronic-communication-clinical
- Australian Health Practitioner Regulation Agency. *National Board policy for registered health practitioners. Social media policy. 2014*. http://www.medicalboard.gov.au/Codes-Guidelines-Policies/Social-media-policy.aspx
- Medical Board of Australia. *Good Medical Practice: A Code of Conduct for Doctors in Australia*. 2014. http://www.medicalboard.gov.au/Codes-Guidelines-Policies/Code-of-conduct.aspx
- The Medical Indemnity Insurance Association of Australia http://www.miiaa.com.au/
- National Health and Medical Research Council. *National Statement on Ethical Conduct in Human Research. 2007 (updated May 2013).* http://www.nhmrc.gov.au/guidelines/publications/e72

United Kingdom

- General Medical Council. *Making and using visual and audio recordings of patients.* http://www.gmc-uk.org/guidance/ethical_guidance/making_audiovisual.asp
- JISC Digital Media. *Making and using clinical and health care recordings for learning and teaching*. http://www.jiscdigitalmedia.ac.uk/clinical-recordings/index.html