



## **RDA Guidelines with regard to the use of personal mobile devices and clinical images**

### **Introduction**

With advancements in technology, easy access to the internet and email, the ability to record, transfer and share information with others has become second nature. For medical practitioners sharing, recording and seeking advice on medical information is part and parcel of the profession. Sharing images can improve communication between clinicians, clinical practices and can improve patient access to timely clinical care, particularly where access to specialist care and advice is limited or absent.

Most medical practitioners have a personal mobile phone, tablet or laptop at their disposal and this allows the immediate visual recording of medical information which can be sent to a colleague in another location for advice on diagnosis, treatment and management. The image may also be taken for the purposes of recording the information on the patient's clinical record and for training or teaching purposes.

A clinical image may be a photo, video recording, or audio recording of a patient's body, injuries, skin lesions (capturing the state of a lesion and tracking changes over time), body fluid, diagnostic image or medication. All this information can be recorded at the swipe of a screen, however clinical images being taken on personal mobile devices ('PMD') raise a number of ethical and medico-legal issues. The images being taken on PMD's form part of a patient's health record and must be treated with the same privacy and confidentiality as any other health information or record.

Clinical images should only be taken where they are reasonably necessary, for example, to aid in treatment or teaching. They must only be collected with the patient's express consent and the patient must be informed of the purpose of the images being taken and who will have access to them. The images must then be secured, for example, by being placed in the patient's medical record and treated as any other medical information.

### **Key points to consider before taking a clinical image:**

- Before taking a clinical image, consider the purpose for which you require the image
- Obtain informed consent from the patient to take the image
- Confirm with the patient that they understand:
  - the purpose for taking the image
  - when the image will be taken (e.g theatre or recovery)
  - how it will be used

➤ to whom it will be shown

- Record the patient's consent and their understanding of the purpose for taking the image
- Inform the patient that they can withdraw their consent at any time, however there may be limitations to removing the image in the future
- Explain what these limitations are and record the patients understanding of these limitations

**Key points to consider once the image has been taken:**

- Clinical images form part of a patient's clinical record and the patient's details must be linked to their image to ensure proper identification
- The clinical image should be clearly labelled with a clear description of the image itself
- The details of the medical practitioner who took the image, when the image was taken and the mode of capture, should be recorded in the patient's clinical record
- Clinical images used for training, teaching and research must always be de-identified unless there is express consent from the patient to be identified
- Once the image has been authenticated, reasonable steps must be taken to transfer the clinical image from the PMD to the patient's health record
- After the image has been saved in the patient's health record it should be deleted off the PMD

**Key points to consider with regard to the use and management of clinical images:**

- Clinical images should only be used or disclosed for the direct purpose for which they are collected or be used or disclosed for a secondary purpose closely related to the direct purpose
- Using clinical images for any purpose other than that for which consent had been obtained or in a non-professional context is inappropriate
- While images stay on PMD's, reasonable steps must be taken to prevent unauthorised access to the images
- Images should not be uploaded to any social media networks or back up sites that might be publically available
- PMD's must have password protection and the images should be able to be removed remotely if the PMD is stolen

**1. Seeking informed consent**

Clinical images are considered sensitive health information and must only be collected where the patient has given their express consent for the image to be taken. Obtaining informed consent is good professional practice and it maintains patient confidentiality and trust in the medical profession. When obtaining consent it is vital that patients are adequately informed about the reasons for

taking or sharing the images and they must confirm that they understand these reasons.

Informing the patient of the reasons for taking the image should include how the image will be used or potentially used, who will have access to the image, whether it will be shared and disclosed to others, how it will be de-identified and where it will be stored. Further the patient should understand what the images may be used for, for example clinical diagnosis, treatment and management, for teaching or research purposes and for publications in clinical journals, text books and may be uploaded on the internet. It should also be explained if images may be taken when the patient is unconscious, for example, while they are in theatre or when in recovery.

The patient's consent including the purposes for which consent has been obtained should be documented in the medical records. Consent should be recorded in writing. Ideally a signed consent form should be stored with the patient's clinical image. If written consent is not possible the discussion should be recorded in the clinical notes noting specifically what was consented to.

Where a patient does not consent to the image being taken this should also be documented in the patient's health record. A refusal to consent should not compromise the patient's care.

Patients should be made aware that they are able to withdraw their consent at any time however they should be informed when obtaining consent that once an image has been taken and forms part of the medical record it may not be able to be deleted from the record. It should also be explained that there may be limits to removing the images in the future because while patients have a right to withdraw their consent it may not be possible to remove a patient's image from, for example, a publication after it has been published or where they have consented to the images being shared. If a patient does withdraw their consent an appropriate mechanism needs to be put in place to identify the patient's image and remove the image to the extent that it is possible.

Only competent patients can consent to the use of clinical images. Where a patient lacks capacity, surrogate consent from the appropriate substitute decision maker must be sought. If the 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 decisions.

## **2. Management of Clinical Images**

Once a clinical image has been taken on a PMD, the patient's details must be linked to the image to ensure proper identification before it is stored in the patient's file. Appropriate identification and storage of a patient's clinical image, in their clinical record, should occur even if the image is taken for the sole purpose of presentation to a colleague. The clinical image remains a part of the clinical record and is akin to clinical notes being recorded to describe an observation of a particular medical condition.

The clinical image itself should be clearly labelled in the medical record, for example 'photograph of lesion, left upper thigh taken on PMD and sent to Dr XXXX for clinical advice'. It is important to record the details of the medical practitioner who took the clinical image, when the image was taken and the mode of capture.

This is important in the provision of timely, safe and effective care (and is important if the images are required to be used as evidence in legal proceedings).

Clinical images used for the purposes of training, teaching and research must comply with relevant research and ethical guidelines and the images must always be de-identified, unless there is a very good reason not to do so. When de-identifying images, features such as tattoos or birthmarks can still make a person identifiable to others. Sometimes even if all identifying features are removed the clinical condition itself may identify the patient. This should be clearly explained to the patient while obtaining consent and should be clearly recorded in the clinical notes.

If images are to be identified there must be clear, express consent from the patient allowing the images to be identified.

Once the image has been authenticated, reasonable steps must be taken to transfer the clinical image from the PMD to the patient's health record. This may include producing a hard copy of the image to store in the patient's record or there may be a system in place to facilitate the storage of digital images at your health service.

After the image has been saved in the patient's health record it should be deleted off your PMD.

### **3. Use and Disclosure of Clinical Images**

Medical practitioners have an ethical, professional and legal duty to respect a patient's right to privacy and confidentiality with regard to their personal health information and how it is used. Clinical images should only be used or disclosed for the direct purpose for which they are collected or be used or disclosed for a secondary purpose closely related to the direct purpose.

#### Direct purpose

The direct purpose for which the image was collected is the purpose the patient was informed about when they provided consent for the image to be collected. This will be related to the provision of clinical care and treatment, medical research or for training purposes.

#### Secondary purpose

A secondary purpose closely related to the direct purpose is one where the patient has a reasonable expectation that the clinical image will be used in this way, for example, an image being shared with a colleague to confirm diagnosis and treatment.

To confirm a patient's reasonable expectation of the use and disclosure of a clinical image that has been taken, the patient should be informed as to how the image may be used when obtaining consent to take the image. This gives the patient an opportunity to object to such use. Secondary purposes and the patient's consent to those secondary purposes should be clearly documented in the clinical notes.

Using clinical images for any purpose other than that for which consent had been obtained or in a non-professional context is inappropriate.

#### **4. Storage and Security of Clinical Images**

Hospitals and their staff have a duty to take reasonable steps to protect the personal information and clinical images they hold, from misuse, loss, unauthorised access, interference, modification and disclosure. While the images stay on PMD's, reasonable steps must be taken to prevent unauthorised access and it must be ensured that the images are not uploaded to any social media networks or back up sites that might be publically available. PMD's must have password protection and the images should be able to be removed remotely if the PMD is stolen. Leaving clinical images on PMD's increases the risk of unauthorised access to the images if the device is lost or stolen or the image being mistakenly forwarded to an unauthorised third party. Therefore as stated above, after the clinical image has been taken, all reasonable steps should be taken to transfer the clinical image from the PMD to the patient's health record. 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 PMD.