

Clinical Images: Medico-Legal issues

Medisec regularly receives queries from members relating to taking and receiving clinical images and the issues that arise. We recommend that you should always have regard to the following matters:

- Whether there is a lawful basis for you to process the clinical image under the General Data Protection Regulation (GDPR). In this regard 'processing' includes receiving, storing, accessing and using the image
- The requirement for patient consent and how to proceed in the context of minor or vulnerable patients or patients lacking capacity
- Whether remote consulting / relying on imaging is in the patient's best interests or whether a face to face consultation is required
- IT considerations
- The applicable ethical guidance from the Medical Council

This factsheet guides you through each of the above issues in sequence.

1. Data privacy

Lawful basis for processing

Article 9.2(h) GDPR provides a lawful basis for the processing of special categories of personal data in general practice, where that processing '*is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3*'. (emphasis added).

Your records should always reflect why you considered clinical imaging necessary in the context of a patient's care.

2. Consent

As above, Article 9.2(h) GDPR provides a lawful basis for the processing of special categories of personal data in general practice. However, in the context of clinical images, we also recommend keeping a record of having obtained explicit patient consent to taking / receiving and storing the imaging.

Consent to clinical imaging should be sought from a parent / legal guardian in respect of young children. Minors can consent to treatment from the age of 16 (with the exception of mental health treatment) but they may have sufficient understanding and maturity at an earlier age to express an opinion or preference and if so, their views should be taken into account.

We recommend exercising caution in the context of a patient who lacks capacity. It may be that no one has official authority to make decisions on their behalf (e.g. pursuant to Wardship proceedings, or on foot of a power of attorney / enduring power of attorney). In such cases you should have regard to where the patient's best interests lie and whether clinical imaging is necessary in the context of their clinical care.

3. Remote consulting

If clinical imagery is provided or requested in order to determine appropriate care or reach a diagnosis in the absence of a face to face consultation, we recommend:

- Considering whether it would be in the patient's best interests to wait until they can attend in person. If this is not feasible and / or delaying could potentially cause further harm or delay further investigation, you may decide the use of clinical imaging and a remote examination is appropriate. Your records should reflect your decision making in this regard.
- Deciding on the most appropriate modality for the imaging. A video consultation may provide a better overview whereas a photograph typically provides better resolution.
- Discussing with the patient the limitations of relying on imaging and conducting examinations remotely. Explain that ultimately, a physical examination may still be required.
- Considering the patient's need for privacy and comfort with their environment and ensuring no interruptions at your end.
- Obtaining the patient's informed consent to proceed.

4. IT considerations

- It is recommended that doctors use a secure platform for processing clinical images, rather than rely on freeware apps or personal devices. If a patient is planning to send you a clinical image, you should advise the patient to send it to your secure Healthmail account.
- You should also let the patient know that any personal device they may be using to take and send the imaging may not be secure and that the transmission from them to you of the imaging may not be secure / encrypted either.
- Any device which you use to take or receive clinical imagery should be properly secured. Your IT consultant can advise on appropriate measures.
- Clinical images should be transferred securely from personal devices to the correct patient's records within the practice software at the earliest opportunity. All images should be securely deleted from the personal device afterwards.
- Just like clinical records, clinical images should be protected with back-up (disaster recovery), robust security, encrypted data transmission and appropriate user access controls.
- The practice IT provider can provide best practice guidance on IT safeguards and controls and practice.
- The practice IT and record keeping policies should specify in detail how clinical images are managed and adherence should be monitored.

5. Ethical Obligations

The Medical Council's Guide to Professional Conduct and Ethics for Registered Medical Practitioners 2024, contains a number of relevant provisions of which doctors should be aware.

Section 31: Photographic, video or audio recording of a patient by a doctor

31.1 Making audio, video or photographic recordings of a patient on your personal or work devices may be necessary for safe patient care. You must take particular care in relation to the storage and sharing of recordings of a patient.

31.2 Where you determine that making audio, video or photographic recordings of a patient is necessary and appropriate for patient- care and/ or beneficial for education and training purposes, you must explain this to the patient and obtain their consent to both the making and any proposed sharing of a recording.

31.3 You must take all reasonable and required steps to ensure that you follow your professional duty of confidentiality as well as your legal duties regarding data protection. You should keep these recordings confidential as part of the patient's record (see paragraph 38). If they are being used for education and training purposes beyond the patient's healthcare team, you must ensure that the patient is neither identified nor identifiable, unless they have given consent to being identified.

31.4 You should be aware of security when sharing information by electronic means, including text, other electronic messaging or emailing, and you should take all reasonable measures to protect confidentiality.

- **Section 24: Physical and intimate examinations (Chaperones)**

While paragraph 24 of the Medical Council Ethical Guide refers to “physical and intimate” examinations, the same standards apply to consultations carried out remotely. That paragraph states:

24.2 Before undertaking any physical examination, including an intimate examination, you should discuss this with the patient, explaining why it is needed, what will be involved and addressing any concerns that the patient may have, and obtain consent.

24.3 Intimate examinations include examinations of breasts, genitalia and rectum. Consent for intimate examinations must be documented in the patient’s medical record.

24.5 A chaperone can act as a safeguard for both the doctor and the patient during an intimate examination. You should ask the patient if they would like a chaperone to be present and record their wishes.

24.6 If a chaperone is not available, you should confirm if the patient wishes to proceed or make alternative arrangements, as long as the delay would not adversely affect the patient’s health.

In summary, clinical images sent to a doctor should be treated as medical records and should be stored securely in the patient’s records, with adequate security systems in place. Patients’ clinical images should not be stored separately to their patient files.

Any medical information, including images should be stored and retained in accordance with data retention policies, having regard to the time periods for each category of data. Please do not hesitate to contact Medisec if you require further guidance.

The contents of this publication are indicative of current developments and contain guidance on general medico legal queries. It does not constitute and should not be relied upon as definitive legal, clinical or other advice and if you have any specific queries, please contact Medisec for advice.

Medisec Ireland CLG is a private company, limited by guarantee, having its registered office at 7 Hatch Street Lower, Dublin 2. Registration No. 216570. Medisec Ireland CLG (trading as Medisec Ireland) is regulated by the Central Bank of Ireland. Medisec’s risk, education and medico-legal advisory services are not regulated by the Central Bank of Ireland.