FACTSHEET

MEDISEC

We look after you

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.

MEDISEC

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 8th edition 2016, as amended, contains a number of relevant provisions of which doctors should be aware.

- **Section 33 : Medical Records**

33.1 Medical records consist of relevant information learned from or about patients. They include visual and audio recordings and information provided by third parties, such as relatives.

33.2 You must keep accurate and up-to-date patient records either on paper or in electronic form. Records must be legible and clear and include the author, date and, where appropriate, the time of the entry, using the 24-hour clock.

33.3 If you are working in out-of-hours services or telemedicine, you should make every effort to ensure that any notes you make about a patient are placed in the patient's medical record with their general practitioner as soon as possible (see paragraph 43).

33.4 You must comply with data protection and other legislation relating to storage, disposal and access to records. You should understand the eight rules of data protection.

33.5 Patients have a right to get copies of their medical reports except where this is likely to cause serious harm to their physical or mental health. Before giving copies of the records to the patient, you must remove information relating to other people, unless those people have given consent to the disclosure.

33.6 You should keep medical records for as long as they are likely to be relevant to the patient's care, for the time the law or practice standards require. You may also wish to take advice from your medical defence organisation or legal advisor about retaining records for medico-legal records.

- ## Section 34 : Recording

34.1 Audio, visual or photographic recordings of a patient, or a relative of a patient, in which that person is identifiable should only be made with their express consent. You should keep these recordings confidential as part of the patient's record. You should be aware of security when sharing information by electronic means, including text, other electronic messaging or emailing, and you should do all you reasonably can to protect confidentiality. You should get consent before sharing videos, photos or other images of patients.

34.2 In exceptional circumstances, you may take images of patients using your personal mobile device. You should do so only when this is necessary for the patient's care. The images must not identify the patient, must be kept for the minimum time needed, and must be deleted as soon as possible. You are responsible for data protection in this regard and you must comply with any rules and procedures of your employer.

- ## Section 35: Offering a Chaperone

While paragraph 35.3 of the Medical Council Ethical Guide refers to "physical and intimate" examinations, the same standards apply to consultations carried out remotely. That paragraph states:

> *"Where an intimate examination is necessary, you must explain to the patient why it is needed and what it will entail. You must ask the patient if they would like a chaperone to be present – for example, a nurse or family member - and note in the patient's record that a chaperone was offered. You should also record if a chaperone was present, had been refused, or was not available but the patient was happy to proceed."*

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 your require further guidance.

MEDISEC

April 2021