FACTSHEET

MEDISEC

We look after you

GDPR – Data Subject Access Requests

It is important to have an agreed process in the practice for dealing with access requests under GDPR and Medisec recommends keeping a log of any Data Protection requests received.

A suggested workflow for handling access requests:

- **[Nominee]** logs the date of receipt of the Data Protection request in a central register and notes the nature of the request.
- **[Nominee]** records the deadline for response and an advance reminder in a Data Protection diary.
- **[Nominee]** acknowledges the request within three working days and confirms that a response will issue before the 30-day deadline.
- **[Nominee]** identifies and locates the relevant records within five working days.
- **[Practice to determine appropriate staff member to carry out preliminary review in respect of different categories of requests.]**
- Decision in respect of the request made and recorded by the DOCTOR, including the reasons for same.
- **[Nominee]** prepares to implement decision made e.g., preparing copy records for release and drafts notification to requestor of decision within 30-day timeline.
- **Treating doctor** reviews any records and the cover letter again prior to release.

While we are aware of the discretions provided to data controllers who are not health practitioners under the Data Protection Act 2018 (Access Modification) (Health) Regulations 2022, given that there may be entries in the medical records which may be likely to cause serious harm to the physical or mental health of a particular patient, we recommend that a GP does not delegate requests to release patient data to a member of their administrative staff. We recommend that a GP carefully reviews and considers each request on a case-by-case basis, which we appreciate can be time consuming. We recommend that the treating doctor should review the records to make decisions on requests for access / correction / deletion in respect of health data and clinical records.

Medisec recommends that an entry be made on the records noting the decision-making process in relation to a Data Protection request, the date when a response and information was sent, what was sent and to whom. We recommend that a doctor should document carefully their decision-making process separate to the consultation records but nonetheless in the patient's file.

Different types of Data Protection Requests

• Access (Article 15 GDPR)

A patient has the right to request confirmation from the practice as to whether or not personal data in relation to him / her are being processed. Where that is the case, the patient has the right to request access to the personal data and the following information:

a) The purposes of the processing;
b) The categories of personal data;
c) Recipients / categories of recipients with whom the personal data have been or will be disclosed;
d) The envisaged period for which the personal data will be kept;

e) The existence of the right to request rectification / erasure / restriction and of the rights to object to processing;
f) The existence of the right to make a complaint to the Data Protection Commissioner;
g) Where personal data are not collected from the patient directly, their source;
h) Whether automate decision making is carried out in relation to the personal data.

A patient can exercise his / her rights by writing to the practice, setting out his / her request. Data Protection requests must be written to be valid. An email is a valid written request.

The practice should be satisfied that the patient has the capacity to make the request and if so, that the request is actually being made by them.

The patient is entitled to request a copy of the personal data and the information set out above, free of charge. A reasonable administrative fee may be charged for providing duplicate copies.

A patient's right to access and obtain their personal data should not affect the rights of others e.g. third party's rights to privacy. This generally means third party information must be redacted out of any medical records before they are released to a patient. If redactions are applies, the rationale for this must be clearly set out to the patient e.g. "*lines redacted from entry dated XX/XX/XXXX constituting third party information.*"

However, the need to redact parts of the records should be considered on a case by case basis and a doctor should consider whether the redactions would defeat the purpose of the request for disclosure. If you have any queries in relation to the redaction of a part of a patient's medical records, please contact the advisory team at Medisec for specific advice.

When it is appropriate to redact information, it should be clear from the records that redactions have been made. This can be done by using a software redaction tool / black marker.

If releasing the records may involve disclosing a consultant's letters or documents, the consultant may be informed, as a matter of courtesy, of the pending disclosure before the records are actually released.

If the patient's records contain consultants' reports on the patient's mental health, the consultant should be asked to provide their opinion on whether the release of such records is likely to harm the patient's health.

• Rectification (Article 16 GDPR)

A patient has the right to request to have inaccurate or incomplete personal data concerning him / her rectified, without undue delay. Additionally, if the practice is keeping personal data with no good reason to hold it i.e. it is irrelevant or excessive for the purpose or was not obtained fairly, the patient may be entitled to have this information rectified (or erased, see next section).

Clinical records are intended to be a contemporaneous record of a consultation and it may not be appropriate to rectify records. It may be possible to deal with a request for by creating a new, separate entry which notes the details of the patient's request and records the doctor's decision and reasoning.

• Erasure (Article 17 GDPR)

A patient has the right to request to have personal data erased without undue delay where one of the following grounds applies:

a) The personal data are no longer necessary for the purpose for which they were collected or processed;

b) The patient has withdrawn consent on which the processing was based and where there is no other legal ground for the processing;
c) The patient objects to the processing of the data and there are no overriding legitimate grounds for the processing;
d) The personal data have been unlawfully processed;
e) The personal data have to be erased pursuant to a legal obligation.

Additionally, if the practice is keeping personal data with no good reason to hold it i.e., it is irrelevant or excessive for the purpose or was not obtained fairly, the patient may request its erasure (or rectification, see section above).

This does not apply to the extent that processing of the personal data is necessary for certain reasons, including that the processing is necessary for the establishment, exercise or defence of legal claims. (**Note:** this is the exception most likely to apply in a General Practice setting.)

Doctors should bear in mind that they are subject to professional, ethical obligations in terms of record keeping and that it is a requirement of most professional indemnity insurance cover. It will rarely be appropriate to erase a clinical record.

Medisec strongly advises any Member who receives a Data Protection access request regarding rectification, erasure, the restriction of / objection to data processing and / or data portability to contact us without delay for case specific advice.

October 2022