Data Subject Rights
(GDPR)

MDDUS
UK INDEMNITY, ADVICE & SUPPORT

Background

The GDPR, or General Data Protection Regulation, is a new piece of European legislation which replaced the Data Protection Act (DPA) 1998 on 25 May 2018. A new Data Protection Act 2018 also came into force at the same time. The purpose of the new DPA 2018 is to apply the GDPR in the UK.

The underlying data protection principles have not changed significantly from those of the DPA – but there is the new principle of 'accountability' (see below). The GDPR also requires organisations to adopt the philosophy of 'Data Protection by Design and Default'. This means that the organisation must be able to demonstrate compliance with the data protection principles. The principles are the backbone of the regulation.

Processing principles

The GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')
- collected for specified, explicit and legitimate purposes ('purpose limitation')
- adequate, relevant and limited to what is necessary ('data minimisation')
- accurate and up-to-date ('accuracy')
- kept in a form which permits identification for no longer than is necessary/archiving ('storage limitation')
- processed with appropriate technical and organisational measures to ensure security of personal data ('integrity and confidentiality').

The GDPR also requires that the data controller must be *responsible for and able to demonstrate compliance with* the principles ('accountability'). This means having the right procedures and processes in place from the point of data collection, so that there is clarity as to the legal basis for data processing at every stage of the life cycle of the data. Organisations have to be able to detect, report and investigate a personal data breach. Reputation management should be considered as part of the process.

Subject access requests (SARs) under GDPR

The new legislation will bring with it enhanced data subject rights. One of these is subject access, which already existed under the DPA 1998 but with different rules. This is where an individual (*usually* a patient or staff member but it can be anyone whose personal data your practice has collected) has the right to access the personal data that you hold about them. It also allows individuals to be aware of and verify the lawfulness of the processing.

Your procedures for handling these requests should be updated to take account of the new rules:

- You must **comply with the request within one month** of receipt.
- You will **no longer be able to charge a fee** for complying with the request. However, if the request is manifestly unfounded or excessive, particularly if it is repetitive, you may charge a 'reasonable fee'. This fee must be based on the administrative costs of providing the information.
- If you **refuse** to respond to a request you must tell the individual why without undue delay and advise them that they can complain to the ICO within one month.

You may need to consider whether further resourcing is required to deal with SARs under the new legislation. The shorter timescale may put pressure on those responsible for complying with requests and could impact on their other work.

Summary of how to process a subject access request

- A SAR can be made in a variety of "means" including orally, in writing and by electronic means.
- There must be enough information in the request to identify the patient and locate the information they have requested.
- You have one month from the day after receiving the request to comply with it. The ICO suggest that oral requests should be confirmed in writing.
- In most cases you will not be able to charge a fee for complying with the request and providing the information. This includes not being able to charge for postage.

- There should be a reasonable length of time between duplicate requests.
- You will be required to redact any information that would identify third parties, or anything that would cause significant harm to the individual's physical or mental health.
- The information supplied should be in a format that is legible and intelligible. Medical terms and abbreviations should be explained.
- If handwritten notes are difficult to decipher they may need to be dictated and retyped dependant on proportionality of effort, or a doctor/dentist/manager may have to sit with the individual to go through them. It is an offence to delete data to avoid complying with a subject access request.
- It should be in a form that is acceptable to the patient/staff member (e.g. on a CD or flash drive, in paper form, as an audio recording or even verbally if appropriate).
- If the request is from a young person, check competency.

If the request comes from a solicitor or insurance company acting on behalf of a patient:

- Ensure that there is valid consent – the mandate should be signed by the patient. No information can be disclosed that was entered into the notes after the date that the consent mandate was signed.
- Does the patient realise exactly what they have consented to (e.g. the full set of casenotes rather than just from a specific date)? Contact the patient, or their guardian/legal proxy, to clarify.
- You are not allowed to charge for the copies or for postage if the request comes from a 3rd party.
- If the SAR is for insurance purposes outright, the ICO and the BMA have issued guidance here. It can also be found on the BMA website under 'Focus on Subject Access Requests for insurance purposes.

If the request is from a parent or guardian wanting to access the case notes of a child:

- Recognising that a child may have competency and, therefore, should be consulted, any person with parental responsibility may apply for access to the records. It is important to remember that a mother always has parental responsibility for her child (unless it has been removed by the courts) but not all fathers do. In relation to children born after December 1, 2003 (England and Wales), April 15, 2002 (Northern Ireland) and May 4, 2006 (Scotland), both biological parents have parental responsibility if they are registered on a child's birth certificate.
- For children born before these dates, the biological father will only automatically acquire parental responsibility if the parents were married at the time of the child's birth or at some time thereafter. If the parents have never been married, only the mother automatically has parental responsibility, but the father may acquire that status by order or agreement.
- GMC guidance on access to medical records clearly states that: "divorce or separation does not affect parental responsibility and you should allow both parents reasonable access to their children's health records".

Other data subject rights

Your practice will have to understand and be in a position to respond to the following rights which apply to all data subjects:

- The right to be informed
- The right of subject access
- The right to rectification
- The right to erase
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

If in doubt contact either the Information Commissioner's Office on 0303 123 1113/Option 4 or call MDDUS on 0333 043 4444 for advice.