GDPR – subject access requests

The GDPR, or General Data Protection Regulation, is a 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 on the same day. The purpose of the new DPA 2018 is to apply the GDPR in the UK.

The new legislation has brought 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.

Basic considerations

Your procedures for handling subject access requests (SARs) 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.

Processing a subject access request

- A SAR can be made in a variety of ways including verbally, in writing and by electronic means.
- There must be enough information in the request to identify the data subject and locate the information they have requested.
- You have one month from the day after receiving the request to comply with it. The ICO suggests that oral requests should be confirmed in writing.
- You will not normally 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 serious harm to any 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 dependent 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 SAR. It should be in a form that is acceptable to the person making the request (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 if they have capacity to make an SAR. If not, the request may need to come from an individual with parental responsibility.

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

- Ensure that there is valid consent – the form should be signed by the patient. No information can be disclosed that was entered into the notes after the date that the consent form was signed.
- Does the patient realise exactly what they have consented to (e.g. the full set of case notes rather than just from a specific date)? Consider contacting the patient, or their guardian/legal proxy, to clarify.
- You are not allowed to charge for the copies or for postage even if the request comes from a third 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 seeking access to the case notes of a child:

- Recognise that a child may have capacity to decide whether disclosure can be undertaken and, therefore, this should be assessed.
- Check that the parent or guardian has parental responsibility.
- Consider what is in the child's best interests to disclose.
- Redact third-party or seriously harmful information.

Other data subject rights

Your organisation 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 non-factual information
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Common Pitfalls

- Many complaints arise because organisations do not comply with the timeframe for responding to SARs.
- GDPR and the Data Protection Act 2018 only apply to living individuals. If a request for access to case notes is received for a deceased patient then the Access to Health Records Act 1990 applies. This has different rules. Contact MDDUS on 0333 043 4444 for more specific advice or see our separate advice sheet on this subject, Access to deceased records.

Key points

- Ensure the practice procedure for subject access requests is compliant with the requirements of the GDPR.
- Ensure that all relevant staff are trained and aware of the rules around subject access requests under the GDPR..

Further guidance

- ICO. *Right of access*: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/
- GDPR toolkit

MDDUS Training & CPD resources: https://www.mddus.com/training-and-cpd/training-for-members