Patient Requests for Records- Following Implementation of GDPR

Subject Access Requests- Following Implementation of GDPR (from 25 May 2018)

On 25 May 2018 the current UK Data Protection Act 1998 (DPA 1998) will be fully replaced by the General Data Protection Regulation (2016/679)

As with the DPA 1998, these new regulations give living individuals the right to request access to personal data held on them by the Trust. This is known as a Subject Access Request (SAR), the person who will hold data about is known as the Data Subject, in many cases this will be the patient, but could be a staff member, a contractor or contact.

Requests must be in writing, this includes, letter, e-mail. There is also an electronic form for requesters to complete if they prefer. SARs can also be submitted via social media, such as our Facebook page or Twitter.

Requesters must be either, the data subject OR have the written permission of the data subject OR have legal responsibility for managing the subject's affairs in order to access personal information about that person. It is the requester's responsibility to satisfy the Trust of their legal authority to act on behalf of the data subject.

We also have to be satisfied of the identity of the requester before we can provide any personal information.

New Requirements for Subject Access

From 25 May 2018 some new requirements were introduced affecting the handling of subject access requests.

These are listed below:

What do we need to provide to a requester?

As well as providing confirmation that their personal is being processed and providing a copy of this personal data that the data subject has asked for; (subject to any exemptions). Individuals will have the right to be provided with additional information which largely corresponds to the information to be provided in a privacy notice:

- Source of the data.
- Recipient, including details international transfers.
- Retention period for the data.
- How to amend inaccurate data.
- How to complain to the Information Commissioner's Office (internal review will usually need to be satisfied first).

Timeframe for responding to requests

The ***Statutory*** timeframe has now been reduced to at least one month of receipt of the request, and in any event ***without delay.***

The period of compliance can be extended by a further two months where requests are determined to be 'complex' or 'numerous'.

The fee of £10 in the previous DPA 1998 has now been removed.

It was the case that £10 could be charged, but GDPR ***does not*** allow for a fee, so it must be provided free of charge. However, some charges can be made in the following circumstances:

- where further copies are requested by the data subject,
- or the request is manifestly unfounded, or excessive (definitions still required by the ICO) a reasonable fee based on the organisations administration costs may be charged.

When can a subject access request be refused?

Organisations can decide to refuse a request where the request is 'manifestly unfounded or excessive', in particular if it is 'repetitive', and the requester must be informed of the reason why, within one month of the receipt of the request.

What format should the response be provided in?

Where a request is received by electronic means, unless otherwise stated by the data subject, the information must be provided in a commonly used electronic format.

What are the penalties for non-compliance with the statutory timeframe?

The penalties are still at the discretion of the ICO. However, for non-compliance the financial penalties are now much greater. Depending on the severity of the infringement, this could be up to £17m approximately.

A new criminal offence has been created

If you receive a Subject Access Request, and records are altered with intent to prevent disclosure, this will be committing a criminal offence, and will be punishable by a fine.

What should you do if you identify that you have received a SAR?

Incoming SARs should be passed on immediately to the Access to Health Records Team, where they will be logged, acknowledged, and processed.