HUMBERSIDE LMCs

The professional voice of general practice

Subject Access Requests from Solicitors and Insurance Companies under the GDPR

Department Title

Subject Access Requests

What is a SAR?

A SAR or Subject Access Request is a request by an individual, or by a third party authorised by them, for access to information under the GDPR. Patients are entitled to make a SAR to access data held about them, including their medical records.

Who can make a SAR on behalf of a patient?

The GDPR allows a patient to make a SAR via a third party. This could be a solicitor or other representative acting on behalf of a patient, but it could also be a friend, family member or anyone the patient authorises to make a SAR for them.

The identity of the requester should be verified. A requester claiming they are a solicitor should not be taken at face value. They should provide their Solicitors Regulation Authority Registration Number and we would expect any request to come on the letterhead of the organisation.

What is the difference between SARs under the GDPR and requests using AMRA?

The purpose of a SAR is for an individual to have access to data held about them, for example their medical records. If a request is made for a copy of a patient's medical record, or some elements of the medical record, it is a SAR. Data controllers have a duty to respond to SARs by providing access to the information requested free of charge.

If a request is asking for a GP report to be written or for an interpretation of information within a patient's medical record, this goes beyond a SAR and should be dealt with under the Access to Medical Reports Act (AMRA). Practices are entitled to charge a fee for requests which fall under AMRA.

If in doubt, practices should clarify what information is being requested before responding.

Insurance Companies seeking medical information for life assurance purposes **should** be using the provisions of the Access to Medical Reports Act 1988 to seek a GP report. They should not be requesting a SAR which gives then access to the entire medical record, including information that is not relevant for the purpose of underwriting a policy. In July 2015, the ICO made a clear statement in this regard and wrote to the insurance industry explaining that they consider the use of SARs in this way to be inappropriate. In reality, however, the LMC is aware that some companies are using a SAR instead of a report under AMRA. In these circumstances, practices are placed in a difficult position as the practice places itself at risk if it fails to respond to the SAR.

The advice given on the ICO website is that:
"GPs have ethnical obligations around how patient records are shared, and we advise GPs to explain to patients, in broad terms, the implications of making a subject access request so that can make a more informed decision on whether they wish to exercise their rights under the Data Protection Act. We also recommend GPs share any responses to subject access requests directly with patients, rather than to insurance companies…… GPs must still respond to subject access requests…… The right to see personal information held about you by an organisation is an important one, and one from which GPs are not exempt."

Can a SAR be refused?

As a general rule, SARs must be complied with and cannot be refused. If a request is 'manifestly unfounded or excessive', access can be refused (or a fee can be charged) but there is little guidance as to what would constitute this. Whilst it may be open to the data controller to decline or to make a charge in relation to a SAR, doing so may prompt a complaint from the data subject (or threats of escalation from a solicitor making a request on behalf of a client). It may therefore prove expedient for the GP to comply with the request rather than risk the complaint or escalation. Practices will need to weigh up the risks accordingly.

Factors to consider when assessing whether a data subject's request can be declined for being 'manifestly unfounded or excessive, in particular because of their repetitive character' include:

- Whether the SAR is repetitive in nature (i.e. requesting information already provided);
- The frequency at which a data subject makes multiple SARs;
- The volume of the data requested, particularly if the request is repeated; and
- The administrative time that may be required in order to comply with the data subject's SAR(s).

There are a number of exemptions where information can be treated as exempt from disclosure, for example where it is likely to cause serious physical or mental harm to the patient or another person, or the information is restricted by the courts. For further details see the BMA's Access to Health Records (PDF).

Can solicitors and other representatives obtain full medical records under SARs?

Yes. A SAR from a solicitor or other representative acting for the patient should be treated as a SAR from the patient themselves. As long as the patient has given written consent to the solicitor or representative, practices should comply with the request.

What if a solicitor makes a SAR in relation to a legal claim?

The purpose of the SAR should not affect whether a practice complies with it. SARs are 'purpose blind' and there is no requirement under the GDPR for a patient or their solicitor or representative to indicate the purpose of the SAR.

Do we have to provide the full medical record in response to a SAR?

If the patients requires the whole medical record, you must provide it. However, Recital 63 of the GDPR does enable you to seek clarification regarding exactly what is required:

"where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates."

Therefore in certain circumstances, for example, where there is an extensive medical record which runs into many hundreds of pages, it may be appropriate to open up a discussion with the patient to check that they do want the whole record rather than just a specific section of it.

Can insurance companies use a SAR to ask for a medical report?

No, this goes beyond the scope of a SAR. Requests for medical reports (rather than a straightforward copy of the medical record) should be dealt with under AMRA.

Can we charge solicitors a fee for SARs?

Responses to SARs, whether they are made by the patient themselves or their solicitor or other representative, almost always have to be provided free of charge.

Only if a SAR is considered to be 'manifestly unfounded or excessive' can a reasonable fee be charged. It's not yet clear when the ICO might consider it appropriate to charge a fee on these grounds, but it's likely that such situations will be extremely limited.

Practices can charge a fee if a request is are made for further copies after the initial SAR. The fee should be based on the administrative costs of providing further copies.

Can we charge for postage under SARs?

No, the process of responding to a SAR – including postage costs – has to be free of charge.

Can we insist that solicitors come to collect copies of the records to save on postage?

You cannot insist on this, although it may be an appropriate option for providing access to the records if it's acceptable to both the practice and the solicitor.

Practices should have a clearly stated policy regarding how requests will be dealt with which is consistently applied.

Do we have to provide photocopies of records or can they be sent electronically?

It would be difficult for a practice to decline to provide paper copies of records in all circumstances. For example, if a patient stated that they had no means of accessing an email or other digital format. However, practices may have a 'preferred' approach which may be to send records via email. Medical records sent by email should be properly encrypted using the NHS mail service which enables information to be emailed securely to any non-NHS email address. Full details of how to utilise this are provided in the encryption guide for NHSmail (PDF).

If an individual makes a request electronically, you should provide the information in a commonly used electronic format, unless the individual requests otherwise.

How does Patient Online fit into the picture?

The GDPR includes a best practice recommendation that, where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information (Recital 63).

The practice could therefore offer a requester to be enabled to securely access their full GP electronic record online. This may provide them with sufficient information to meet their needs. This option may not be appropriate for all practices or in all circumstances.

Further reading

BMA GDPR guidance and resources page

Access to Health Records, BMA, May 2018

Information Commissioner's Office guidance on rights of access

LMC September 2018

HUMBERSIDE LMCs

The professional voice of general practice

The Humberside Group of Local Medical Committees Ltd

Albion House
Albion Lane
Willerby
Hull
HU10 6TS

01482 655111
humberside.lmcgroup@nhs.net
www.humbersidelmc.org.uk

@HumbersideLMC. Follow us for news and updates.