Subject Access Request Policy

Version:	1.1
Author:	Data Team
Name/Title of responsible individual:	Management
Date issued:	26.04.18
Review date:	26.02.20

Subject Access Requests

What is subject access?

Patients have the right to request and receive a copy of the information that is held about them. This is known as a subject access request. This right of subject access means that patients can make a request under the Data Protection Act and GDPR to any organisation processing their personal data. The Act calls these organisations 'data controllers'. Patients can ask the organisation that is holding, using or sharing the personal information, to supply them with copies of both paper and computer records and related information held about them. This is a 'subject access request' (SAR).

What happens when the Practice receives a request:

SARs can be written, either letter or email and also be made verbally. Whether a request is written or verbal the Practice will need to check that the requestor is the person they say they are, appropriate security questions will be asked to ensure this.

The Practice will provide the patient a response within **1 calendar month (or 28 days).** The Practice can ask the patient for more specific information about what they would like, this is to narrow down what data is required to satisfy their request. The Practice will clearly document this within the patient record; as if the patient asks for subsequent information about the same subject then this could become chargeable.

All requests are to be authorised by a GP – if it is likely to cause the patient serious harm when providing the information, the request may be declined.

Giving the patient the information they have asked for:

A SAR applies to all the information the Practice holds about the patient, electronic and paper – this includes Lloyd George envelopes. If the Practice receives a SAR verbally then we will ask the patient what information they require, if any date ranges apply and how they would like to access the information. A task will be sent to the secretaries advising them of the request. If the Practice receives a letter or email request this this request will be scanned onto the patient record and assigned to the secretaries.

Secretarial team duties:

If the patient has access to online services then the secretarial team will send a task to the Data Co-ordinator who will enable full clinical record access for the patient once the record has been reviewed by a GP. The Practice will then write back to the patient and advise them they can review their information online.

If the patient requires a written response, then our usual processes apply to ensure the Practice is not sharing 3rd party information inappropriately, once this has been reviewed we will then provide the relevant print outs.

Responding to SARs – the options

1. The Practice can agree. If the Practice agrees to a SAR, the Practice must respond within **one month** and include all the data held on the data subject plus whichever of the information requested that applies. Providing all the data the Practice holds is regarded as the norm.

2. The Practice can decline. The Practice can decline to provide a SAR, or as the GDPR states, 'not take action'. However the Practice will have to justify why within the universal **one-month** deadline and explain how the data subject can complain against the Practice decision. One obvious reason for declining is if the data has not changed since a previous request.

3. The Practice can request more time. The Practice can inform a patient that extra time is required, where it has been decided that it will take longer than a month to collate and supply the data. In this case the Practice must tell them this within the usual **one-month** deadline and the Practice will then have up to an additional two months to provide the information.

4. The Practice can negotiate. A SAR was defined under the Data Protection Act as the entire contents of the patient record and under GDPR that is the same basic default assumption, but it has now been recognised that over 20 years on the Practice hold masses of data on registered patients, so a new option has been introduced: the Practice can supply less than the entire record by mutual agreement.

This means the Practice can agree with the patient (within the **one-month** period) to narrow down the data required to satisfy their request, provided they agree voluntarily and freely. The Practice must not coerce people into asking for less than they want or need. In these circumstances clearly document what is agreed within a first SAR – e.g., only the records of a hip operation. Subsequent SARs could then be chargeable, although the Practice should take a reasonable approach. If the patient asks for one additional letter it would be unreasonable to charge a fee, but if they ask for hundreds more pages, then a charge would be reasonable.

When could the Practice negotiate?

The Practice may feel a negotiated SAR is going to be more difficult and time consuming than just handing over the lot, but remember GDPR applies to all data formats – including the paper in Lloyd George envelopes. So, a sensible negotiated SAR might be everything stored regarding the patient in electronic form.

In most circumstances the patient is unlikely to want copies of the irrelevant historical paper records. Another option is to take everything from a certain date. It is the

Practice's responsibility to protect any other data subjects mentioned in the requestors records, so the practice must redact any information on non-medical third parties.

What if the request is about a child?

Even if a child is too young to understand about a SAR their personal data does not belong to anyone else.

Before responding the Practice will consider whether the child is mature enough to understand their rights. If the Practice is confident that the child can understand then the Practice must respond to the child rather than a parent or guardian. The Practice should consider:-

- The child's level of maturity and ability to make decisions
- Nature of the personal data
- Any court orders
- Duty of confidence owed to the child
- The consequences of providing a parent or guardian with this information
- The detriment if an SAR is not provided
- Views of the child for disclosing information to a parent or guardian

Can a SAR be made on behalf of others?

If the Practice is satisfied that the third party making a request is entitled to act on behalf of the individual then yes. Evidence for proof of entitlement might be a written authority to make the request or it could be a more general power of attorney.

A 3rd party including legal representatives can ask for a patient record on behalf of the patient and the Practice cannot charge for this, however the Practice must ensure that appropriate consent is in place before releasing the information.

PLEASE NOTE:

- Solicitors are not permitted to seek a SAR to support an application that should be made under the Access to Medical Reports Act (AMRA), i.e., reports for employment and insurance purposes. This covers accident claims and insured negligence as well as mortgages and life insurance – anything covered by an insurance contract that requires a medical report. If a solicitor's letter does not make the precise purpose of the request and report clear, then ask them if the report is being requested under GDPR or AMRA. If the report is to support an actual or potential insured claim then AMRA applies. The Practice can charge and no additional information is needed.
- The same applies to employers – so if the report is in connection with proposed or actual employment, it's not classed as a SAR, meaning the Practice can charge and no additional information is needed.

What if insurers get patients to make SARs?

Clause 181 of the Data Protection Bill (due to be enacted later this year) will extend the offence of 'enforced subject access' to cover medical records, so this will become a criminal offence. Insurers will not want to be found guilty of the crime of enforced subject access. If The Practice suspects that an insurer is doing this, they should report them to the Information Commissioner's Office and the Association of British Insurers. Guidance on this from the ABI and the BMA is unchanged under GDPR.

How much is the fee?

In the past the Practice has been able to charge patients for SARs, the Practice has asked for:

- £10.00 for print out of the electronic record and dealing with the request
- Up to £50.00 for combination of manual and electronic record

The Practice is no longer allowed to charge for a SAR under the GDPR. The Practice charges for Non NHS services document has been updated and is available on our webpages.

For a repeat request the Practice can only charge a fee to cover administrative costs. So, the fee might involve the cost of professional time to redact records, for example. If the Practice invokes the unfounded or excessive clause the Practice will justify any reasons to the patient.

What information is an individual entitled to?

Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them. However, subject access goes further than this and an individual is entitled to be:

- Told whether any personal data is being processed (including where there is no information held)
- Given a description of the personal data, the reasons it is being processed and whether it will be given to any other organisations or people
- Given a copy of the personal data
- Given details of the source of the data (where available)

What happens if the requestor dies before a response is provided?

If the requestor dies after a SAR is received then the response must be provided to the individual's personal representative. As a matter of good customer service the Practice must check with the personal representative(s) that they still want to receive the information before anything is sent to them.

What if the information has someone else's information within it?

The Practice does not have to comply with a SAR if doing so would disclose information about another individual who is identifiable unless:-

- The individual has consented to the disclosure
- It would be reasonable in all circumstances to comply with a request without consent

Remember:-

Step 1 – Does the request require the disclosure of information that identifies a third party?

Step 2 – Has the third-party individual consented?

Step 3 – Would it be reasonable in all the circumstances to disclose without consent?

What additional data must the Practice supply?

The additional information that must be supplied, along with the original personal data concerning the patient (data subject), comprises an explanation of:

- The purpose(s) of the processing
- The categories of personal data being processed
- The recipients or categories of recipients
- How long the patient's information will be held
- The rights of rectification, restriction, objection and where applicable erasure
- The right to complain to the Information Commissioner's Office
- The patient's right to be told more about the source of their data received from other organisations.
- The existence of and logic behind and consequences of any automated processing.

This information, or an easily accessible link to it, has to be provided as well as the actual data relating to the patient.

Is any information exempt from subject access?

Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR. Information may be exempt because of its nature or because of the effect its disclosure is likely to have.

Beyond the 'excessive or unfounded' clause the Practice can also refuse to provide data where the patient already has the information. Other relevant exceptions include where:

- It would involve a disproportionate effort (eg, letters from the 1960s that are no longer relevant)
- It would disclose comments about a third party to the patient (except for others involved in their care)
- It could result in harm to the patient or anyone else
- The information is subject to a court order or is privileged, or subject to fertilisation or adoption legislation.

Exemptions and restrictions – general

The Data Protection Act 1998 (DPA), furthered by the General Data Protection Regulations (GDPR), recognises that in some circumstances the Practice might have a legitimate reason for not complying with a subject access request (SAR), so it provides a number of exemptions from the duty to do so. Where an exemption applies to the facts of a particular request, the Practice may refuse to provide all or some of the information requested, depending on the circumstances. It is a matter for the Practice to decide whether or not to use an exemption – the DPA/GDPR does not oblige the Practice to do so, so the Practice is free to comply with a SAR even if the Practice could use an exemption.

If challenged, the Practice will be prepared to defend to the Information Commissioner's Office or a court the Practice decision to apply an exemption. It is therefore good practice to ensure that such a decision is taken at a suitably senior level in within the organisation and that the Practice document the reasons for it.

Exemptions

Confidential references

From time to time the Practice may give or receive references about an individual, e.g. in connection with their employment, or for educational purposes. Such references are often given 'in confidence', but that fact alone does not mean the personal data included in the reference is exempt from subject access.

The DPA/GDPR distinguishes between references the Practice provides and references the Practice receives.

References the Practice provide are exempt from subject access if the Practice provide them in confidence and for the purposes of an individual's education, training or employment or the provision of a service by them.

There is no such exemption for references the Practice receives from a third party. If the Practice receives a SAR relating to such a reference, the Practice must apply the usual principles about subject access to decide whether to provide some or all of the information contained in the reference.

Relevant considerations are likely to include:

- any clearly stated assurance of confidentiality given to the referee;
- any reasons the referee gives for withholding consent;
- the likely impact of the reference on the requester;
- the requester's interest in being able to satisfy himself or herself that the reference is truthful and accurate; and
- any risk that disclosure may pose to the referee.

Publicly available information

If an enactment requires an organisation to make information available to the public, any personal data included in it is exempt from the right of subject access.

The exemption only applies to the information that the organisation is required to publish. If it holds additional personal data about an individual, the additional data is not exempt from the exemption to justify denying subject access to whole categories of personal data if for some individuals the crime and taxation purposes are unlikely to be prejudiced.

Personal data that:

- is processed for the purpose of discharging statutory functions; and
- consists of information obtained for this purpose from someone who held it for any of the crime and taxation purposes described above is also exempt from the right of subject access to the extent that providing subject access to the personal data would be likely to prejudice any of the crime and taxation purposes. This prevents the right applying to personal data that is passed to statutory review bodies by law-enforcement agencies, and ensures that the exemption is not lost when the information is disclosed during a review.

Management information

A further exemption applies to personal data that is processed for management forecasting or management planning. Such data is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice the business or other activity of the organisation.

Negotiations with the requester

Personal data that consists of a record of your intentions in negotiations with an individual is exempt from the right of subject access to the extent that complying with a SAR would be likely to prejudice the negotiations.

Social work records

Special rules apply where providing subject access to information about social services and related activities would be likely to prejudice the carrying out of social work by causing serious harm to the physical or mental health or condition of the

requester or any other person. These rules are set out in the Data Protection (Subject Access Modification) (Social Work) Order 2000 (SI 2000/415). Their effect is to exempt personal data processed for these purposes from subject access to the extent that its disclosure would be likely to cause such harm.

A further exemption from subject access to social work records applies when a SAR is made by a third party who has a right to make the request on behalf of the individual, such as the parent of a child or someone appointed to manage the affairs of an individual who lacks capacity. In these circumstances, personal data is exempt from subject access if the individual has made clear they do not want it disclosed to that third party.

Other exemptions

The DPA/GDPR contains additional exemptions that may be relevant when dealing with a SAR. For more information about exemptions, see the ICO Guide to Data Protection.

An organisation that makes appropriate use of the exemptions in the DPA/GDPR might have the following indicators of good practice:

- **Withholding or redacting information**

If information is withheld in reliance on an exemption, the response explains, to the extent it can do so, the fact that information has been withheld and the reasons why. The explanation is given in plain English, and does more than simply specify that a particular exemption applies.

Information to be redacted is approved before source material is copied in a redacted form. It is then subject to at least one quality review by a manager to confirm that all data has been excluded appropriately. A copy of the disclosure bundle showing the redactions and the reasons behind them is retained for reference.

Once approved, redaction is either carried out manually using black marker which is then photocopied, or electronically using Adobe Acrobat or bespoke redaction software.

- **Ensuring consistency**

Advice on applying the exemptions most likely to be relevant to the organisation’s activities is included in SAR guidance for staff. Quality assessments are carried out to ensure that exemptions are applied consistently.