|  |  |
| --- | --- |
| **Author:** Sian Owen | **Subject Access Request Policy** |
| **Date issued:**  | 12/02/2019  |
| **Review date:**  | 12/01/2019  |

**Introduction**

This policy provides the Practice with a process for the management of requests for personal information (for living individuals) under the Data Protection Act (DPA), the General Data Protection Regulations (GDPR) and (for deceased individuals) the Access to Health Records Act 1990.

It defines a process for achieving legislative requirements and ensuring effective and consistent management of such requests.

The policy ensures that all staff are aware of how a subject access request should be made and to respond quickly.

Under the Data Protection Act, subject to certain conditions, an individual is entitled to be:

* Told whether any personal data is being processed;
* 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; and
* Given a copy of the information comprising the data; and given details of the source of the data (where this is available).

The Data Protection Act extends equally to all relevant records relating to living individuals, including records held in the private health sector and health professionals’ private practice records.

**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 are to be requested using the SARs request form. Once received 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 (name, DOB, address).

The practice will then contact the patient to discuss options for them receiving their information as if they are not classed as vulnerable they can have access to their full medical record online for 1 calendar month. If they refuse this and want a paper copy the Practice will ask if this is for personal or insurance purposes and can narrow down dates or ailments if for insurance. 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. When the Practice receives a SARs request we will ask the patient what information they require, if any date ranges apply and how they would like to access the information. If the Practice receives a letter or email request this will be put in date order in the appropriate folder and receipt of the request is to be documented on to the patient’s records. It is everyone’s responsibility to ensure that the SARs is completed.

**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. If the request is regarding an incident or ongoing health condition and the request is for a full medical record a SARs letter is to be sent to the solicitors advising them that it is seen as excessive and we can provide a Medical Report or they can send an updated request for specific dates or conditions.
4. If the request is for an insurance company a SARs letter will be sent to the company informing them that they are not ask for a SARs and either the patient must or they are to write asking specific questions in the form of a report from a Clinical Professional.
5. If a request is received from an Insurance company that is classed as excessive we are to write to the patient informing what has been request and whether they were aware and consent to this and informing it is found to be excessive. We also write to the Insurance Company informing them the same and if they can narrow down their request this will allow us to complete in a timely manner.
6. 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.
7. 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.

1. When the patient records are collected, if the solicitor comes to collect the information they are to bring confirmation of who they are along with a letter with patient details and reference number. If the patient comes to collect their own records they would need to provide photo ID. Before information if given to a friend or family member signed consent would need to be provided.

**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?**

Information relating to children belongs to the child even if they are too young to understand the implications of SAR and make decisions about their information and how it is handled. Just because they are either too young or do not have the mental capacity to make decisions about their information the information still belongs to them not any other individual such as a parent or guardian, however in these cases the child’s rights are usually exercised by an individual with parental responsibility.

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**:

* Insurance companies 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.

**How much is the fee?**

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

* £50.00 for full medical record

The Practice is no longer allowed to charge for a SAR under the GDPR.

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.

**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 (e.g., 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.

**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.

**SARS Checklist**

* If a SARs comes in from insurance company the standard letter (fig 1 below) will be sent informing them that a SARs must be made by the patient and the should be requesting a report. They can then send a report or the patient can ask for a SARs. This letter is also sent to the patient.
* If the report comes from a solicitor we write to both the patient (fig2) and the solicitor (fig 3) to inform of how much information has been requested and the necessity of this.
* If it cannot be negotiated inform it will have to be discussed with the Caldecott Guardian as it is an excessive request clause.
* Once details of the request are clarified we start the response to the request and complete the checklist along the way (fig4).
* We have 28 days to fulfil the request and redact any third party references (to be documented on the checklist.
* If we are unable to meet this- contact the solicitors/patient to inform more time is required. This must be done within the original 28 days. If this is done we are entitled to a further two months to complete the SARs. This is to be dated on the checklist
* Once the SAR is completed it is to be signed off by the Caldecott Guardian (Chris). To be documented on the checklist.
* Once it is signed we are to inform the patient of this and that they are to collect their paperwork where possible however if they do not agree to this we are to post them just explain that this is requested due to the sensitive information. To be documented on the checklist.
* Upon collection of notes we must see photo ID with a signature to be compared to the consent signature.

**FIG 1**



The Medical Centre

2 Frances Street

Doncaster

DN1 1JS

Tel: 01302 349431

**Subject Access Request**

**First Response to Insurance Companies**

<Today's date>

Private & Confidential

RE: <Patient Name>

<Patient Address>

<Date of Birth>

Dear

I am writing in relation to the request you made for the above named patient’s medical records.

The letter reads that you wish for the patient to consent to copies of **full** medical records be sent to you. We will be sending a copy of this letter to our patient to confirm this information, as in some cases it may be more appropriate for a medical report to be requested and a medical professional to provide their opinion on request. The below statement from the Financial Ombudsman is a public document that states;

Only relevant information should be provided and it is ethically unacceptable

To provide extraneous information. Doctors must not send originals, photocopies

or printouts of full medical records in lieu of medical reports […] The full records

not necessary and will very probably include information that is not relevant

to the insurance being applied for. (Financial Ombudsman)

 The disclosure of this information is likely to breach the Data Protection Act 1998.

We look forward to your reply.

Yours Faithfully

The Medical Centre

**FIG 2**

The Medical Centre

2 Frances Street

DONCASTER

DN1 1JS

Telephone: 01302 349431

<Today's date>

<Patient Name>

<Patient Address>

Dear <Patient Name>

I am writing to you as your insurance company has requested access to your **full** medical record. I understand that you have signed a form of consent; however, we need to be satisfied that you have provided specific and informed consent for your **full** medical records to be shared with the insurance company. Your records include sensitive information which you may not expect to be shared or may not need to be shared as part of your application for insurance or the assessment of any claim.

I also want to let you know that The British Medical Association has questioned whether the law allows insurance companies to use Subject Access Requests to obtain confidential and sensitive personal data. The Data Protection Act 1998 states that only data which is sufficient for the purpose for which it is required should be disclosed and sensitive personal data which is not relevant or excessive in relation to this purpose should not be disclosed.

The Information Commissioner’s Office has recently written to the insurance industry to confirm that they consider the use of Subject Access rights in this way is inappropriate and an abuse of that right.

As the guardian of your medical records we are responsible for ensuring only necessary and relevant information held is shared with an insurance company, however we also have a duty to comply with a Subject Access Request made by you as a patient and do not want to cause any delays to your application.

We can provide you with a copy of your full medical records under a Subject Access Request. This would not be considered as excessive as we are providing the information to you, not the insurance company. It is then entirely your decision whether you give your medical records to the insurance company in full or not.

Alternatively, you can ask your insurer to request a Medical Report from the practice which will only cover information in your record that is relevant to your application. Medical reports also exclude some information, in line with agreement reached with the insurance industry, such as genetic test results and certain information about sexually transmitted infections.

**Please therefore let us know if you would like a copy of your full medical records under a subject access request or whether you plan to ask your insurer to seek a medical report.**

The BMA has let the Association of British Insurers (ABI) and insurance companies know that we are offering patients this choice. If your insurance company expresses concern about this please ask them to contact the ABI.

Yours faithfully

The Medical Centre

**FIG3**



The Medical Centre

2 Frances Street

Doncaster

South Yorkshire

DN1 1JS

Tel: 01302 349431 Fax: 01302 247622

**Subject Access Request**

**Letter to Solicitor**

<Today's date>

Private and Confidential

RE: <Patient Name>

<Patient Address>

<Date of Birth>

I am writing in reply to your recent letter. Under GDPR guidelines we find the request to be excessive. It is documented in your letter that the information you require is in relation to an incident. If you require information on specific conditions, injuries or require medical records within specific time scales, please write to us with your revised Subject Access Request. Alternatively you may wish to request a report to be completed by a medical professional, to which a member of the clinical team would answer specific questions relevant to the incident. If you require a revised SAR or a medical report please seek a new consent form from the patient outlining the specific requests made.

With regards to the sending of medical records we request that, where possible, these are collected due to the sensitivity of the information within and due to unsecure emails we are also unable to send them via this route. We can make the records available to yourselves or the patient to collect in person where possible.

We look forward to your response.

Yours faithfully

The Medical Centre

**FIG 4**

Subject Access Request

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |
| --- | --- | --- |
| Patient Name: | NHS:  | DOB: |
| Date Request Received:  | Name of Company: | Patient consent: SAR? If patient requests: |
| Letter sent to patient? | Member of Staff:  | Date: |
| Letter sent for time extension ? (if needed) | Date: | Staff: |
| Target Date for completed records | Date: | Contact company for collection: |
| Redacted Info?Lloyd George & Computer Notes | Date Completed:Date Completed:  | Staff:  |
| Checked by Caldecott Guardian Agreed to send? | Date: | Signature:  |

 |

Notes :