Subject Access Request Policy

Version:	1.4
Author:	Data Team
Name/Title of responsible individual:	Management
Date issued:	Sept 2021
Review date:	March 2025
Review date:	March 2026

Introduction

This policy sets out the procedures for handling subject access requests (SARs) made by individuals in relation to their personal data held by the practice.

Purpose

The purpose of this policy is to ensure compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, and to ensure that individuals are aware of their rights in relation to their personal data.

Scope

This policy applies to all personal data held by the practice, whether in paper or electronic format.

Who can make an Access Request?

An application for access to personal data may be made to the Practice by any of the following:-

- an individual
- a person authorised by the individual in writing to make the application on an individual's behalf e.g. solicitor, family member, carer
- a person having parental responsibility for the individual where he/she is a child.
- a person appointed by a court to manage the affairs of an individual who is deemed incompetent
- individuals who hold a health and welfare Lasting Power of Attorney
- where the individual has died, the personal representative and any person who may have a claim arising out of the individual's death (the executor of the deceased's will; someone who has been appointed as an Administrator of the Estate by the Courts; someone who has the written consent of either of the above to be given access, someone who is in the process of challenging the deceased's will)

Police Requests

The Police may, on occasion, request access to personal data of individuals. Whilst there is an exemption in the Data Protection Act which permits the Practice to disclose information to support the prevention and detection of crime, the Police have no automatic right to access; however they can obtain a Court Order.

Solicitor Requests

A patient can authorise their solicitor or another third party to make a SAR. As long as the solicitor has provided the patient's written consent to authorise access to the records, the SAR process should be followed as usual.

Insurance Requests

Insurance companies however do not have the same privileges to access patient records – the ICO has said that insurance companies using SARs to obtain full medical records is an abuse of the process (the DPA 2018 still says that information must be adequate, relevant and not excessive in relation to the purpose the data is processed).

It is a criminal offence to make a SAR to access information about individuals' convictions and cautions – the law sets out various levels of fines, and a clause in the DPA 2018 will soon be enacted to extend this to cover medical records. If you suspect that a SAR from an insurer is not relevant or excessive then it should be reported to the ICO and the Association of British Insurers

Employers Requests

Any requests in connection with proposed or actual employment is not classed as a SAR, an ap[plication should be made under the Access to Medical Reports Act (AMRA).

Requests relating to children/young persons

Parental responsibility for a child is defined in the Children's Act 1989 as 'all the rights, duties, powers, responsibilities and authority, which by law a parent of a child has in relation to a child and his property'. Although not defined specifically, responsibilities would include safeguarding and promoting a child's health, development and welfare, including if relevant their employment records. Included in the parental rights which would fulfil the parental responsibilities above are:

- having the child live with the person with responsibility, or having a say in where the child lives;
- if the child is not living with her/him, having a personal relationship and regular contact with the child;
- controlling, guiding and directing the child's upbringing.

Foster parents are not ordinarily awarded parental responsibility for a child. It is more likely that this responsibility rests with the child's social worker and appropriate evidence of identity should be sought in the usual way.

The law regards young people aged 16 or 17 to be adults for the purposes of consent to employment or treatment and the right to confidentiality. Therefore, if a 16 year old wishes HR or a medical practitioner to keep their information confidential then that wish must be respected.

In some certain cases, children under the age of 16 who have the capacity and understanding to take decisions about their own treatment are also entitled to decide whether personal information may be passed on and generally to have their confidence respected.

Where a child is considered capable of making decisions, e.g. about his/her employment or medical treatment, the consent of the child must be sought before a person with parental responsibility may be given access. Where, in the view of the appropriate professional, the child is not capable of understanding the nature of the application, the holder of the record is entitled to deny access if it is not felt to be in the patient's best interests.

The identity and consent of the applicant must always be established.

The applicant does not have to give a reason for applying for access however, 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 is a Data Controller and can only provide information held by the organisation. Data controllers in their own right must be applied to directly, the Practice will not transfer requests from one organisation to another.

Application

Individuals wishing to exercise their right of access should:

- Make a verbal or written application to the Practice holding the records,
- Provide such further information as the Practice may require to sufficiently identify the individual

Fees and Response Time

Under GDPR the Practice musts provide information free of charge. However, we can charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The fee must be based on the administrative cost of providing the information only.

The request should be initially passed to the secretarial team who will manage Subject Access Request.

Responding to SARs – the options

1. The Practice can agree. If the Practice agrees to a SAR, the Practice must respond within **28 days** 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 **28 day** 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 **28 day** 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 **28 day** 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.

If the request involves creating a medical report or interpreting the information in an existing medical record or report, then this would be a request under the **Access to Medical Reports Act (AMRA)**. Unlike a Subject Access Request, these requests will require new material to be created. **This would mean that a fee is payable in such circumstances.**

The Release Stage

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 unless they have provided consent or were present in the consultation.

If a record contains information that relates to a third party who has not given their consent for disclosure, it may be reasonable not to disclose that information if you believe the duty of confidentiality you owe to the third party outweighs the individuals right of access.

The format of the released information must comply with the requester's wishes. Where no specific format is requested, the Practice should provide the information in the same manner as the original request. For example, requests received via email can be satisfied via email.

During the collation and redaction process, any entries or communications which the secretary is unsure whether the information should be withheld, a task will be sent to the partners for clarification. Once the response is received the record should be sent to the requester. On no account must the original record be released.

In denying or restricting access, a reason for the decision does not need to be given but the applicant should be directed through the appropriate complaint channels.

Exemptions

Access may be denied or restricted where:

- The record contains information which relates to or identifies a third party that is not a care professional and has not consented to the disclosure. If possible, the individual should be provided with access to that part of the record which does not contain the third party information
- Access to all or part of the record will prejudice the carrying out of social work by reason of the fact that serious harm to the physical or mental well-being of the individual or any other person is likely. If possible the individual should be provided with access to that part of the record that does not post the risk of serious harm
- Access to all or part of the record will seriously harm the physical or mental well-being of the individual or any other person. If possible the individual should be provided with access to that part of the record that does not pose the risk of serious harm

There is no requirement to disclose to the applicant the fact that certain information may have been withheld.