

Subject Access Request

Redaction in General Practice and Disclosure of Information Requests

Table of Contents

[What is a Subject Access Request? 1](#_Toc17720561)

[How is a Subject Access Request made? 1](#_Toc17720562)

[Who can make a Subject Access Request? 1](#_Toc17720563)

[The request is made in person 1](#_Toc17720564)

[The request is made over the telephone 1](#_Toc17720565)

[The request is made in writing 1](#_Toc17720566)

[The request is made via a representative 2](#_Toc17720567)

[Preparing a Subject Access Request 2](#_Toc17720568)

[Redacting Prior to Release 2](#_Toc17720569)

[Third party identifiers 2](#_Toc17720570)

[Information provided by third parties 3](#_Toc17720571)

[Legal professional privilege 3](#_Toc17720572)

[‘Do not release without the consent of the author’ 3](#_Toc17720573)

[Multi-Agency Risk Assessment Conference (MARAC) forms 3](#_Toc17720574)

[Non-medical information 3](#_Toc17720575)

[Non-relevant information 3](#_Toc17720576)

[Storage of requests 4](#_Toc17720577)

[Introduction 4](#_Toc17720578)

[Subject Access Request (SAR) 4](#_Toc17720579)

[Access to Medical Reports Act (AMRA) 5](#_Toc17720580)

[Access to Health Records Act (AHRA) 5](#_Toc17720581)

[Freedom of Information Act (FOIA) 6](#_Toc17720582)

[Section 251 of the NHS Act 2006 (S251) 6](#_Toc17720583)

[Disclosure of Information to the Police (Schedule 2(1)(2)) 6](#_Toc17720584)

**Appendices**

[Appendix I: Police request information flowchart 1](#_Toc17720585)

Redaction in General Practice

# What is a Subject Access Request?

A subject access request (‘SAR’) is a request made by a natural living individual, also known as the ‘data subject’. The data subject can request a copy of their medical records from the practice (or other medical service provider) under a SAR. The information can include computerised records, letters, notes, recorded telephone conversations and emails.

The practice has one calendar month in which to comply with the request, although this can be extended to three months in the event the collection, collation and production of a SAR is complex. The practice must notify the data subject whether an extension is required to comply with their request for their medical records.

# How is a Subject Access Request made?

Requests can be made in writing, on an in-house form, on the practice’s social media site(s) or orally to any member of staff. Recognising a SAR and following the practice’s procedure is the responsibility of every member of staff, making practice-wide understanding of the process vital.

# Who can make a Subject Access Request?

Only the data subject, to whom the information pertains, can apply for a SAR; however, the data subject can employ or ask a third party to make the request on their behalf. The third party making the request is known as the ‘representative’. A representative can be either another person or an organisation, usually a solicitor. In each case, the practice must satisfy itself regarding the identity of the data subject and the authenticity of the consent provided to the representative to make the request on their behalf.

## The request is made in person

If the request is made in person, either verbally or via a hard copy of an in-house request form, staff must ask for sight of the data subject’s identification.

## The request is made over the telephone

If the request was made over the telephone, staff can ask some security questions (such as providing matching identifiers to those in the medical records); however, if staff wish for further clarification it would not be remiss to request the data subject to present to the practice with their identification.

## The request is made in writing

If the request is made in writing, including via social media, staff must satisfy themselves that it is the data subject making the request; again, this can be done either over the telephone (security questions) or request they present to the practice with proof of identify.

## The request is made via a representative

The data subject can make a request via a representative, either someone known to them or a legal representative such as a firm of solicitors. These SAR applications must be accompanied by the data subject’s consent which allows the representative to make the request on their behalf. It will be necessary to confirm with the data subject that they have consented for a representative the make a SAR application on their behalf.

# Preparing a Subject Access Request

Whilst any employee can receive a SAR, not every employee can prepare one. The task of collection and collation of the medical records prior to the production of a SAR will be the remit of staff identified by the practice to undertake the task.

On receipt of a SAR from the identity of the data subject or their representative, clarification of the request must be made. This task is undertaken because data subjects have little comprehension of the amount and type of personal and special category data held in their medical records.

It is common to receive a SAR requesting the data subject’s *full* medical records. This may happen because the data subject may be unaware of targeted SARs (TSAR). A targeted SAR provides the medical records within a specified timeframe, for example the last 5 years; or a specific condition, such as musculoskeletal conditions. Clarifying the request with the data subject can reduce the practice’s workload; however, the practice must not attempt to sway the data subject to apply for a targeted SAR if the data subject is clear they would like a copy of their full medical record.

Once satisfactory identification of the data subject (photographic identity, such as a driving licence or passport, or a proof of address and a bank card) and clarity of their request is established, the SAR can be produced.

# Redacting Prior to Release

The Information Commissioner’s Officer (‘ICO’) states that when determining whether it is reasonable to disclose information, the controller (the practice) must consider:

1. The type of information that is to be disclosed
2. Any duty of confidentiality owed to the other individual (third party)
3. Steps taken to seek consent from the other individual
4. Whether the individual can give consent
5. Any express refusal of consent by the other individual

## Third party identifiers

Third party identifiers (‘TPI’) include the names of parties other than the data subject and healthcare professionals; they also include the roles, such as wife, husband, brother, daughter, friend, neighbour, boss, etc. TPIs also include any information which may help to identify third parties, for example: Mrs Smith’s husband works as a butcher on High Street in the town. This sentence identifies the third party’s relationship to the data subject, as well as his occupation and location of employment. If the TPI ‘husband’ was removed, the remaining information would enable someone to identify the third party, and therefore must be redacted.

Although the removal of third party identifiers needs to be undertaken, there are other considerations to be mindful of when redacting.

## Information provided by third parties

Information provided by third parties is not information provided by the data subject; therefore, it must be redacted. For example: A mother is concerned about her son’s anti-social behavior which is exacerbated by his intake of excessive alcohol. She speaks to her son’s doctor about her concerns and her son’s issues. In this example, the consultation is a ‘third party consultation’ and must be redacted prior to releasing the medical records to the data subject.

## Legal professional privilege

If a SAR has been made for the purpose of gathering the medical records of a data subject contemplating litigation against the practice, legal professional privilege exemption can be used to restrict access to personal data contained within documents.

There are two types of legal professional privilege:

1. *Litigation privilege*: This relates to communication pertaining to contemplated litigation which is either a real prospect of there is a likelihood.
2. *Advice privilege*: This applies where no litigation is in progress or contemplated. It is communication where legal advice has been sought or given.

For example: Correspondence from the data subject’s legal representative requesting a copy of the medical records because the data subject is seeking to make a claim against the practice (litigation privilege).

## ‘Do not release without the consent of the author’

Some documents instruct non-disclosure without the author’s authorisation. These are applied to sensitive reports and can include medico-legal reports, psychiatric reports (especially if the patient has been sectioned) and community multi-disciplinary team reports. Compliance with the author’s instruction must be adhered to.

## Multi-Agency Risk Assessment Conference (MARAC) forms

MARAC forms are minutes of community multi-disciplinary team meetings and concern whole families, not a single data subject. Their contents must not be released to the data subject or their representatives.

## Non-medical information

Medical records also contain documents received from non-medical sources; these include solicitors, insurance companies, the Department of Work and Pensions and the Police. They do not make up part of the medical records and must be redacted.

## Non-relevant information

The data principle of data minimisation requires the information released to be limited for the purpose. If the practice is in doubt about the purpose of the request, contact the data subject. They are not obliged to inform you for the reason for the SAR application; however, most data subjects will divulge the purpose. It is increasingly common for legal representatives to request a copy of the data subject’s full medical records via the data subject themselves. A direct data subject SAR application would contain most of the contents of their medical records; however, a request direct from the data subject for use by their legal representative should focus on the information limited for purpose. If the purpose of the SAR application is in doubt provide the information to the data subject and inform them of their right to review their records and redact them as they see fit prior to them release them to their legal representative.

# Storage of requests

The Records Management Code of Practice for Health and Social Care 2016 states the following storage periods prior to destruction of a SAR application:

1. If a SAR application has been made for the purpose of litigation, the information must be retained for 10 years after the whole process has ceased, including the litigation. These requests must not be kept on file.
2. If a SAR application was not made for the purpose of litigation, the information must be retained for 3 years after the closure of the SAR.
3. If a SAR application was not made for the purpose of litigation but was there was a subsequent appeal, the information must be retained for 6 years after the closure of the appeal.

Disclosure of Information Requests

# Introduction

Most employees who are responsible for dealing with requests for medical information are familiar with the Subject Access Request (SAR) and the Access to Medical Reports Act (AMRA). These are the most common methods used to request the information; however, there are others which you must become familiar with to enable you to make the correct decision on what information to collate and how to release it. Below is a very brief outline of the different Acts used by patients, the patient’s representative and third parties to make a request.

# Subject Access Request (SAR)

A SAR can be made to the practice for disclosure of medical records by a *living* patient or their representative. This information includes both computerised and paper records. The information must focus on the patient and be subjected to redaction of third-party identifiers and any information that may cause harm or distress to the patient or another individual.

The release of the finalised records will be subject to practice policy. Some practices will only release information directly to the patient, while other practices will release the information to the patient’s representative at the patient’s request. Whatever the practice policy is, the records must be available within one calendar month from the date the request was received by the practice, except for complying with complex requests where an extension of a further two calendar months is permitted under the General Data Protection Regulation (GDPR).

# Access to Medical Reports Act (AMRA)

An AMRA is a request for a medical report made by a third party but is not the patient’s representative, for example an employer or an insurance company. These requests can only be processed if the practice is in receipt of the patient’s consent. Using the examples of the third parties (above) the reports are used to form part of the third parties’ risk assessment to determine if the patient is fit to undertake their role within their place of employment, or to determine the risk of insuring them.

The Act permits the patient to see the report before it is released. The practice must be informed of the patient’s intention to view the report. If the patient wishes to see the report, they have 21 days from the date of completion in which to do so. If they do not attend to view the report, it may be forwarded to the third party after the 21st day. The patient is also allowed to comment and make amendments/corrections to the report prior to its release; however, these can only be accepted by the GP if the GP agrees with them.

As the report is a creation of new information, the practice is entitled to charge for the work.

# Access to Health Records Act (AHRA)

An application for the medical records of a *deceased* patient must be made under AHRA. The records can be requested by:

* A personal representative (the executor or administrator of the deceased person’s estate); or
* Someone who has a claim resulting from the patient’s death (this could be a relative or someone else).

‘Next of kin’ is not a legal basis to request the medical records, nor justification to give them to someone. Requests made by the next of kin without any further reason for the request must be denied.

Only information directly relevant to a claim can be disclosed.

Once a deceased patient’s paper records have been returned to the Primary Care Support England (PCSE), the practice is no longer the data controller of the records; however, the practice retains the role of data holder of the electronic records.

If, whilst alive, the deceased patient asked for non-disclosure of their medical records, neither the practice nor the PCSE are permitted to release any information. Any request for non-disclosure must be marked on the patient’s clinical records.

# Freedom of Information Act (FOIA)

The NHS is a public authority and is obliged to publish certain information about its activities. Any member of the public can request information from publish authorities; however, what they cannot do is request access to their personal data, nor request information pertaining to other people or organisations, for example an employee’s private information.

The FOIA request must be clear about what information is required. The practice must reply within 20 working days, with any extension period not exceeding 40 days.

A fee can be made for an FOIA for disbursements.

# Section 251 of the NHS Act 2006 (S251)

S251 forms the legal basis for sharing patient identifiable information without the patient’s consent. Its application to a request for records is limited to a suite of programmes previously known as ‘confidential enquiries’. It allows the common law of duty to be temporarily lifted.

The safeguards for release include:

* The activity must be a medical purpose, ie medical research with ethics committee approval, and the management of health and social care services;
* The activity must be in the public interest or the interest of improving patient care;
* The activity must be compliant with the provisions of the Data Protection Act 2018; and
* All applications must undergo an annual review to evidence whether support is still necessary.

# Disclosure of Information to the Police (Schedule 2(1)(2))

Patient information can be shared with the Police if it upholds the patient’s right to confidentiality and allows the Police to have sufficient and appropriate information to help with their enquiries. Both the Police and the practice must be able to justify the release of information being in the public interest. The request from the Police must be on a DP2 form and either signed by an officer of the rank of Inspector or above, or authorised by someone with the rank of Inspector or above (the authorisation must accompany the form.

The reasons for the Police to request records are varied, as is whether consent is required or not. The pathways are shown in Appendix I.

# **g**Appendix I: Police request information flowchart

**What is the nature of the police request for information?**

Patient victim of crime

Missing person

For authorised break-in in emergency

RTA – basic demographic release

To prevent or detect crime or a serious arrestable offence\*

Access to clinical records – no consent

Life or death, emergency or terrorism

Must have a completed and signed DP2 form

Inform IG Lead

Get patient’s or relative’s consent

In- patient?

Ask for police switchboard number – ring them back on it

Release as justifiable and proportionate

Consent withheld

Consent given

No consent

YES

Release if in patient’s best interest

Inform police – relatives need not be told

Release basic demographics only

Record decision and disclosure in medical records

NO

**\* In an emergency situation, release only what is necessary, relevant and justifiable. Record actions undertaken in medical records**

Adapted by Howbeck Healthcare for General Practice: taken from Southern Health NHS Foundation Trust