

Subject Access Request Policy

Version History

Version	Date Issued	Details	Brief Summary of Change	Author
0.1	20 April 2018	Draft	New document	NCL IG Leads
0.2	27 April 2018	Draft	Amended following comments from Michael Fox – Camden CCG	NCL IG Leads
0.3	06 Feb 2019	Draft	DPO suggested revisions	Steve Durbin, Data Protection Officer
1.0	03 June 2020	Final	Updated for practices and Brexit	Steve Durbin, Data Protection Officer
1.1	16 Dec 2020	Updated	Updated for children guidance and removing comments	Steve Durbin, Data Protection Officer
1.2	23 June 2021	Updated	Improvements to ensure people are aware that no forms can be imposed and there is no written requirement	Steve Durbin, Data Protection Officer
1.3	03 Sept 2021	Updated	Changes to clarify processes	Steve Durbin, Data Protection Officer
1.4	29 June 2023	Review	ICO link updated, minor orthographic errors corrected	Steve Durbin, Data Protection Officer
1.5	23 November 2023	Updated	Added details of “citizen access”	Steve Durbin, Data Protection Officer

For more information on the status of this policy, please contact:

North Central London CCGs	Information Governance Leads
Approved by	Management Team
Approval Date	14 June 2024
Next Review Date	2 years after approval
Responsibility for Review	Practice Manager
Contributors	NLC IG Group and NCL General Practices
Audience	Practice staff and patients

Contents

1. Introduction	3
2. Aim	4
3. Legislations and Code of Practice	4
4. Roles and Responsibilities	5
4.1 Accountable Officer	5
4.2 Data Protection Officer	5
4.3 All Managers and Staff	5
4.4 Practice as a Data Controller	6
5. Requirements for a valid subject access request	6
5.1 Providing personal information under subject access request	6
5.2 Types of personal information that can be disclosed	6
6. Timescales for responding to subject access requests	8
6.1 Suspension of response time	8
6.2 Advice and assistance to applicants	8
6.3 The appropriate limit (Fees)	9
7. SAR made by a third party/representative of a data subject	9
7.1 SAR relating to children	9
7.2 SAR relating to other individuals who can be identified	10
7.3 Disclosure of information that may harm someone's health	10
7.4 Grounds to limit or not provide personal data	10
8. Applying an exemption under the data protection legislation	11
9. Sharing personal data of an individual with law enforcement, regulatory bodies and others	11
10. Internal reviews and complaint procedures	12

11. Training.....	12
12. Dissemination and Implementation.....	12
13. Monitoring & Compliance	13
Appendix 1 - Subject Access Request Flow Chart	14
Appendix 2: OPTIONAL Subject Access Request form.....	15
Appendix 3: Standard Templates	17

1. Introduction

The UK law on data protection is currently laid out via a number of laws, key among them being the Data Protection Act 2018 which, along with the Data Protection, Privacy and Electronic Communications (Amendments etc.)(EU Exit) Regulations 2019 and the EU GDPR created the “UK GDPR”. We shall refer to this and the other laws involved as the “data protection legislation”.

This Subject Access Request (SAR) Policy has been written in line with the present law as noted above.

The data protection legislation details rights of access to both manual data (which is recorded in a filing system) and computer data for the individual/data subject.

This right, commonly referred to as Subject Access Request (SAR) is given via Article 15 of the UK GDPR¹, gives rights to a data subject in the UK to request personal information the Practice holds about them. Anyone with full mental capacity can also authorise a representative / third party, for example solicitors / advocates to help them make a SAR. For children, parents can make requests (see later). Those appointed by the Court of Protection having powers for Health and Welfare (e.g. Deputies, Powers of Attorney) for the data subject can also request.

Under the data protection legislation data subjects have the right to obtain from Practice confirmation as to whether or not personal data concerning the individual/data subject are being processed, and, where that is the case, access to the personal data and the following information:

- a) the purposes of the processing;
- b) the categories of personal data concerned;
- c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

¹ The right would also apply to persons resident in Europe, but would then come from the original European GDPR. Other countries may also have extraterritorial laws in this area. Consult the DPO if it is not clear which law applies.

- e) the existence of the right to request from the controller rectification or erasure (where necessary) of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- f) the right to lodge a complaint with a supervisory authority (Information Commissioner's Office);
- g) where the personal data are not collected from the data subject, any available information as to their source;
- h) the existence of automated decision-making, including profiling, referred to in Article 22 (1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- i) right to be informed about the appropriate safeguards where personal data is transferred to a third country or international organisation;
- j) right to request a copy of any personal data undergoing processing.

In line with the Information Commissioner's subject access Codes of Practice, organisations are encouraged to have SAR Policy or Procedure in place to ensure that individuals' rights of access are met within a timely and appropriate manner, and seek to enable all who wish to do so to have access to the records that are held about them.

2. Aim

This Subject Access Request Policy details how Practice will meet its legal obligations concerning individual's access to their information. The requirements within the Policy are primarily based upon the data protection legislation as noted above.

This Subject Access Request Policy has been written to ensure that all staff of Practice are aware of their responsibilities to provide information if requested.

3. Legislations and Code of Practice

For the purpose of this Policy, other relevant legislations and appropriate guidance may be referenced. The legislations listed below refer to issues of security and/or confidentiality of personal data:

- Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Crime and Disorder Act 1998
- Computer Misuse Act 1990
- Criminal Justice and Immigration Act 2008
- Information Commissioner's Office: Subject Access Request Code of Practice

4. Roles and Responsibilities

4.1 Accountable Officer

The Practice Manager has overall accountability and responsibility for subject access requests. The Accountable Officer has delegated SAR operational responsibilities to various administrative staff.

4.2 Data Protection Officer

The Data Protection Officer (DPO) has day-to-day responsibilities for providing advice and guidance on all aspects relating to data protection matters. The responsibilities of the DPO include:

- To advise the practice on issues relating to data protection by providing guidance;
- monitor organisational compliance with the Data Protection Legislations including policies and procedures that underpins the protection of personal data within the organisation;
- to provide awareness-raising and training for staff involved in processing operations, and the related audits;
- to liaise with the Information Commissioner's Officer (ICO) on matters around confidentiality and data protection, information security and records management;
- to provide advice where requested as regards to Data Protection Impact Assessment (DPIA) and monitor the risk management process;
- to consult with the ICO prior to data processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the organisation to mitigate the risk.

The DPO shall in the performance of his/her functions have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

4.3 All Managers and Staff

All managers are to ensure that staff in their team/service area are aware of, and adhere to this SAR Policy. They are also responsible for ensuring that the staff are updated with regards to any changes in the Policy.

All staff have a responsibility to ensure that they comply with the statutory obligations under the data protection legislation, and any guidance lay down to ensure compliance.

Particularly, staff should ensure that:

- They are aware of their responsibility to support SARs and where in the organisation such requests are ultimately handled;
- Personal data and records (whether in electronic or manual) relating to patients/service-users and staff are kept secure, accurate, relevant and up to date.

Staff wishing to access to personal confidential information that the Practice holds about them should submit their requests in writing to the Practice Manager.

4.4 Practice as a Data Controller

The Practice is a data controller in respect of any personal data and special categories of personal data within its remit and as part of its statutory functions, the Practice determine the purposes for which, and the manner in which those personal information are, or are to be, processed. Therefore, any of staff may be required to respond to a SAR relating to personal information they hold within their team/service area.

5. Requirements for a valid subject access request

Requests can be made in writing, verbally or by electronic means e.g. email. Adequate steps must be taken to identify the identity of the requester before providing the information – however this must be limited to establishing the person's identity.

Each applicant / data subject can be asked to supply copies of their identification if we are not able to confirm identity. Examples include:

- Driving licence or Passport or Birth Certificate or Residence Card;
- Proof of address, e.g. Driving licence or a utility bill (no more than 3 months old)

However, **the key test is proportionality**; if you have doubts about the identity of the person making the request you can ask for more information. It is important that you only request information that is necessary to confirm who they are – you must not, for example, refuse a SAR because a person cannot provide photo ID.

5.1 Providing personal information under subject access request

The SAR provides a right for the data subject / applicant to see their own personal data, rather than a right to see copies of documents that contain their personal data. Often, the easiest way to provide the relevant information is to supply online access, or copies of original documents, where it is reasonable to do so. [See the ICO Code of Practice on SAR.](#)

Data should be provided electronically by default if it was requested electronically. The data subject / applicant can request other media e.g. printed copies, but we are only required to supply one copy – so, for example, if a request is made for both electronic and paper copies, we can require that they pay for the paper copies. If the data subject / applicant requests ONLY a paper copy, we must supply free of charge.

Information must be supplied to the data subject / applicant in an intelligible, easy to understand form, unless to do so would involve 'disproportionate' effort. For manual records this would involve photocopies. For computerised records these can be supplied in electronic format but must contain explanations of codes or abbreviations where appropriate. If the 'disproportionate' effort issue arises, the records can be shared with the individual on a face-to-face basis who can be asked to visit the premises to view their records.

5.2 Types of personal information that can be disclosed

Any information that constitutes personal data or special categories of personal data of the subject/applicant should be provided (subject to any data protection exemptions which include information that may cause harm or distress).

Under the data protection legislation the term “*personal data*” means any information relating to an identified or identifiable living natural person (‘data subject’); an identifiable living natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier; they include:

- Demographics - name; address; postcode; telephone number; date of birth;
- an identification number - NHS number, National Insurance Number, location data, an online identifier and Driving licence number [Note that driving licence number is included in this list because it directly yields date of birth and first part of surname]

Special categories of personal data include:

- Health records or data concerning a natural person’s sex life or sexual orientation
- Genetic data
- Biometrics, DNA Profile, Fingerprints
- Child Protection Records
- Adoption Records
- Tax, Benefit or Pension Records
- Racial or ethnic origin;
- Social Services Records
- Housing Records
- Political opinions;
- Religious or philosophical beliefs

For the deceased, the data protection legislation no longer applies, but the common law duty of confidentiality still applies. There is GMC guidance on this sharing available online, and the DPO has produced FAQs and other guidance on sharing. In general, we would provide information to anyone with a claim on the estate – commonly family – but only information related to that claim, under the Access to Health Records Act 1990.

5.3 The NHS App, “citizen access” and other online access.

Since October 2023, NHS patients have had a full right of access to “prospective” records by default. “Prospective” means records created after October 2023 or when the patient joined their current practice, whichever is later.

All GP surgeries are now required by their contract to give patients in England online access to new information as it is added to their GP health record (unless the patient has individually decided to opt-out or any exceptions apply)

Patients with online accounts should be able to read new entries, including free text, in their health record. This applies to prospective record entries and not historic data. This does not replace the right of subject access – patients can still ask for a copy of their records.

Patients can use a variety of digital platforms to view the data including but not limited to the NHS App, NHS portal, Patient Online, MyGP App.

A Data Protection Impact Assessment has been carried out for the practice to identify any risks to patient data. This indicates a cautious approach must be taken as it is not possible to assess the

risk of these platforms due to lack of transparency and with there being no suitable software available to easily review records for information that should not be shared before granting access.

Some of the risks relate to

- The impact of viewing certain the information on the patient.
- The risk of a patient being coerced into sharing their record with a 3rd party or their record being hacked by someone they know.
- The impact of the practice inadvertently sharing 3rd party information from the record with the patient that the practice does not have the right to share.
- The risk of the online platforms being accessed by malign actors.

The practice has therefore taken a cautious approach. The practice has risk assessed the coded data in patients' records and where there is possibility of any of the above risks the record has been flagged for review before online access is granted. This does not affect the right of subject access.

6. Timescales for responding to subject access requests

Under the data protection legislation the Practice is required to respond to subject access requests without undue delay and in any event within **one calendar month** of receipt of the request from the data subject. The period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

In the case of further extension, the Practice will inform the data subject / applicant of any such extension within one calendar month of receipt of the request, together with the reasons for the delay. Failure to do so is a breach of the legislation and could lead to a complaint being made to the ICO. It is strongly recommended that the Practice consult the DPO before taking such an extension.

To assist the obligation to provide information within the time limits, the Practice will ensure that all staff are aware of the SAR process, and requirements to provide the information when requested by the data subject.

SARs will be acknowledged by the Practice or DPO within 2 working days after the date of receipt of the request.

6.1 Suspension of response time

Where the Practice requires clarification of a request is considering or required the identity of the applicant the one calendar month rule is suspended until the clarification is received.

6.2 Advice and assistance to applicants

Where required, the Practice will endeavour to provide advice and assistance in respect to complex request. This may include:

- If the request is unclear and further clarification is needed;
- if the information has been requested in a particular unacceptable acceptable or unreadable format;
- Where complying with the request would involve disclosure of personal data about another individuals;

- If the information requested is subject to one or more of the exemptions in the Data Protection Legislations.

6.3 The appropriate limit (Fees)

Request for personal information and communication provided under the data protection legislation shall be provided free of charge in a single format. However, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Practice may either:

- Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
- refuse to act on the request.

The Practice will ensure the balance of probability and fairness have been carefully considered when demonstrating the manifestly unfounded or excessive character of the request.

7. SAR made by a third party/representative of a data subject

Where personal information is being requested by a representative (e.g. solicitor/advocate) of the data subject, the Practice must be satisfied that the representative has the authority to make the request on behalf of the data subject and that the appropriate authorisation to act on their behalf has been included.

In these cases, you need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement.

Where solicitors are acting for the data subject, if the solicitor is in good standing with the Law Society² we do **not** need to ask for further identification of the data subject.

The representative / third party may provide the following proof of identity of the data subject before personal information can be disclosed:

- Driving licence or, Passport or birth certificate;
- Proof of address, e.g. a utility bill (no more than 3 months old);
- A signed letter of authorisation from the data subject consenting that the solicitor can act on their behalf or;
- Lasting Power of Attorney or Deputyship covering health and welfare

7.1 SAR relating to children

Children's data is their data, no matter what their age. Those with parental responsibility for the child may make a Subject Access Request on behalf of the child. However, if the child is Gillick Competent we **must** consult the child for their view on whether they wish the information to be released. This is generally regarded as being around age 13 but can be younger or older depending on the child.

If the child refuses the disclosure we do not need to complete the request for the parent.

² You can check this at <https://www.sra.org.uk/consumers/register/>

7.2 SAR relating to other individuals who can be identified

Where the Practice cannot comply with a request without disclosing information relating to other individuals who can be identified from that information, the Practice is not obliged to comply with the request unless –

- a) the other individual has consented to the disclosure of the information to the person making the request, or,
- b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual, for example, redacting (blanking out) the name or other identifying features.

The Practice will provide the data subjects/applicants with information that constitute their personal information only, and will ensure that any duty of confidentiality owed to the other individual(s) is respected. Note that for medical professionals involved in treatment, this is part of the record and not personal data, so should not be redacted.

7.3 Disclosure of information that may harm someone's health

Where a representative/solicitor is making a SAR on behalf of an adult who lacks full mental health capacity, the DPO or staff dealing with the request must be satisfied that the request has been made in the individual's best interest. This may include requesting approval from the data subject's legal guardian or medical practitioner.

A medical professional may believe that providing an individual with access to certain information might cause serious harm to their physical or mental health or to that of another person. If so, the data protection legislation allows the Practice (data controller) to withhold the information. However, only a medical professional can make such a decision, and it must be fully documented.

This exemption does not apply to information the individual already knows.

If an individual disputes some of the information held within their record this should be discussed with the DPO or the Practice.

7.4 Grounds to limit or not provide personal data

There are various grounds where personal data does not have to be provided, in part or in full, these include:

- 1) Where complying with the request would involve disclosure of personal data about other individuals who have not given their consent, and redacting (blanking out) their personal information or other identifying features is impossible.
- 2) Where disclosure would be likely to prejudice an ongoing enquiry or investigation. Where this can be demonstrated the Practice do not need to disclose the existence of such information.
- 3) If the information requested is subject to one or more of the exemptions in the data protection legislation.
- 4) Where it is a repeated or similar request and the Practice had previously complied with the request, unless a reasonable interval has elapsed.
- 5) If providing documents would involve disproportionate effort or expense. If this is the case the data subject must be informed what information is held, the source of the information, the purpose it is being processed and who it may be disclosed to. This 'exemption' would

usually only apply to situations where there is a very large amount of data held within an unstructured (paper) filing system.

The term 'disproportionate effort' refers to the time and cost of complying with a request and this must be balanced against the effects on the individual requesting the information of not supplying the information. In practice this situation should seldom arise.

8. Applying an exemption under the data protection legislation

The data protection legislation has certain provisions which allow public authorities to withhold information from an applicant where an exemption applies. Therefore, in some cases, there will be valid reasons why some information may not be released to an applicant and these include:

- If the data consist of information in respect of which a claim to legal professional privilege could be maintained in legal proceedings.
- If the disclosure of personal data to third parties contravenes the first data protection principle (process fairly and lawfully).
- For some issues regarding safeguarding of vulnerable persons

It is important to note that if an exemption is applied under data protection legislation the DPO or staff of the Practice applying the exemption should be aware that they may need to substantiate their decision if challenged by the applicant or the ICO as part of the review process. It is therefore advisable to document decisions (including legal basis) made in relation to using exemption or redaction.

In all cases where an exemption is used this should be explained to the requester as clearly as practicable without defeating the purpose of the exemption.

A recording sheet is provided for practices to record exemptions used and it is recommended that this is completed for every Subject Access Request where exemptions are exercised. This should NOT be provided to the requester but held for any enquiries by the DPO or the regulator

9. Sharing personal data of an individual with law enforcement, regulatory bodies and others

In some circumstances the Practice may be legally required to share personal information with law enforcements and regulatory bodies (without the consent of the data subject). There are also circumstances (e.g. legal cases, public health risks) where other bodies may be involved. The legal basis and justification for the sharing may be underpinned by the following Articles of the UK GDPR (this list is not exhaustive):

Article 6(c) - necessary for compliance with a legal obligation to which the controller is subject;

Article 6(d) - necessary in order to protect the vital interests of the data subject or of another natural person;

Article 9(f) – necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

Article 9(g) - necessary for reasons of substantial public interest

There are specific exemptions and qualifications in the data protection legislation allowing these disclosures.

The Practice will review each request based on its merits before deciding whether to release information to the 'relevant authorities'. It is recommended that the DPO is consulted for a view in each case.

10. Internal reviews and complaint procedures

If the applicant is dissatisfied with either the way their request has been handled or the response provided, they may appeal to the Practice for a review within 20 working days of receiving their response. The internal review will be carried out promptly and in no more than 20 working days from the date of the request for review.

The DPO and Practice can be contacted at:

Data Protection Officer (DPO): Steve Durbin, Ex Cathedra Solutions Ltd

Email: dpo.ncl@nhs.net

(or by post to the practice address, marked for the attention of the DPO)

Postal Address: The Practice @ 188, 188 Golders Green Road, London, NW11 9AY

If the applicant remains dissatisfied about the decision, they must be advised on their rights to complain to the Information Commissioner who can be contacted at:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

Tel: 0303 123 1113

Online: <https://ico.org.uk/>

11. Training

The Practice will ensure all staff are adequately trained SARs. Training will include but not limited to:

- What information to provide or not to provide
- Correct identification of the requesting individual;
- Location of personal information;
- Timescales for compliance;
- Provision of information in an intelligible format;
- Action to be taken if the information includes third party data

12. Dissemination and Implementation

This Policy and other related documents will be publicised on the Practice internet/intranet. All staff are required to ensure that their teams understand its application to their business areas.

Awareness of any new content/change in process will be through the staff bulletin, in the first instance. Where a substantive revision is made then a separate plan for communicating and implementing this change will be agreed with DPO.

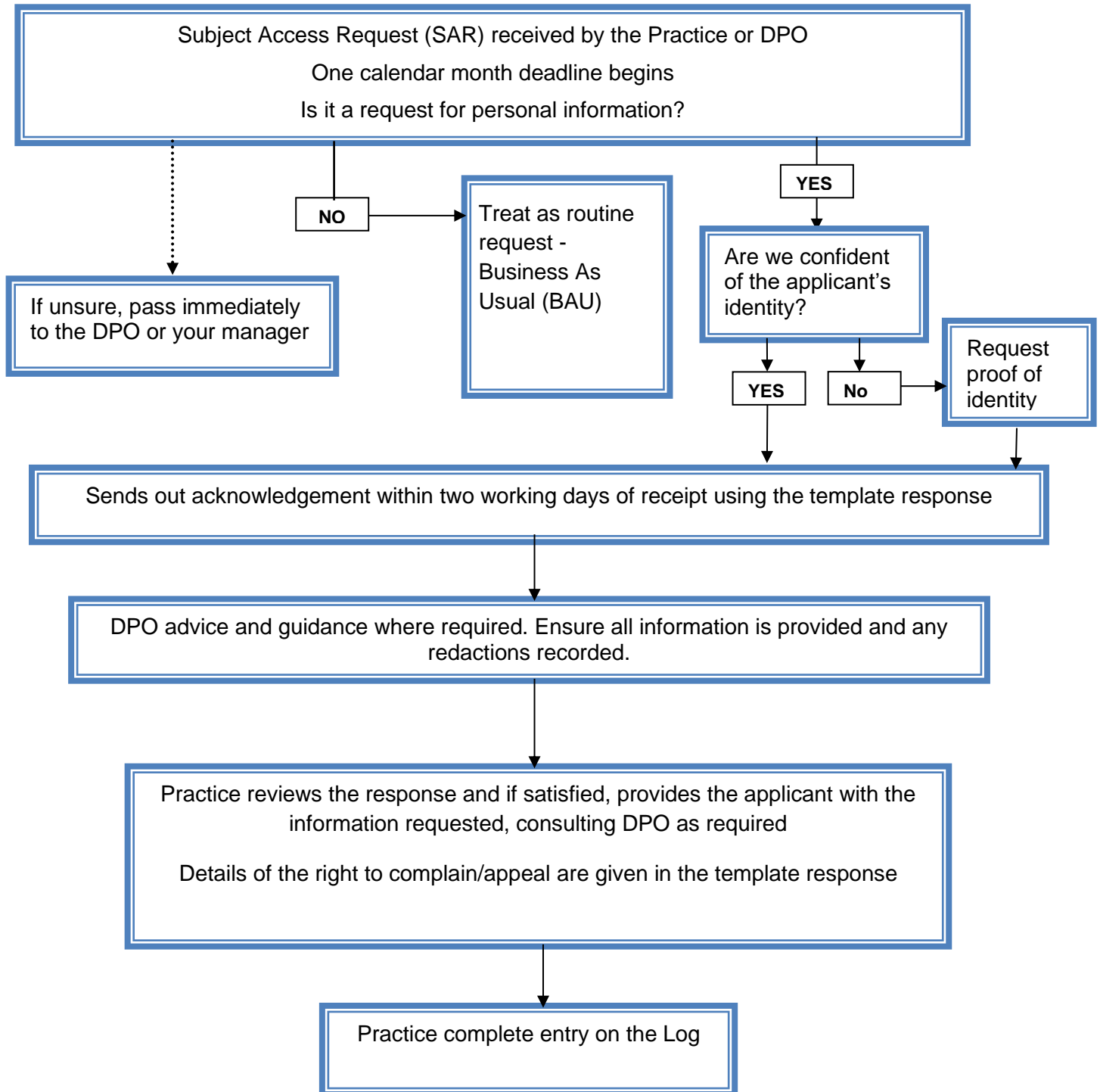
13. Monitoring & Compliance

The Practice will annually evaluate the effectiveness of this Policy. Monthly reports on information requests received are provided to the Practice Manager.

Noncompliance

Noncompliance with this Policy by staff will be brought to the attention of the Accountable Officer and their line managers.

Appendix 1 - Subject Access Request Flow Chart



**ANY DELAYS IN THE PROCESS MUST BE REPORTED TO THE DPO AND PRACTICE
MANAGER IMMEDIATELY**

Appendix 2: OPTIONAL Subject Access Request form

This form can be provided if requested but cannot be required or enforced. It gives the requester a standard format for their request if needed

a) Details of person requesting information (the Applicant):

Full name:	
Date of birth:	
Address:	
Telephone Number:	
Email:	

b) Are you the Data Subject (for example the named individual who the requested records refer)?

YES: If you are the data subject please go to question e)

NO: Are you acting on behalf of the Data Subject with their written authority? If so, the written authority must be included. Please answer questions c) d) and f).

c) Details of the Data Subject if different to those given in answer to question a).

Full name:	
Date of birth:	
Address:	
Telephone Number:	

d) Please describe your relationship with the Data Subject that leads you to make this request for information on their behalf:

e) Please give details as to the information you would like to review:

Include the date range(s) for the information held (approximate dates are acceptable):

f) Please provide the following proof of Identity and authorisation from the Data Subject:

- Driving licence or, Passport or birth certificate of the data subject.
- Proof of address, e.g. a utility bill (no longer than 3 months old) of the data subject.
- A signed letter of authorisation from the data subject consenting that the person can act on their behalf, Lasting Power Attorney or Deputyship for Health and Welfare, Solicitor registration and statement that you are acting for the data subject

NOTES:

The Practice will normally respond to a Subject Access Request within one calendar month of receipt. This period will not commence until the Practice is satisfied as to the identity and authority of the applicant.

Information will usually be provided in an encrypted email unless the request specifies a preferred alternative method.

Solicitors applying are advised that they should provide evidence that they are acting for the data subject although a signed authority is NOT required if the solicitor is in good standing and registered as practicing by the Law Society. **The practice is aware of the code of practice on use of medical information for insurance requests and will ensure that this guidance is followed; solicitors not following it will be reported to the regulatory bodies.**




The Practice may seek further information from the applicant as to the specific information requested. Any request for clarification may suspend the one calendar month period until the required information is received.

Please return this completed Subject Access Request (SAR) Form and any requested documentation to the address below:

The Practice @ 188, 188 Golders Green Road, London, NW11 9AY

Appendix 3: Standard Templates

The templates have been embedded in the table below:

Embedded Templates	
Response letter	 SAR Response Template_GP Practice
Schedule of information provided	 Schedule of information provided_
Redaction Recording worksheet	 SAR%20Redactions% 20Workbook.xlsx