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

For more information on the status of this policy, please contact:	
North Central London CCGs	Information Governance Leads
Approved by	**Menaka Kugarajan**
Approval Date	**27.06.2018**
Next Review Date	**2 years after approval**
Responsibility for Review	**TBC**
Contributors	**NLC IG Group and NCL General Practices**
Audience	**Rainbow Practice**

Contents

1. Introduction

The UK Data Protection Bill will become law when enacted as the Data Protection Act 2018. It will explicitly bring provisions of the EU General Data Protection Regulation (GDRP) 2016 into UK law and establish continuity of the GDPR. The Act will legislate in areas where the GDPR allows flexibility at national level. It will also introduce legislation on processing for law enforcement purposes (in support of the EU Law Enforcement Directive) and by the intelligence services, and make provision for the Information Commissioner (the UK regulator). The current Data Protection Act (DPA) 1998 will be completely repealed when DPA 2018 comes in force.

This Subject Access Request (SAR) Policy has been written in line with the present DPA 1998 and EU GDPR as they govern the use and protection of personal data, and sensitive personal data (known as special categories of personal data under the GDPR).
The Policy will be reviewed when the DPA 2018 comes in force and when further changes to the Act necessitate additional review.

The current DPA 1998 and EU GDPR 2016 ((hereinafter called the Data Protection Legislations) 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 created under section 7 of DPA 1998 and Article 15 of GDPR 2016, gives rights to a data subject/individual to request personal information the Rainbow Practice holds about them. Anyone with full mental capacity can authorise a representative/third party, for example solicitors/advocates to help them make a SAR.

Under the DPA and GDPR Legislations data subjects have the right to obtain from Rainbow 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;
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 Commission'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 Rainbow Practice will meet its legal obligations concerning individual's access to their information. The requirements within the Policy are primarily based upon the DPA 1998 and EU GDPR 2016 as they are the key legislations covering rights to personal information.

This Subject Access Request Policy has been written to ensure that all staff of Rainbow 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 the Practice Manager

4.2 Data Protection Officer

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

- To advise all staff on issues relating to data protection by providing guidance and templates;
- 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.

A quarterly report on the number of SARs received will be submitted to the Practice Manager. The report will detail all aspects of the disclosure and non-disclosure of recorded information by the Rainbow Practice.

4.3 All Managers and Staff

All managers are to ensure that staff in their practice 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 Legislations, 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 Rainbow Practice holds about them should submit their requests in writing to:

Mrs Menaka kugarajan

1 Smythe Close, London

N9 0TW

Rainbow.practice@nhs.net

4.4 Rainbow Practice as a Data Controller

The Rainbow Practice' is a data controller in respect of any personal data and special categories of personal within its remit and as part of its statutory functions, the Rainbow 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

Adequate steps must be taken to identify the identity of the requester. Each applicant/data subject must be asked to supply the following copies of their identification:

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

5.1 Providing personal information under subject access request

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 copies of original documents, where it is reasonable to do so. See page 8 of the ICO Codes of Practice on SAR.

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 or information that may cause harm or distress).

Under the Data Protection Legislations the term *"personal data*" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable 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

6. Timescales for responding to subject access requests

Under the EU GDPR the Rainbow 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 DPO will inform the data subject 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.

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

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

6.1 Suspension of response time

Where the Rainbow 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 Rainbow Practice will endeavor 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 GDPR shall be provided free of charge. However, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Rainbow 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 Rainbow 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 Rainbow 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.

The representative/third party must be required to 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 Attorney (property and financial affairs).

7.1 SAR relating to other individuals who can be identified

Where the Rainbow Practice cannot comply with a request without disclosing information relating to other individuals who can be identified from that information, the Rainbow 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 Rainbow Practice will provide the data subjects/applicants with information that constitute their personal information only, and will ensure that a duty of confidentiality owed to the other individual (s) is respected.

7.2 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 (Subject Access Modification) (Health) Order 2000 allows the Rainbow 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 Rainbow Practice.

7.3 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 whom 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 Rainbow 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 Legislations.
4) Where it is a repeated or similar request and the Rainbow 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 Data Protection Legislations

The DPA and GDPR give 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).

It is important to note that if an exemption is applied under Data Protection Legislations the DPO or staff of the Rainbow 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 cited (and a refusal notice issued) the balance of factors for and against should be explained to the applicant in the reply.

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

In some circumstances the Rainbow Practice may be legally required to share personal information with law enforcements and regulatory bodies (without the consent of the data subject). The legal basis and justification for the sharing may be underpinned by the following EU GDPR Articles:

Article 6(C) - sharing/processing is necessary for compliance with a legal obligation to which the controller is subject;

Article 6(e) - the sharing/processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The Rainbow practice will review each request based on its merits before deciding whether to release information to the 'relevant authorities'.

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 Rainbow Practice for a review. The internal review will be carried out promptly and in no more than 28 working days from the date of the request for review. The DPO and Rainbow Practice can be contacted at:

Menaka Kugarajan
Rainbow Practice
1 Smythe Close
London
N9 0TW

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 or 01625 545 745
Email: https://ico.org.uk/global/contact-us/

11. Training

The Rainbow 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 Rainbow Practice website. All staff are required to ensure that their teams understand its application to their business areas.

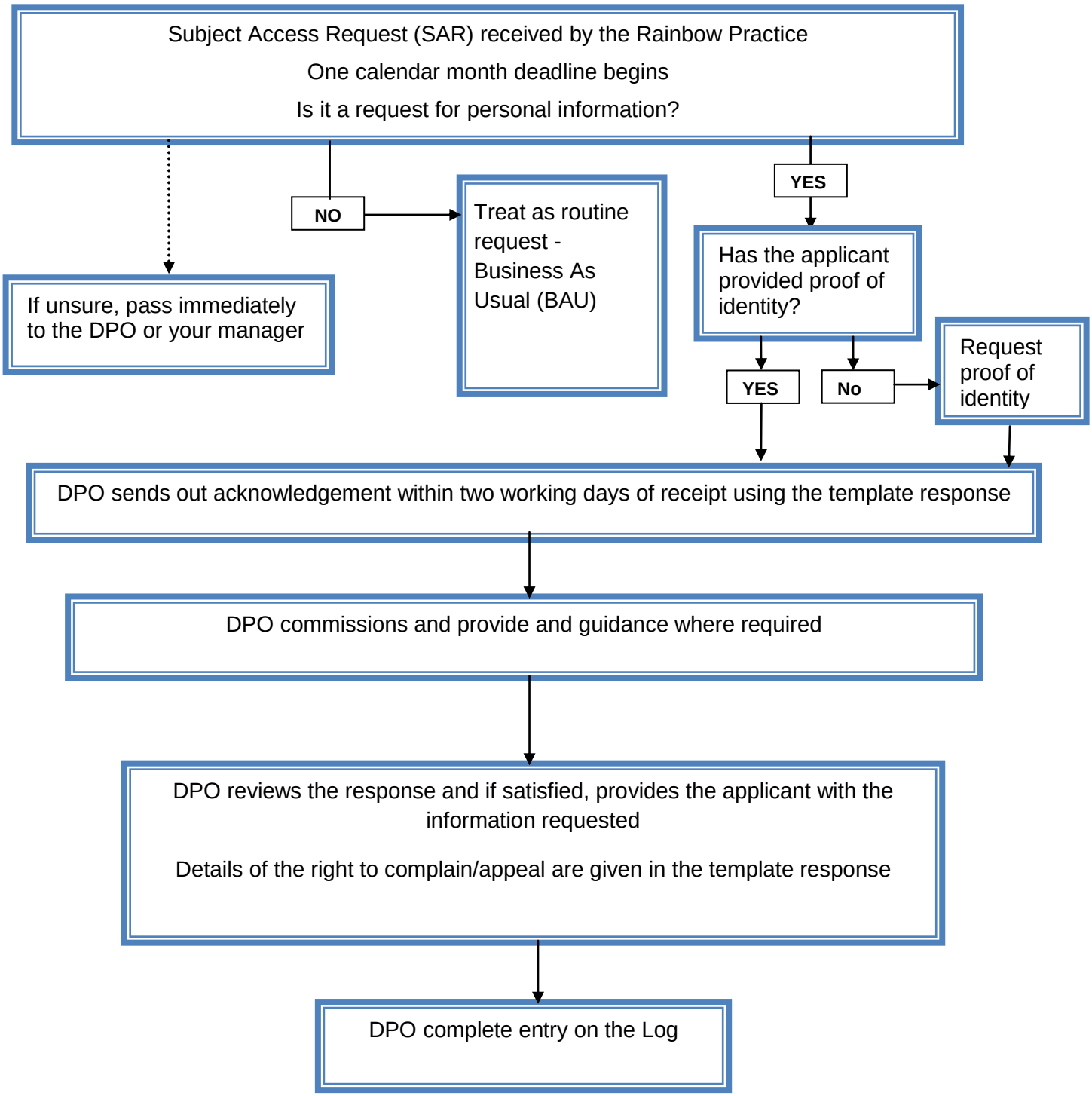
Awareness of any new content/change in process will be through the staff bulletin, in the first instance. Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the DPO.

13. Monitoring & Compliance

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

Non compliance
Non compliance 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 IMMEDIATELY

Appendix 2: Subject Access Request form

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

Full name: Date of birth:

Address:

Telephone Number:

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):

Please provide the following proofs of Id of 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 solicitor can act on their behalf or;
  Lasting Power Attorney (property and financial affairs

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 solicitor can act on their behalf or Lasting Power Attorney.

NOTES:

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

The Rainbow Practice may seek further information from the applicant as to the specific information requested. Any request for clarification will 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:

Menaka Kugarajan
Rainbow Practice
1 smythe close
London, N9 0TW
rainbow.practice@nhs.net