****

**Template**

**Subject Access Request Protocol**

**July 2018**

**Process Summary**

1. Receive request of SAR (clock starts).
2. Pass request to ATRL.
3. ATRL assures SAR is legitimate.
	1. Confirm identity of requestor
	2. Confirm informed consent of data subject
	3. Confirm that request is not excessive
	4. Confirm that request is not unfounded
4. ATRL logs request on SAR tracking log.
5. ATRL contacts requestor for more information (if required).
6. ATRL assigns SAR to staff member.
7. Nominated staff member retrieves data subject information.
8. Nominated staff member passes retrieved data subject information to ATRL.
9. ATRL assigns information to relevant staff member for redaction.
10. Relevant staff member redacts third party or harmful information.
11. Redacted information passed back to ATRL.
12. ATRL arranges for information to be passed to requestor (clock stops).

**1. Background**

1.1 This procedure has been written to assist with a responsibility for dealing with requests for personal data from a Data Subject (the individual whom particular personal data is about). These will be known as Subject Access Request (SAR).

The EU General Data Protection Regulation (GDPR) came into force on 25 May 2018 and
the Data Protection Act 2018 now applies to **living** natural persons.

1.2 Except in the case of a deceased individual, the Access to the Health Records Act 1990
has been repealed and access to all records for living individuals now comes under the
General Data Protection Regulation / Data Protection Act 2018.

1.3 Individuals (Data Subjects) have a right:

• be informed whether personal data is processed (which includes being held or stored);
• a description of the data held, the purposes for which it is processed and to whom the data may be disclosed;
• a copy of the information constituting the data;
• information as to the source of the data.

1.4 This protocol relates to legislation as set out in the General Data Protection Regulation / Data Protection Act 2018., covering the use of personal data. The Freedom of Information Act 2000 relates to non-personal information and legislation will give individuals the right to access non-personal information held by the NHS from January 2005.

If an application for personal data is made under Freedom of Information for either alive or
in respect of the deceased, the application should be managed under the Data Protection
Act or Access to Health Records Act and the requestor informed.

**2. Access to Records Lead (ATRL):**

All staff should forward requests for copies of health records to the nominated Access to Records Lead. The ATRL is **NAME**

**3. Timescale for complying with Subject Access Requests**

3.1 **PRACTICE NAME** should comply with the request promptly, preferably within 21 days but no later than one month after the request has been made.

3.2 Under the Access to Health Records Act 1990, if the record has been updated during the
40 days preceding the access request, access must be given within 21 days of the request. Where the record concerns information all of which was recorded more than 40 days before
the application, access must be given within one month with no fee.

3.3 The period for compliance can be extended by a further two months where requests are
complex or numerous. If this is the case, the individual MUST be informed within one month
of the receipt of the request and explain why the extension is necessary. Please see 1 .1
for further details regarding timescales.

**4. Charging for Subject Access Requests**

4.1 The **PRACTICE NAME** will no longer be able to charge a fee for processing a request for records unless the request is deemed manifestly unfounded or excessive. In such circumstances a reasonable fee may be charged. Currently, the terms of manifestly excessive and unfounded are undefined. The **PRACTICE NAME** has created a definition to use until such time there is national clarity on the matter.

For the purpose of **The PRACTICE NAME**, **manifestly excessive** is defined as

* Records of greater than 60 A4 pages that requires redaction of information.
* Repeated (i.e. > 1) request for the same information
* Copies of the same information

For the purpose of **The PRACTICE NAME**, **unfounded** is defined as

* Lack of **informed consent** from the data subject
* Inability to prove identity and relationship to data subject

The fee is not fixed and must be based on the real administrative cost of providing the information.

**5. Processing a Subject Access Request**

5.1 What is a subject access request?
A subject access request is a request made by or on behalf of an individual for the
information which he or she is entitled to ask for under Articles 12-15 of the General Data
Protection Regulation 2018. The request does not have to be in any particular form. Nor
does it have to include the words ‘subject access’ or make any reference to the General
Data Protection Regulation/Data Protection Act 2018. A request may be a valid subject
access request even if it refers to other legislation, such as the Freedom of Information Act.

There is no legally prescribed subject access request form. The requestor may be invited to use the **PRACTICE NAME** access request form, please note that this is **not** a condition of recognising a subject access request. A subject access request might also be received via email, fax or social media. Reasonable adjustments must be considered and/or made for disabled people, for example, recognising a formal request in a verbal format and responding in an appropriate format such as in Braille or large print.

5.2 Log Sheet / File
An individual log/tracking sheet will be started by the ATRL to track the request through the service, detailing

* the date the request was received.
* when each stage of the request was completed.
* handover to the originator of the requestor.

Copies of relevant correspondence and/or documentation in connection with the request
will be placed in a file and maintained by the ATRL for a period of 3 years before destroyed.
A check must be made of previous requests to ensure that a minimum of 6 months has elapsed since any previous request from the same individual.

5.3 Letter in Reply
A letter or email of acknowledgement will be sent to the requester. The letter may also
include the **PRACTICE NAME** subject access application form should any aspect of the request require clarification

5.4 Request for further information
To comply with the law, information relating to the Data Subject must only be disclosed to that person (data subject) or someone with their written consent to receive it.

Adequate steps must be taken to identify the requestor before commencing the work to
comply with the request under the act.

Where there is any doubt, proof of identity will be required. Examples of suitable
documentation could include **copies** of:

• Valid Passport.
• Driving Licence.
• Birth Certificate along with some other proof of address,

 e.g. a named utility bill or a Medical Card.

If the originals of these documents are received, the **PRACTICE NAME** must take due care of them and ensure their safe return.

To enable a search of the records, sufficient details are required, for example, data
subject’s name, previous name, date of birth or NHS number. The ‘Subject Access
Application Form’ may be sent to the Data Subject enabling clarification of the information
required.

5.5 Reply Received
When a reply is received from the Data Subject in response to any request for further
information, this will be checked by the ATRL to ensure that it is satisfactory and adequate
to continue the process.

5.6 Search for data/files
The ATRL will nominate a member of the **TEAM NAME** to search for both manual and electronic information regarding the data subject.

The nominated individual will be responsible for checking systems (including computer held
records), emails and files for any reference, directly or indirectly, relating to the Data
Subject.

Copies of the information will be obtained via printing, photocopying and returned to the
ATRL dealing with the request.

5.7 Withholding Information (review of data/files)
Information may be withheld if it:

• Third party
• Could cause serious harm to the physical or mental health or condition of the Data
Subject, or any other person
• Legal Privilege – information that relates to legal advice is classed as legally privileged

5.8 Definition of a Third Party:
There are generally two components to the meaning of third party:

• A person who has provided information (about the data subject)
• An organisation, other than the data controller (the **PRACTICE NAME**) or data processor (the **PRACTICE NAME** or authorised organisation that processes data on behalf of the **PRACTICE NAME**) that has provided information (about the data subject)

Information ***provided*** by a third party, for example, neighbour, friend, family member,
employer, Police, teacher, play group assistant, other agencies – DVLA, Benefits Agency, ***about*** the service user is classed as ‘Third Party Information’. This could also be data from a third party organisation, for example Police, Social Services,
School and DVLA

The designated person (ATRL) will seek the consent of the appropriate Health
Professional/Consultant/Department Manager for the release of the records. For clinical
records, this will be the person currently or most recently responsible for the clinical care
of the Data Subject to which the information relates.

For non-clinical records this will be the **PRACTICE MANAGER**.

5.9 Legal Privilege
Legal Professional Privilege protects all communication between a professional legal
adviser and his or her clients from being disclosed without the permission of the client.
The privilege is that of the client and not that of the professional legal advisor. This type of
data is exempt from the right of subject access requests.

5.10 Collating Responses/Redaction
The ATRL will collate the information received and prepare the disclosure response to the
Data Subject as necessary. The purpose of redaction is to irreversibly remove the exempt information from the final copy. Please remember to redact information using a safe and secure process, for example, black marker, Banner Correction Roller (correction tape), tipex or Microsoft Office functionality.

NB: Remember to keep a record of what information has been removed and why, for
example, legal privilege.

5.11 The definition of 60 A4 pages has been chosen as manifestly excessive based upon the need for a clinician to assess the information at an average of 1 page per minute. The **PRACTICE NAME** deems that loss of a clinician for 60 or more minutes as likely to impact upon our ability to provide appropriate clinical care and as such is by definition, excessive.

5.12 Sending Copies of Data – disclosure of information
When the information is complete and agreed/signed off – a copy of the record can be
made. Copies of the information and a covering letter will then be sent by the ATRL.

5.13 Where the information can be sent via secure email this is the preferred mechanism of communication. See the Doncaster LMC website for guidance on how to do this. <http://www.doncasterlmc.co.uk/secureemail.html>

5.14 Supervised access to view records
Viewing the records/information is an option but only if both parties agree. If not, copies
will be provided as above.

If viewing is supported – the process of reviewing the data sources and records must take
place as before (with the removal of third party information). The information/records must
not be left unattended with the requestor – so the registered holder of data must remain in
the room at all times to ensure the records are not tampered with and to explain any
entries or terminology; or to decipher and help with any legibility queries.

**6. Disclosure - Other than directly to the Data Subject**

6.1 Information may be requested by third parties (e.g. solicitors, relative, Ofsted etc.) on
behalf of the Data Subject. Where this is accompanied by authorisation (documented
consent) from the Data Subject then this request can be processed using this procedure.

6.2 Where a legitimate relationship between the requestor and the Data Subject cannot be demonstrated, or where the requestor has not shown appropriate informed consent of the Data Subject, the request will be deemed as **unfounded**.

6.3 Where the disclosure request is made by a third party on behalf of a Data Subject who
lacks capacity, further advice should be sort from the **PARTNERS**. The **PARTNERS** must be satisfied that disclosure would be in the Data Subject’s best interests. If this is not the case, disclosure cannot proceed.

6.4 Under the Mental Capacity Act 2005 – Independent Mental Capacity Advocates (IMCAs)
have rights of access to health/clinical records relating to the service user they are
representing. The **PRACTICE NAME** must “give access to relevant records when
requested by an IMCA under Section 35(6)(b) of the Act”. Therefore, disclosure may occur without the service user’s explicit consent.

6.5 Where necessary, the third party may be contacted for additional details to enable an
effective search for the information required for their purpose.

6.6 A person with parental responsibility has the right to request a copy of a child’s health
record if the child is deemed competent to give consent for themselves; consent should be
sought directly from them. The legal position regarding ‘competence’ is different for
children aged over and under 16.

6.7 **Children aged 16 and 17:** The Mental Capacity Act covers and empowers children aged
16 and 17 (‘young persons’). A young person has capacity unless it is established he or
she lacks it. If a young person lacks capacity because of an impairment of, or a
disturbance in the functioning of, the mind or brain, the Mental Capacity Act will apply in
the same way as it does to adults (people aged 18 or over). However if the young person
is unable to make a decision for another reason, for example, because he or she is
overwhelmed by its implications the common law principles set out in Gillick will apply.

6.8 **Younger Children:** Children under 16 are not automatically presumed to be legally
competent to make decisions about their healthcare. However, some under 16s are
deemed competent if they have sufficient understanding and intelligence to enable him or
her to understand what is proposed (‘Fraser ruling/competence’ or ‘Gillick competence’).
If a child of 16 or 17 is not considered competent, a person with parental responsibility can
make a request on behalf of a minor. Before releasing the data, consideration must be
given to the fact that the request is made solely in the interests of the minor.

However, when a child understands fully the choice to be made and its consequences,
based on the Gillick competency, the child's decision prevails

6.9 O**nce a child reaches the age of 18** they are assumed to be a competent adult and capable of making informed decision. Therefore
access requests cannot be accepted by a third party on their behalf without their consent.

6.10 **Children with learning disabilities**: it should not be assumed that a child with learning
disabilities is not competent to make his/her own decisions. Many children will be
competent if information is presented in an appropriate way and they are supported
through the decision-making process.

**7. Disclosure Exemptions**

The General Data Protection Regulation/Data Protection Act 2018 recognises there may
be valid reasons for not disclosing personal data; these are referred to as exemptions. In
these circumstances, the disclosure of information may not be viewed as subject access
request providing the exemption was valid. Therefore, this type of request must be
considered on a case-by-case basis ensuring only the relevant information is disclosed to
satisfy the exemption requirements.

7.1 Crime and taxation:
The listed GDPR provisions and Article 34(1) and (4) of the GDPR (communication of
personal data breach to the data subject) do not apply to personal data processed for any
of the following reasons:

- the prevention and detection of crime or
- the apprehension or prosecution of offenders
- the assessment or collection of tax or duty

Any request from the Police must be in writing to comply with the General Data Protection
Regulation/Data Protection Act 2018.

Please remember to confirm the identity of the person representing themselves as a Police Officer, for example, ask to see
their warrant card.

If the police are asking for access to the victim’s records, consideration must be given to
informing the victim of the request to release information so they understand the possible
consequences of a future court case where this information may be shared.

7.2 Other Requests
The same exemption can be applied to other organisations that have crime prevention or
a law enforcement function. For example, Department of Work and Pensions – Benefit
Fraud Section, NHS Fraud Department (NHS Act 2006)

**8. Medical Act 1983**

The Medical Act 1983 sets out the basic legislative framework for the governance of the
General Medical Council (GMC). The Medical Act gives the GMC powers and
responsibilities, under Section 35A for taking action when questions arise about fitness to
practice. As part of fitness to practice investigation, the GMC may request access to
medical records. The registered holder must comply with this request and have 14 days
(Section 35 A (6A)) to process and provide copies of the information held.

**9. Disclosure required by statute**

**Court Orders, Coroners Courts & Criminal CasesReview Commission**

9.1 All **Court Orders** and associated documents must be immediately forwarded to the
nominated ATRL for processing. Authorisation will be requested from the **PRACTICE NAME**
involved and photocopies of the records given to the Court. The originals will not be sent without the authorisation of the **PARTNERS**.

9.2 **Coroners** do occasionally ask for records. The **PRACTICE NAME** needs to negotiate with the Coroner whether they want the originals, and if so, a copy of the record should be
made prior to disclosure. The Coroner is entitled to the originals, however if the Coroner will accept a copy, then that can be supplied.

9.3 Access to clinical records requested by the **Criminal Cases Review Commission** is via
Criminal Appeal Act 1995, section 17(2). This is a statutory duty, and consent from the
service user is not required. All information held by the **PRACTICE NAME** must be disclosed
as requested. In the event of the originals being handed over, a complete copy of the records, documents, files must be made and retained by the **PRACTICE NAME.**

**10 War Pensions and Benefit Agency**

Originals will not be sent; copies must be taken and forwarded.

**11 Requests connected to Mental Health Review Tribunals**

It is acknowledged that a number of requests for access are received in preparation for
Mental Health Review Tribunals. The tribunals have to be arranged within a set time
frame. Relevant staff are aware that such requests have to be dealt with urgently and
they make every effort to ensure copies are provided in a timely fashion.

**12. Access to Medical Reports Act 1998**

The Access to Medical Reports Act 1998 governs access to medical reports made by a
medical practitioner who is, or has been responsible for the clinical care of the patient, for
insurance or employment purposes. Reports prepared by other medical practitioners, such
as those contracted by the employer or insurance company, are not covered by the Act.

The patient can apply for access to the report at any time before it is supplied to the
employer/insurer, subject to certain exemptions. The medical practitioner should not supply
the report until this access has been given, unless 21 days have passed since the patient
has communicated with the doctor about making arrangements to see the report. Access
incorporates enabling the patient to addend to the report and providing the patient with a
copy of the report.

Once the patient has had access to the report, it should not be supplied to the
employer/insurer until the patient has given their consent. Before giving consent, the patient
can ask for any part of the report that they think is incorrect to be amended. If an
amendment is requested, the medical practitioner should either amend the report
accordingly, or, at the patient’s request, attach to the report a note of the patient’s views on
the part of the report which the doctor is declining to amend. Patients should request
amendments in writing. If no agreement can be reached, patients also have the right to
refuse supply of the report.

Medical practitioners must retain a copy of the report for at least 6 months following its
supply to the employer/insurer. During this period patients continue to have a right of
access.

The medical practitioner is not obliged to give access to any part of a medical report whose
disclosure would in the opinion of the practitioner:

• cause serious harm to the physical or mental health of the individual or others,
or
• indicate the intentions of the medical practitioner towards the individual,
or
• identify a third person, who has not consented to the release of that information or who
is not a health professional involved in the individual’s care.

A medical practitioner may make a reasonable charge for supplying the patient with a copy
of the report.

**13. A patient living abroad**

Patients who move outside the UK are not permitted to take their health records with them,
however, they are entitled to request a copy of their records, and then take a copy abroad
with them.

**14 Filing of Subject Access Requests**

The log and all documentation relating to a particular request should be kept and retained
for a period of three years.

A copy of the disclosure letter which sets out the outcome of the request, must be retained
on the data subjects record.