

Subject Access Request

Reference Number: RDF1550-23

Date of Response: 13/06/23

Further to your Freedom of Information Act request, please find the Trust's response(s) below:

Please be aware that the Royal Devon University Healthcare NHS Foundation Trust (Royal Devon) has existed since 1st April 2022 following the integration of the Northern Devon Healthcare NHS Trust (known as Northern Services) and the Royal Devon and Exeter NHS Foundation Trust (known as Eastern Services).

Dear Royal Devon University Healthcare NHS Foundation Trust,

I am currently conducting a benchmarking exercise looking at Subject Access compliance within the NHS to identify any trends that correlate to higher compliance levels and best practice. Please can you provide me with the following information for the 2022/23 financial year.

- 1. How Many Subject Access Requests have been received by your organisation? (Please provide only those requests relating to Health and Social records where possible i.e Exclusion of requests for HR information. If this is not possible please provide the total number of all requests).*

Answer: 4,133.

- 2. Please provide the number of these requests which exceeded the one calendar month timeframe for processing (or those which have exceeded a total of three calendar months where an extension has been issued).*

Answer: 1,736.

- 3. How many of the total requests received were issued an extension.*

Answer: 1,139.

- 4. What system(s) is currently used to process / log these requests.*

Answer: Microsoft Office 365.

- 5. Do you have any software or systems for redaction purposes.*

Answer: Yes – Adobe Acrobat Pro.

- 6. Please provide the number of staff within the team processing (logging, facilitating and releasing) these requests including the relevant Agenda for Change grades. Please provide WTE and HC.*

Answer: 11.53 WTE.

- 7. Please provide the department in which the team processing these requests resides. If multiple teams/ departments process Subject Access Request, please provide details for both.*

Answer: Information Governance.

8. *Are your organisations medical records paper based, electronic or a mixture.*
Answer: A mixture.
9. *If electronic do you use a single EPR or multiple sources?*
Answer: Multiple sources.
10. *Are staff processing requests provided with a list of systems/ default locations to check in order to obtain the records requested.*
Answer: Yes.
11. *Are all records reviewed prior to disclosure? If so who are these reviews conducted by.*
Answer: The team processing the SARs have full training and review prior to releasing.
12. *Which roles carry out redaction of records prior to disclosure.*
Answer: Disclosure Officers.
13. *Do you issue or make available to data subjects a Subject Access Request, request form? (including any web based forms).*
Answer: Yes.
14. *If you have a procedure or standard operating procedure covering the processing of these requests can you please provide this.*
Answer: Please see SAR Policy attached.
15. *Would you like to receive a copy of the anonymised Benchmarking report, please advise accordingly within your response.*
Answer: Yes please.

Subject Access Request (SAR) Policy	
Post holder responsible for Procedural Document	██████████ Information Governance Manager
Author of Policy	Deputy Information Governance Manager
Division/ Department responsible for Procedural Document	Digital Services, Information Governance
Contact details	██████████
Date of original document	26/01/2018
Impact Assessment performed	<u>Yes</u> / No
Ratifying body and date ratified	Information Governance Steering Group: 26/07/2018. Extension until December 2022 has been approved at IGSG on 22/6/2022 including SIRO approval
Review date (and frequency of further reviews)	December 2022 (every 3 years)
Expiry date	25/07/2022 extended until December 2022
Date document becomes live	26/07/2018


Please *specify* standard/criterion numbers and tick ✓ other boxes as appropriate

Monitoring Information		Strategic Directions – Key Milestones	
Patient Experience		Maintain Operational Service Delivery	
Assurance Framework		Integrated Community Pathways	
Monitor/Finance/Performance		Develop Acute services	
CQC Fundamental Standards - Regulation:		Infection Control	
Other (<i>please specify</i>):			
Note: This document has been assessed for any equality, diversity or human rights implications			

Controlled document

This document has been created following the Royal Devon and Exeter NHS Foundation Trust Development, Ratification & Management of Procedural Documents Policy. It should not be altered in any way without the express permission of the author or their representative.

Full History		Status: Final	
Version	Date	Author (Title not name)	Reason
1.0	26/01/2018	Deputy Information Governance Manager	New Policy
2.0	2/9/2021	Information Governance Manager	Minor tweaks and extension to expiry date for integration
2.1	17/06/2022	Information Governance Manager	This policy has been given an extension until December 2022 whilst an integrated Royal Devon policy is developed to cover all sites. This policy applies to Eastern Services and sites only.

Associated Trust Policies/ Procedural documents:	Closed Circuit Television (CCTV) Policy Information Governance Policy Health Records Policy
Key Words	Data Protection, Subject Access, Access to Health Records
In consultation with and date: Equality & Diversity Manager and HR (13/04/2018), Patient Equality Lead (13/04/2018) Health Records Manager (13/04/2018), Trust Solicitor (13/04/2018), Radiology Department (13/04/2018), Occupational Health Department (13/04/2018), Fertility Department (13/04/2018), Trust Security Management Specialist (13/04/2018) Governance Managers (13/04/2018), Corporate Managers (13/04/2018), Department Managers (13/04/2018), Service Managers (13/04/2018), Senior Operational Managers (13/04/2018), Lead Nurses (13/04/2018), Senior Nurses (13/04/2018), Matrons (13/04/2018), Community Divisional Director (13/04/2018), Assistant Directors of Nursing , including Community Division (13/04/2018) Policy Expert Panel/Quality Assurance: 29/05/2018 Records Management Group: 30/04/2018 Information Governance Steering Group: 26/07/2018	
Contact for Review:	Deputy Information Governance Manager
Executive Lead Signature: <i>(Applicable only to Trust Strategies & Policies)</i>	 Medical Director

CONTENTS

1.	INTRODUCTION	4
2.	PURPOSE	4
3.	DEFINITIONS	4
4.	DUTIES AND RESPONSIBILITIES OF STAFF	5
5.	LEGISLATIVE CONTEXT	5
6.	RECOGNISING A SAR	5
7.	BUSINESS AS USUAL REQUESTS	6
8.	RECEIVING A SAR	6
9.	VALIDATING A SAR	6
10.	FEES & CHARGING	6
11.	LOGGING AND ACKNOWLEDGING A SAR	7
12.	FINDING THE REQUESTED INFORMATION	7
13.	WITHHOLDING INFORMATION FROM THE REQUESTER (EXEMPT AND THIRD PARTY PERSONAL DATA)	7
14.	CONSULTING WITH A HEALTH PROFESSIONAL	8
15.	RESPONDING TO A REQUEST	8
16.	KEEPING A RECORD OF DECISIONS AND DISCLOSURES	8
17.	REQUESTS FOR CCTV IMAGES/FOOTAGE	9
18.	REVIEWS	9
19.	STAFF TRAINING	9
20.	ARCHIVING ARRANGEMENTS	10
21.	PROCESS FOR MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF THE POLICY	10
22.	REFERENCES	10
	APPENDIX 1: THE DATA PROTECTION ACT 2018: SUBJECT ACCESS REQUESTS (A GUIDE FOR HEALTH PROFESSIONALS)	12
	APPENDIX 2: COMMUNICATION PLAN	14
	APPENDIX 2: EQUALITY IMPACT ASSESSMENT TOOL	15

KEY POINTS OF THIS POLICY:

This document is the Subject Access Request (SAR) Policy and Procedure of the Royal Devon University Healthcare NHS Foundation Trust (“the Trust”). It seeks to provide a framework for the processing of subject access requests received by the Trust.

The purpose is to ensure that the Trust complies with its obligations under the UK General Data Protection Regulation ‘Right of Access’.

1. INTRODUCTION

1.1 This document is the Subject Access Request (SAR) Policy and Procedure of the Royal Devon University Healthcare NHS Foundation Trust (“the Trust”). It seeks to provide a framework for the processing of subject access requests received by the Trust.

1.2 **Failure to comply with this policy could result in disciplinary action.**

2. PURPOSE

- 2.1 To ensure that the Trust complies with its obligations under the UK General Data Protection Regulation ‘Right of Access’.
- 2.2 To ensure that all staff are aware of their responsibilities in relation to data subjects exercising the right of access.
- 2.3 To establish consistency in the handling of SARs across the Trust.

3. DEFINITIONS

- 3.1 **UK General Data Protection Regulation (UK-GDPR)** – a UK law governing the processing of personal data by data controllers in the UK. The GDPR became law in all EU member states including the UK on 25th May 2018 and was retained in domestic law in 2021 following the UK’s exit from the EU.
- 3.2 **Data Protection Act 2018 (DPA2018)** – a UK law governing data protection, it supersedes the 1998 Act and works with the UK-GDPR to provide the clauses and exemptions.
- 3.3 **Data Controller** – the legal entity which determines the purpose and manner of the processing being undertaken on the personal data.
- 3.4 **Personal data** – information about a living, identifiable individual. This includes the individual’s opinions and expressions of opinion about the individual.
- 3.5 **Data Subject** – the individual to whom the personal data relates.
- 3.6 **Subject Access Request** – a written request to a data controller from a data subject for a copy of their personal data.
- 3.7 **Health Record** - a record consisting of information about the physical or mental health or condition of an identifiable individual, made by, or on behalf of, a health professional, in connection with the care of that individual.
- 3.8 **Disclosure Officer** – the individual responsible for case-managing a subject access request, for ensuring that appropriate searches are undertaken and appropriate consideration is given to whether the requested information can be disclosed. The disclosure officer is responsible for keeping a record of all decisions and actions relating to the requests assigned to them.
- 3.9 **Information Commissioner’s Office** – regulatory body for Data Protection.

Subject Access Request Policy

Ratified by: *Information Governance Steering Group, 26/07/2018*
and *22/06/2022. Review Date December 2022*

DUTIES AND RESPONSIBILITIES OF STAFF

- 3.10 **Medical Director/Senior Information Risk Owner (SIRO)** – responsible for delegation of monitoring and compliance with this policy.
- 3.11 **Information Governance Manager/Data Protection Officer** – responsible for monitoring, and establishing measures for, compliance with this policy.
- 3.12 **Deputy Information Governance Manager** – responsible for supporting the Information Governance Manager and Data Protection Officer by monitoring compliance with this policy and ensuring that accurately and timely information is gathered which evidences the state of compliance across those areas of the Trust processing subject access requests.
- 3.13 **Information Governance (IG) Team, Radiology Department, Fertility Department, Occupational Health Department**– responsible for processing subject access requests (see Section 8 for distinctions).
- 3.14 **Consultants** – responsible for making decisions about the application of exemptions in relation to requests for health records.
- 3.15 **All staff** – responsible for being able to recognise a subject access request, for signposting it immediately to the correct department and for cooperating with the Information Governance Team by providing any information requested to comply with a SAR.

4. LEGISLATIVE CONTEXT

- 4.1 The [UK General Data Protection Regulation \(GDPR\)](#) governs how organisations process personal data. It affords data subjects certain rights. These rights include the right of access, which allows a data subject to request a copy of his personal data from the data controller. A data controller must respond within a calendar month to advise whether he is processing the data subject's personal data and provide a copy of the requested data, subject to exemptions.
- 4.2 Where the requested data constitutes a health record, the data controller should respond within 21 working days. This is stipulated in the Department of Health Guidance for Access to Health Records.
- 4.3 The UK GDPR does not apply to information about deceased individuals. Requests for access to such information must be processed in accordance with the [Access to Health Records Act 1990](#).

5. RECOGNISING A SAR

- 5.1 Any written request for a copy of the data subject's own personal data should be treated as a potential subject access request (SAR), irrespective of who in the Trust has received it. The nature of the request will dictate whether it is best dealt with as a formal subject access request or responded to as 'business as usual'.

6. BUSINESS AS USUAL REQUESTS

- 6.1 Whilst the subject access rights technically apply once a valid request has been received, a pragmatic approach should be taken to dealing with patients and other service users who request information in writing; for example, an email asking for confirmation of an appointment time may constitute a SAR, but would be best dealt with as a business-as-usual enquiry and responded to quickly, in accordance with relevant local and organisational processes.

7. RECEIVING A SAR

- 7.1 If a SAR has been received and it is decided that it should be processed formally, the request must be forwarded immediately to the appropriate department, depending on what has been requested:
- X-Ray images – Radiology department
 - Occupational Health records – Occupational Health
 - Fertility records – Fertility department
 - All other requests – Information Governance Team
- 7.2 Where the requester is contemplating litigation against the Trust, the request must be forwarded to the Legal Team to process.

8. VALIDATING A SAR

- 8.1 Upon receipt of a SAR, the team responsible for processing the request must check that the request is valid. For a Subject Access Request (SAR) to be valid, the requester must:
- Provide sufficient clarity in their request to enable the data controller to determine whether it is processing the requested data, and to locate it
 - Satisfy the data controller of his identity
- 8.2 The Trust will publish a SAR application form on its website to assist requesters with providing the necessary information; however, the requester is not obliged to use any pre-determined form. Provided that the request meets the above criteria, it must be accepted as a valid SAR and processed accordingly.

9. FEES & CHARGING

- 9.1 Under UK GDPR, the Trust must provide a copy of the information free of charge.
- 9.2 A 'reasonable fee' may be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive
- 9.3 A fee may also be charged for requests for further copies of the same information, but a charge should not ordinarily be levied for all subsequent access requests.
- 9.4 The fee must be based on the administrative cost of providing the information.

10. LOGGING AND ACKNOWLEDGING A SAR

- 10.1 SARs must be assigned a unique reference number and recorded on a log.
- 10.2 If any validity checks are outstanding (e.g., the requester has not provided proof of ID), then this should be requested after the request has been logged. The 1 calendar month response timeframe does not begin until the request has been validated.
- 10.3 Once the request has been validated, an acknowledgement should be sent to the requester confirming receipt of the request and providing the requester with the reference number and deadline for the response.

11. FINDING THE REQUESTED INFORMATION

- 11.1 The disclosure officer must undertake all the necessary searches for the requested information as soon as possible after the request has been allocated to them. These searches must yield a copy of the requested information or confirmation that it is not being processed by the Trust. The Trust is required to undertake “all reasonable searches” for the information.
- 11.2 Where the disclosure officer has difficulty deciding where the requested personal data may be held, they should consider liaising with the requester about their interactions with the Trust.
- 11.3 A record of the searches undertaken must be kept, including what the outcome of those searches was.

12. WITHHOLDING INFORMATION FROM THE REQUESTER (EXEMPT AND THIRD-PARTY PERSONAL DATA)

- 12.1 Once the requested information has been located, it must be reviewed to determine whether the data subject is entitled to it.
- 12.2 In general, there is a presumption in favour of disclosure. However, the requester might not be entitled to some, or all, of his personal data where:
 - The requested personal data contains the personal data of another individual (third party personal data); and/or,
 - An exemption applies
- 12.3 Third party personal data should not normally be disclosed unless:
 - It is already known to the requester; or,
 - The third party has consented; or,
 - The information relates to a health professional who has contributed to the health record of the data subject, or been involved in their care; or,
 - It would be reasonable in the circumstances to release the information
- 12.4 Information may also be exempt from disclosure where disclosure would:
 - Harm the physical or mental health of the applicant or another individual
 - Prejudice the prevention/detection of crime, apprehension/ prosecution of offenders or collection/imposition of tax

Subject Access Request Policy

Ratified by: *Information Governance Steering Group, 26/07/2018*
and *22/06/2022. Review Date December 2022*

- Constitute a confidential reference given by the data controller
- Prejudice negotiations with the requester
- Prejudice management planning
- Be subject to legal professional privilege

12.5 Decisions about whether information should be withheld will generally be made by a trained disclosure officer, in consultation with relevant parties; however, a decision about whether the disclosure of information would harm the physical or mental health of an individual must only be made by a health professional.

12.6 As much of the requester's personal data as possible must be provided, without revealing exempt or third-party personal data. Whole documents or pages should not be withheld in totality if it would be possible to redact some of the exempt/third party data and still disclose the requester's personal data. Where this is the case, the exempt/third-party data must be adequately removed using a robust method of redaction.

13. CONSULTING WITH A HEALTH PROFESSIONAL

13.1 All SARs for a copy of a health record that are found to contain sensitive material not previously known to the requester must be reviewed by the most recent health professional involved with the patient's clinical care, as well as any other relevant health professionals. As part of this consultation exercise, the disclosure officer must provide the health professional(s) with a copy of the requested health record data, alongside the "Subject Access Requests – Guide for Health Professionals" (Appendix 1).

14. RESPONDING TO A REQUEST

14.1 Before responding to the request, the copy of the information being disclosed to the data subject should be watermarked with "SUBJECT ACCESS REQUEST – DATA SUBJECT COPY" and the unique reference number.

14.2 The information must then be provided to the data subject with a covering letter containing the following information:

- An apology if the response did not meet the statutory deadline
- A summary of the searches undertaken to find the information
- If applicable, an explanation of whether and why information was withheld (unless to do so would reveal exempt data)
- Details for the person/department who can answer any further queries about the request

15. KEEPING A RECORD OF DECISIONS AND DISCLOSURES

15.1 A record of all subject access requests must be retained for a period of 3 years from closure of the SAR (or 6 years where there is any subsequent review or complaint). This record must include the following:

- A copy of any withheld data, alongside an adequate explanation of why the information was withheld
- Any relevant correspondence relating to the request (including consultations and information searches.
- A copy of the request (the requester's ID documents do not need to be retained once they have been verified; however, a record of what was provided and who verified it should be)
- A copy of the information disclosed and covering letter

16. REQUESTS FOR CCTV IMAGES/FOOTAGE

- 16.1 Requests for copies of closed-circuit television (CCTV) footage, where the requester is present in the footage, must be dealt with as a formal subject access request by the Information Governance (IG) Team. The IG Team must be satisfied that the request is from the individual in the footage and seek adequate proof of this.
- 16.2 Requests for CCTV images showing property damage or a suspected criminal offence, where the requester was not present at the time of the incident, should not be dealt with as a subject access request. Such data may only be released to the police, or to the requester's insurance company. Any request of this nature on the Wonford & Heavitree site must be immediately forwarded to the acute security team for processing, in accordance with the [Trust's CCTV Policy](#). For community sites, all requests must be made to NHS Property Services (NHSPS) using the appropriate NHSPS access request forms for approval to facilitate the access / download in accordance with the Trust's CCTV Policy.
- 16.3 CCTV footage is ordinarily only kept for between 14-28 days, therefore any request for CCTV footage must be immediately notified to the Security team or NHSPS, as appropriate, to ensure that the requested footage is not destroyed.

17. REVIEWS

- 17.1 Where a requester expresses dissatisfaction with the handling of their request, then a review must be conducted by a trained senior colleague of the disclosure officer (such as their line manager). Where the request was processed by a team besides Information Governance, the reviewing officer should contact the IG Manager or Deputy IG Manager for advice.
- 17.2 The review must seek to determine whether the requester's right of access has been upheld. Examples of reasons for seeking a review include, but are not limited to:
- That the response was not issued within the statutory timeframe
 - That all the requested information was not supplied
 - That the application of an exemption could not be justified
- 17.3 Reviews must be concluded, and a response provided to the requester, within 21 days.

18. STAFF TRAINING

- 18.1 All staff will complete mandatory Information Governance Training on an annual

Subject Access Request Policy

Ratified by: *Information Governance Steering Group, 26/07/2018*
and *22/06/2022. Review Date December 2022*

basis. This training will explain what a SAR is, how to recognise one and what to do if you receive one.

- 18.2 The Deputy IG Manager will provide annual face-to-face training to all staff responsible for any part of the SAR handling procedure, from logging/acknowledging a SAR, through to making a disclosure or conducting a review.

19. ARCHIVING ARRANGEMENTS

The original of this policy will remain with the author who is the Deputy Information Governance Manager, Information Governance Team. An electronic copy will be maintained on the Trust Intranet, (A-Z,) P – Policies (Trust-wide) – S – Subject Access Requests Policy. Archived electronic copies will be stored on the Trust's "archived policies" shared drive and will be held indefinitely. A paper copy (where one exists) will be retained for 10 years.

20. PROCESS FOR MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF THE POLICY

20.1 To evidence compliance with this policy, the following elements will be monitored:

What areas need to be monitored?	How will this be evidenced?	Where will this be report, and by whom?
Compliance detailing the number of SAR's received	Statistics such as charts in reports – Bi monthly	The Deputy IG Manager will report to: Records Management Group Information Governance Steering Group
Compliance detailing the number of SAR's not responded to in the Statutory timeframe	Statistics such as charts in reports – Bi-monthly	The Deputy IG Manager will report to: Records Management Group Information Governance Steering Group
Compliance with the Data Security and Protection Toolkit (DSPT)	DSPT Action plan and Internal Audit report	Records Management Group, Data Quality and Integrity Forum, Information Security Forum and Information Governance Steering Group Presented by Information Governance Manager

21. REFERENCES

Data Protection Act 2018. (c.12). London: Stationery Office. Available at:
<http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>
(Accessed 29-05-18)

Access to Health Records Act 1990. (c.23). London: Stationery Office. Available at:
<http://www.legislation.gov.uk/ukpga/1990/23/contents>

Information Commissioner's Office website: <https://ico.org.uk/>
(Accessed 29-05-18)

Information Commissioner's Office (2012). *Subject Access Code of Practice: Dealing with requests from individuals for personal information. (version 1.2).*

London: ICO. Available at:

<https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf>

(Accessed 29-05-18)

Department of Health (2010). *Guidance for Access to Health Records Requests.*

http://webarchive.nationalarchives.gov.uk/+http://www.dh.gov.uk/en/Managingyourorganisation/Informationpolicy/Patientconfidentialityandcaldicottguardians/DH_4084411

APPENDIX 1: THE DATA PROTECTION ACT 2018: SUBJECT ACCESS REQUESTS (A GUIDE FOR HEALTH PROFESSIONALS)

THE DATA PROTECTION ACT 2018

Subject Access Requests

A Guide for Health Professionals

Data Protection Act Definitions

Data Protection Act 2018 – a law regulating the processing of personal data

Personal Data – information about a living, identifiable individual

Data Subject – the individual to whom the personal data relates

Data Controller – the organisation with legal responsibility for complying with the Data Protection Act (e.g., Royal Devon & Exeter Healthcare NHS Trust)

Health Record – this applies to all health records relating to the physical or mental health of an individual, which has been made by, or on behalf of, a health professional, in connection with the care of an individual

Health Professional – includes a registered medical practitioner, a registered nurse or midwife and professions allied to medicine, i.e., physiotherapists, occupational therapists, etc.

The Right to Subject Access

The UK GDPR and Data Protection Act 2018 sets rules for the processing of personal data by data controllers.

It applies to some paper records as well as those held on computers. The Data Protection Act also gives data subjects the right to obtain a copy of their own personal data from the data controller, subject to exemptions. This right is known as the Right to Subject Access.

Making a Subject Access Request

To exercise this right, the data subject must make a subject access request, by putting their request in writing, providing proof of their identity, and paying a fee. Requests may only be made on behalf of a data subject by someone else if the data subject has provided consent, or where the requester has Power of Attorney for the data subject, or has been appointed by the Court of Protection.

Deadlines

A data controller must respond to a subject access request within one calendar month of receipt.

Subject Access Request Policy

Ratified by: *Information Governance Steering Group, 26/07/2018*
and *22/06/2022. Review Date December 2022*

Handling a Request for Subject Access

Formal requests for subject access are logged and assigned a reference number by the Information Governance Team. The exceptions are requests for X-Ray images (which are facilitated by Radiology) and Occupational Health information (facilitated by Occupational Health). Where a subject access request is made for a health record and the requester is contemplating litigation against the Trust, the request is managed by the Legal Team.

Consulting with a Health Professional

Where a subject access request has been made for a copy of a health record (see Definitions), the Information Governance (IG) Team is required to consult with relevant health professionals so that an informed decision may be made about whether any information is exempt from disclosure.

In such a scenario, the IG team will contact the health professional who was most recently involved in the patient's care, and any other relevant health professionals, asking them to review the requested information. The decision to disclose or withhold information lies with the health professional, who will be allowed 7 calendar days to respond to the IG team. If no response is received within 7 days, the IG Team will assume that no exemptions apply.

Exemptions

The exemptions which the health professional is asked to consider apply when:

- The information requested identifies another person (third party), for example, where a relative has provided certain information. The identity of the health professional(s) involved in the care would not be exempt.
- The request for access is made on behalf of the data subject by someone else (such as parent for a child) and the data subject had either provided the information in the expectation it would not be disclosed to the applicant, or had indicated it should not be disclosed, or if the data was obtained as a result of any examination or test to which the data subject consented on the basis that information would not be disclosed.
- If releasing the personal data would be likely to cause serious harm to the physical or mental health of the data subject or any other person (which may include a health professional).

Responding to a Subject Access Request

Once the health professional has been consulted, the Information Governance Team will respond to the requester with a copy of the information that they are entitled to. The health professional does not need to do anything else in respect of the request.

Contact Us

If you are asked by the IG Team to assist with a subject access request and you would like to discuss this further, please speak to the member of staff who contacted you, in the first instance.

Otherwise, our telephone numbers are ext. [REDACTED]

You can find our Information Governance HUB pages here - [REDACTED]

Subject Access Request Policy

Ratified by: *Information Governance Steering Group, 26/07/2018
and 22/06/2022. Review Date December 2022*

APPENDIX 2: COMMUNICATION PLAN

COMMUNICATION PLAN

The following action plan will be enacted once the document has gone live.

Staff groups that need to have knowledge of the policy	All staff
The key changes if a revised policy	Minor changes only. For full review as part of integration policy review.
The key objectives	To ensure that the Trust complies with its obligations under Article 15 of the GDPR – Right of Access by the data subject.
How new staff will be made aware of the policy and manager action	Induction, HUB
Specific Issues to be raised with staff	What a SAR is, how to recognise one and what to do if you receive one
Training available to staff	All staff will complete mandatory Information Governance Training on an annual basis. This training will explain what a SAR is, how to recognise one and what to do if you receive one. The Deputy IG Manager will provide annual face-to-face training to all staff responsible for any part of the SAR handling procedure, from logging/acknowledging a SAR, through to making a disclosure or conducting a review.
Any other requirements	
Issues following Equality Impact Assessment (if any)	No negative impacts
Location of hard / electronic copy of the document etc.	HUB, Information Governance shared drive via Information Governance Manager

APPENDIX 2: EQUALITY IMPACT ASSESSMENT TOOL

Name of document	Subject Access Requests Policy
Division/Directorate and service area	Digital Services
Name, job title and contact details of person completing the assessment	██████████ Information Governance Manager
Date completed:	August 2021

The purpose of this tool is to:

- **identify** the equality issues related to a policy, procedure or strategy
- **summarise the work done** during the development of the document to reduce negative impacts or to maximise benefit
- **highlight unresolved issues** with the policy/procedure/strategy which cannot be removed but which will be monitored, and set out how this will be done.

1. What is the main purpose of this document?

To ensure that the Trust complies with its obligations under Article 15 of the GDPR (Right of Access).

2. Who does it mainly affect? (Please insert an “x” as appropriate:)

Carers x Staff x Patients x Other (please specify)

3. Who might the policy have a ‘differential’ effect on, considering the “protected characteristics” below? (By differential we mean, for example that a policy may have a noticeably more positive or negative impact on a particular group e.g. it may be more beneficial for women than for men)

Please insert an “x” in the appropriate box (x)

Protected characteristic	Relevant	Not relevant
Age	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Disability	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Sex - including: Transgender, and Pregnancy / Maternity	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Race	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Religion / belief	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Sexual orientation – including: Marriage / Civil Partnership	<input type="checkbox"/>	<input checked="" type="checkbox"/>

4. **Apart from those with protected characteristics, which other groups in society might this document be particularly relevant to...** (e.g. those affected by homelessness, bariatric patients, end of life patients, those with carers etc.)?

None

5. **Do you think the document meets our human rights obligations?**

Feel free to expand on any human rights considerations in question 6 below.

A quick guide to human rights:
<ul style="list-style-type: none"> • Fairness – how have you made sure it treat everyone justly? • Respect – how have you made sure it respects everyone as a person? • Equality – how does it give everyone an equal chance to get whatever it is offering? • Dignity – have you made sure it treats everyone with dignity? • Autonomy – Does it enable people to make decisions for themselves?

6. **Looking back at questions 3, 4 and 5, can you summarise what has been done during the production of this document and your consultation process to support our equality / human rights / inclusion commitments?**

The application guidance has been amended to ensure that patient communication needs are taken into consideration. Applications can be made in writing, through the MYCARE Patient Portal, by phone or with support from PALS.
--

7. **If you have noted any ‘missed opportunities’, or perhaps noted that there remains some concern about a potentially negative impact please note this below and how this will be monitored/addressed.**

“Protected characteristic”:	
Issue:	
How is this going to be monitored/ addressed in the future:	
Group that will be responsible for ensuring this carried out:	