TRUST POLICY FOR ACCESS TO PERSONAL DATA (SUBJECT ACCESS)

Reference Number POL-RM/1721/24	**Version:** V6		**Status** Final	**Author:** Lisa Vaughan **Job Title: Deputy Head Health Records**
Version / Amendment History	**Version**	**Date**	**Author**	**Reason**
	V2	2010	Head of Records Management	Reformat plus minor amendments
	V2.1	March 2014	Deputy Case note Services Manager	Review and minor amendments
	V3	Sept 2015	Information Governance Manager / Case note Services Assistant General Manager	Change from health records to include all personal data, including change to title
	V4	May 2018	Assistant General Manager, Health Records	To include GDPR changes
	V4.2	July 2018	Assistant General Manager, Health Records	Minor changes to reflect Trust merger
	V5	July 2021	Service Manager, Health Records	Minor changes to reflect team merger
	V6	August 2024	Deputy Head Health Records	Re written
Intended Recipients: This Policy applies to all Trust staff involved in processing requests for access to personal information				
Training and Dissemination: Via intranet and localised training				
To be read in conjunction with: • Data Protection and Confidentiality (Dealing with Confidential Information) - Trust Policy and Procedure • Information Governance - Trust Policy and Procedure				
In consultation with and Date: Information Governance Steering Group : May 2021				
EIRA stage One Completed Yes Stage Two Completed No				
Approving Body and Date Approved			Trust Delivery Group November 2024	

Review Date and Frequency	August 2026
Contact for Review	Deputy Head Health Records
Executive Lead Signature	Executive Chief Digital Information Officer
Approving Executive Signature	Executive Chief Digital Information Officer

Content Page

1. Introduction

Individuals have the right under current data protection legislation subject to certain exemptions, to have access to their personal records that are held by University Hospitals of Derby & Burton NHS Foundation Trust (UHDB).

This is known as a 'subject access request' (SAR). Requests may be received from members of staff, service users or any other individuals who the Trust has had dealings with and holds data about that individual. This will include information held both electronically and manually and will therefore include personal information recorded within electronic systems, spreadsheets, databases or word documents and may also be in the form of photographs, x-rays, audio recordings and CCTV images etc.

All SAR requests received must be forwarded to the subject access team.

Access to records of the deceased is still governed by the Access to Health Records Act 1990.

2. Purpose

The purpose of this policy is to inform staff on, how to advise service users on how to make a subject access request, how to recognise a subject access request and know what action to take on receipt.

A subject access request (SAR) is request made by or on behalf of an individual for the information about them, which is held by the Trust. This request does not need to be in any particular format and does not need to mention that it is a subject access request. Data Protection Legislation entitles all individuals to make requests for their own personal data.

An individual is not entitled to information relating to other people (unless they are acting on behalf of that person), appropriate proof of their entitlement to act on behalf of that individual must be provided, but the right of access remains that of the data subject

3. Scope of the Policy

The policy applies to all employees and must be followed by all those who work for the organisation, including those on temporary or honorary contracts, secondments, pool staff, contractors and students.

The Trust has a legal obligation under current Data Protection Legislation including ensuring compliance with individual's right of access to personal information held by the Trust, therefore breach of this policy will be regarded as serious misconduct and may result in:

- dismissal;

- termination of secondment for secondees and a request for their employer to apply their internal disciplinary procedures;

- termination of contracts for interim resources, temporary workers, agency workers and/or contractors; and

- legal action being taken against the discloser and/or any other third party

4. Definitions/Explanation of Terms

Person-identifiable information is anything that contains the means to identify a person, e.g., name, address, postcode, date of birth, NHS number, National Insurance number, pseudonymised data, biometric and genetic data, and online identifiers and location data, etc. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition.

4.1 Special Category Data

Special category data includes, Health Data, Trade Union membership, Political opinions, Religious or philosophical beliefs, Racial or Ethnic Origin, Sex life and sexual orientation, Biometric Data and Genetic Data.

5. Key Responsibilities / Duties

The Assistant Director of Systems & Integration has overall responsibility for the implementation of this Policy.

The management and co-ordination of Subject Access Requests is delegated to the following:

Head of Health Records will:

- Ensure a central register is maintained of all Subject Access Requests received by the Trust
- Ensure requests are responded to correctly in accordance with statutory requirements
- Act as a reference point for procedure and complaints
- Monitor compliance and ensure effectiveness with Policy and guidelines
- Be responsible for the timely provision of data held within the Trust's health records

Head of Workforce Management will be responsible for the timely provision and redaction of any type of personal data retained in relation to employment.

Head of Patient Advice & Liaison (PALs) will be responsible for the timely provision and redaction of personal data held in connection with either the formal NHS complaints process or informal PALS concerns.

Head of Occupational Health will ensure that requests for the provision and redaction of Occupational Health records are processed within the agreed timescales.

UHDB Security Manager will ensure that requests for the provision of CCTV are processed and redacted within the agreed timescales.

Imaging Department will ensure that requests for the provision of copy imaging are processed within the agreed timescales.

Information Governance Steering Group will receive and consider quarterly reports on the Trust's compliance in this area.

Health Professionals will conduct assessments as requested by the SAR case handler, and respond within the stipulated timescale.

All Staff will ensure that they provide and redact where appropriate information as requested and within the timescales.

6 How to recognise a Subject Access Request

A subject access request (SAR) is made by or on behalf of an individual for the information about them, which is held by the Trust.

A request does not need to be in any particular format and does not need to mention that it is a subject access request or the Data Protection Act. It may be made in writing (This may be by letter, email, or even social media, such as Facebook or twitter). The request may be made verbally, where this occurs a record of the request must be made detailing the information requested, the date requested and by whom.

Proof of identity of the applicant and/or the applicant's representative, and proof of right of access to the data subject's personal information, by reasonable means must be obtained.

The request must contain sufficient information to be able to locate the record or information requested.

All requests must be responded to without delay and at the latest within one calendar month of receipt of the request, the one calendar month starts on the receipt of appropriate proof of identity. This time can be extended by a further 2 months where requests are complex or numerous. However, if this is the case we must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

If the request relates to, or includes information that should not be requested by means of a SAR (e.g. it includes a request for non-personal information) then, the request must be treated accordingly, e.g. as a Freedom of Information (FOI) request where purely non-personal data is being sought or as two requests: one for the requester’s personal data made under Data Protection Legislation; and another for the remaining, nonpersonal information made under FOI Legislation. If any of the non-personal information is environmental, this should be considered as a request made under the Environmental Information Regulations (EIR).

7 Assisting and advising services users in making a request

Where an individual is verbally making a request:

Make a written record of the request, detailing the information being requested and from which service to enable its location and verify with the requestor that the written record is correct.

Requesters do not have to advise of their reason for making the request or what they intend to do with the information requested, although it may help to find the relevant information if they do explain the purpose of the request.

Note some requestors may require additional assistance and therefore details might have to be supplied in an alternative accessible format, e.g., braille. Applicants can be referred to the Patient Advice & Liaison Team to obtain appropriate assistance in making their application.

Obtain the requestors contact details, proof of identity and details on how they would like the response to the application to be returned to them. Note that responses to requests

should be made in a format requested by the requestor, therefore alternative formats may be needed e.g., braille.

Data Protection Legislation does not introduce an exemption for requests that relate to large amounts of data, however it may be possible to consider whether the request is manifestly unfounded or excessive.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we can:

a) Charge a reasonable fee taking into account the administrative costs of providing the information; or

b) Refuse to respond. Where we refuse to respond we must explain the reason for the refusal to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

Responses to SAR requests must be returned by a secure methodology, such as the NHS Mail Secure service i.e., social media must NOT be used to return information requested.

8 Requests on behalf of other individuals General Third Party

A third party, e.g., solicitor or relative may make a valid SAR on behalf of an individual. However, where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individual's consent or evidence of a legal right to act on behalf of that individual e.g., power of attorney must be provided by the third party.

If we think an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, we may send the response directly to the individual who is the subject of the SAR rather than to the third party and inform the third party that the information has been sent directly to the data subject.

The individual may then choose to share the information with the third party after having had a chance to review it.

9 Requests on Behalf of Children

Even if a child is too young to understand the implications of subject access rights, information about them is still their personal information and does not belong to anyone else, such as a parent or guardian. So, it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a SAR for information held about a child, we should consider whether the child is mature enough to understand their rights. If the clinician responsible for the child’s treatment plan is confident that the child has the capacity to understand their rights and any implications of the disclosure of information, then the child’s permission should be sought to action the request.

The Information Commissioner has indicated that in most cases it would be reasonable to assume that any child that is aged 12 years or more would have the capacity to make a subject access request and should therefore be consulted in respect of requests made on their behalf.

The Caldicott Guardian or their nominated representative should also be consulted on whether there is any additional duty of confidence owed to the child or young person as it

does not follow that, just because a child has capacity to make a SAR, that they also have capacity to consent to sharing their personal information with others as they may still not fully understand the implications of doing so.

What matters is that the child is able to understand (in broad terms) what it means to make a SAR and how to interpret the information they receive as a result of doing so. When considering borderline cases, the following should be taken into account:

• Where possible, the child's level of maturity and their ability to make decisions like this.

• The nature of the personal data.

• Any court orders relating to parental access or responsibility that may apply.

• Any duty of confidence owed to the child or young person.

• Any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment.

Any detriment to the child or young person if individuals with parental responsibility cannot access this information; and

Any views the child or young person has on whether their parents should have access to information about them.

10 Requests in respect of Crime and Taxation e.g., from the Police or HMRC

Requests for personal information may be made by the above authorities for the following purposes:

• The prevention or detection of crime.

• The capture or prosecution of offenders; and

• The assessment or collection of tax or duty.

A formal documented request signed by a senior officer from the relevant authority is required before proceeding with the request. This request must make it clear that one of the above purposes is being investigated and that not receiving the information would prejudice the investigation.

These types of requests must be considered by a senior manager and the decision on whether to share the information or not must be documented before any action is taken. Advice can be sought from the Information Governance Team.

11 Court Orders

Any Court Order requiring the supply of personal information about an individual must be complied with. If the order is unclear, for example whether the court requires the information in a redacted or unredacted form, it is reasonable to check this with the court prior to disclosure

12. Access to Personal Records

12.1 Informal access to health records

The Trust encourages informal, voluntary arrangements whereby patients or those caring for them, during or at the end of their treatment, are able to ask what has been recorded about them during that episode of care. Access is allowed to this part of the health record at the discretion of the appropriate health professional but is still subject to safeguards and exemptions.

In these cases, the Trust will have no formal record that access has taken place other than an entry that must be made as standard on either the clinical sheets or the nursing notes.

12.2 Formal access to health records

If a patient (or their representative) asks the Trust to provide them with access to their health records in compliance with legislation then the following points must be noted:

(i) The individual has a right to receive a copy of the record, and to be given an explanation of any terms which are required to make them intelligible

(ii) The right of access is to records made at any time.

12.3 Employment records

If an employee asks for informal access to their locally held employment records this can be actioned and approved by their Line Manager but is still subject to safeguards and exemptions.

If formal access to centrally held employment records is requested the following points must be noted:

(i) The individual has a right to inspect and to receive a copy of the record, and to be given an explanation of any terms which are required to make them intelligible. The individual only has the right to view information about themselves and not that of a third party

(ii) The right of access is to records made at any time.

The request should be made to the Subject Access Team, but will then be processed through Workforce Management. The Caldicott Guardian will act as an independent arbitrator where necessary in order to ensure the process is professional, independent and transparent.

13 Copies of Trust emails

The requestor will be asked to narrow the scope of the request as much as possible by providing timeframes, keywords and identifiers for searches.

The Trust will not search for initials, as this is considered manifestly excessive. However, if it is obvious or known that a file labelled with the data subjects initials is held, this should be considered for disclosure.

The Trust will not provide emails that would be classed as business as usual or any emails that the data subject was copied into.

The Trust may not be able to provide information where there is an ongoing investigation or other negotiations (see exemptions below).

14 Fees

There is usually no fee for accessing personal records. Where requests are manifestly unfounded or excessive, in particular because of their repetitive nature, the Trust may charge a reasonable fee (taking into account administrative costs) or may refuse to act on the request.

15 Refusing a request & Exemptions

Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR.

Information may be exempt because of its nature or because of the effect its disclosure is likely to have. There are also other restrictions on disclosing information in response to a SAR, for example where this would involve disclosing information about another individual.

If an exemption applies, a request can be refused (wholly or partly). Not all of the exemptions apply in the same way, and each exemption should be considered carefully to see how it applies to a particular request.

For more information around exemptions see the Information Commissioners Office website. A guide to the data protection exemptions | ICO

You can also refuse to comply with a subject access request if it is:

• manifestly unfounded; or

• excessive.

Where it is decided to refuse a request, we must be very sure of the legal basis for doing so and advice should be taken from our Data Protection Officer.

The individual must be informed without undue delay and within one month of receipt of the request. We should inform the individual about:

• the reasons for the decision.

• their right to make a complaint to the ICO or another supervisory authority; and

• their ability to seek to enforce this right through a judicial remedy

We should also provide this information if you request a reasonable fee or need additional information to identify the individual.

We must ensure that we fully document the decision and the reasoning behind it in case of further challenges.

Information may be exempt from disclosure because of its nature or because of the effect its disclosure is likely to have. There are also other restrictions on disclosing information in response to a SAR. Exemptions should not routinely be relied upon or applied in a blanket fashion. Any exemption must be considered on a case-by-case basis. A guide to the data protection exemptions | ICO

16. Monitoring Compliance and Effectiveness

Monitoring Requirement :	The number of requests received and compliance with timescales as dictated by legislation.
Monitoring Method:	Reports will be presented to the Information Governance Steering Group
Report Prepared by:	Deputy Head, Health Records
Frequency of Report	Quarterly

17. References

	Date of publication / issue
Access to Health Records Act	01 November 1991
Data Protection Act	May 2018
General Data Protection Regulation	May 2018
Information Commissioners Office- a guide to data protection exemptions	September 2022