NHS
Bridgewater
Community Healthcare
NHS Foundation Trust

Subject Access/Access to Health Records Policy

Policy Number	**IG/Pol/011**
Target Audience	**All Staff including Bank, Temporary, Learners in Practice and Contractors**
Lead Executive	**Chief Nurse**
Recommending Committee/Group	**DIGIT**
Approving Committee	**Corporate Clinical Policy Group**
Ratifying Committee	**Trust Board**
Date First Approved	**May 2018**
Last Full Review Date	**December 2022**
Next Full Review Date	**December 2024**
Policy Author	**Senior Information Governance Officer**
Version Number	**3.0**

Applicable Statutory, Legal or National Best Practice Requirements	Access to Health Records Act 1990 c.23 Access to Medical Reports Act 1988 c.28 Children's Act 2004 c.11 Data Protection Act 2018 Chapter 3 c.45 Department of Health (2003) NHS Code of Practice Confidentiality Freedom of Information Act 2000 c.14 Gender Recognition Act 2004 Information Commissioners Office (ICO) (2017) Subject Access Code of Practice version1.2 NHS England (2022) Access to health records and care records of deceased people Records Management Code of Practice for Health and Social Care (2016) UK General Data Protection Regulation c.15

The Trust is committed to an environment that promotes equality, embraces diversity, and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the Trust's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Version Control Sheet

Version	Date	Reviewed By	Comment
1	Feb 2018 May 2018 May 2018 May 2018	Jan McCartney Policy Approval Group J. McCartney S. Arkwright	New document combining IG/Pol/008 and IG/Proc/002 Approved subject to amendments and chair approval Amendments completed Approved by chair action
2.0	March 21 June 21 June 21 June 21	Jackie McKay Corporate Clinical Policy Group J. McKay S. Arkwright	Reviewed Approved subject to minor amendments and final chair approval. Amendments completed Approved by chair action
2.1	Oct 2022	J McKay	Full review
2.2	Oct 2022	DIGIT	Sign-off confirmed
2.3	Nov 2022	M. Corkery	Reviewed, comments made
2.4	12th December 2022	Corporate Clinical Policy Group	Approved subject to minor amendments, final chair approval and ratification by the Board
2.5	December 2022	J. McKay	Amendments completed
2.6	20th January 23	Jimmy Cheung	Amendments approved by chair action
3.0	27th January 23	Trust Board	Ratified

Equality impact assessment

Consider if this document impacts/potentially impacts:

- Staff
- Patients
- Family members
- Carers
- Communities

Yes [ ] **complete box A**	**No** [x] **complete box B**
Box A Contact the Trust's equality & inclusion manager at: **Email: ruth.besford@nhs.net** **Date contacted:**	**Box B** Complete details below: **Name: Jackie McKay** **Email: jacquelinemckay@nhs.net** **Date: 15th November 2022**

Education & Professional Development Question

In order to ensure that any training requirements are discussed, and resources planned and allocated to meet the needs of the service, you must consider whether this document has additional training requirements.

Please answer the following question by entering a cross in the box below:

	Yes	**No**
Does this document have any additional training requirements or implications?		No

Contents

1 Introduction

As Data Controller, Bridgewater Community Healthcare NHS Foundation Trust (hereafter the Trust) processes personal data about patients (health records) and staff. It also holds records of deceased patients and staff.

Such persons are entitled to certain rights under the Data Protection Act (DPA, 2018) and the UK General Data Protection Regulation (UKGDPR) to view and/or obtain a copy of all personal data that the Data Controller holds about them.

A request for information relating to a living individual is known as a Subject Access request (SAR) under UKGDPR and DPA 2018 and requests for information related to deceased persons are made under the Access to Health Records (1990).

This policy applies to all requests received from patients and staff for access to personal data which the Trust holds about them regardless of the format in which that data is held in. It also applies to requests received from individuals requesting access to personal data of the deceased.

Failure to comply with the SAR in relation to time and or access to the information will be reported through the Trust risk management reporting system (Ulysses).

1.1 Objective

The purpose of this policy is to set out how the Trust will support the exercise of the rights of access and ensure that staff are aware of their responsibilities in recognising, handling, and processing SARs and requests for deceased persons. It is expected that the service will make a written process to support this policy, which includes retaining a log of all information shared and within what time frame.

1.2 Scope

This policy applies to Trust staff, including bank, temporary, learners in practice and contractors.

2 Definitions

The definitions applicable to this document are as follows:

Data Controller	A person (organisation) who determines the purposes for which and the manner in which personal data, is processed.
Data processor	A processor is responsible for processing personal data on behalf of a controller.
Data subject	An individual who is the subject of the information (service user or staff member).

Health records	A health record is a record consisting of information relating to the physical or mental health or condition of an identified individual made by or on behalf of a health professional in connection with the care of that individual. A Health Record may be recorded in computerised or manual form or in a combination of both. It may include handwritten clinical notes, letters, laboratory reports, radiography and other images i.e. X-rays, photographs, videos and tape recordings.
Subject access rights	Under DPA 2018 and UKGDPR, the data subject to have the right to access to their own personal data.
Third party	A person identified in the health record other than the data subject, or a professional involved with the care. For example, health professional, social worker.
Redact/redacting/redaction	To remove third party data before releasing information. The notes should be printed then third-party information should be redacted by crossing out all the letters and going over with a black marker pen, then photocopying.
Service users personal representative	Defined as the executor or administrator of the deceased estate or where a data subject has consented for someone to act on their behalf.
Caldicott Guardian	The Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. This is a statutory requirement for all public bodies exercising functions that relate to the health service, adult social care or adult carer support in England and which handle confidential information about patients. The Trusts Caldicott Guardian is the chief nurse.
Statutory gateway	Permits disclosure of information by using certain exemptions set out in DPA Schedule 2.

Access to Health Records Act 1990	The Access to Health Records Act (AHRA, 1990) provides certain individuals with a right of access to the health records of a deceased individual. Individuals other than the personal representative have a legal right of access under the Act only where they can establish a claim arising from a patient's death.
United Kingdom General Data Protection Regulation (UKGDPR)	UKGDPR formerly GDPR 2018 is a regulation by which the European Parliament, the Council of the European Union and the European Commission strengthened to unify data protection for all individuals within the European Union (EU). The 'UK GDPR' sits alongside an amended version of the DPA 2018.
Adequacy decision	An adequacy decision permits a cross-border data transfer outside the EU, or onward transfer from or to a party outside the EU without further authorisation from a national supervisory authority. Now that the UK has exited the EU, the UK can no longer process a European individual's data without being granted an adequacy decision by the EU.
Freedom of Information Act (FOIA) 2000	An Act to make provision for the disclosure of information held by public authorities. Personal data of the applicant is exempt under section 40(1) of the FOIA 2000; these requests will instead be dealt with as a SAR under the UK General Data Protection Regulations UKGDPR. Personal data of another person is exempt under section 40(2) of the FOIA 2000 if disclosure would breach one of the General Data Protection Regulations principles. In the case of the deceased, there are limited alternative rights under the Access to Health Records Act 1990.
Access to Medical Reports Act 1988	An Act to make provision for the individual to access medical reports written by a health professional for the provision of a service.
Non-health records	This could be a Human Resource (HR) record.

Parental responsibly	Parental responsibility is defined in the Children Act 1998 as 'all the rights, duties, powers, responsibilities and authority which by law a parent of a child has in relation to the child and his property. A person with parental responsibility is defined in law and by reference to the circumstances of each child and any legal proceedings or lawful processes affecting persons who may be in a parent role for that child.
Personal data	Data that can identify an individual for example, name, address, date of birth (DOB). To process personal data there needs to be a legal basis under Article 6 of the UKGDPR.
Special category data	Special category data is personal data that needs more protection because it is sensitive. To process special category data there needs to be a legal basis under Article 6 and under Article 9 of the UKGDPR.
Gender Recognition Act 2004	Legal framework by which people can change their legal gender. Provides particular protection for consent to disclosure of gender recognition certificate and restriction and access to records.
One month to respond to a request	You must comply with a SAR without undue delay and at the latest within one month of receiving the request. An incident should be raised via the online Risk Management Reporting System (Ulysses) for SARs that breach this deadline.
Information Society Service (ISS)	This covers most online services including websites, apps, search engines, online market places and online content services such as on-demand music, gaming and video services and downloads. It does not include traditional television or radio transmissions that are provided via general broadcast rather than at the request of an individual.
Grant of Probate or Letters of Administration	The Letters of Administration grant the legal authority for an Administrator to manage and distribute the deceased estate. Collectively a Grant of Probate and Letters of Administration are called Grants of Representation.

3 Abbreviations

The abbreviations applicable to this document are as follows:

SAR	Subject Access Request
UKGDPR	United Kingdom General Data Protection Regulation
FOI	Freedom of Information
FOIA	Freedom of Information Act
HR	Human Resources
ICT	Information and Communication Technology
ID	Identification
ICO	Information Commissioners Office
AHRA	Access to Health Records Act
DIGIT	Digital, Information Governance and Information Technology Group
EU	European Union
LNCSOP	Local Non-Clinical Standard Operating Procedure
IT	Information Technology
DSPT	Data Security and Protection Toolkit
ISS	Information Society Service
DOB	Date of Birth
DPO	Data Protection Officer
EPR	Electronic Patient Record
IG	Information Governance
CQC	Care Quality Commission
GM	General Medical Council
NMC	Nursing and Midwifery Council

4 Other Relevant Procedural Documents

This document should be read in conjunction with the following documents:

Information Governance Framework Policy

Data Protection and Confidentiality Policy

Freedom of Information and Environment Information Regulations Policy

Health Records Policy

Acceptable use (IT) Policy

Incident Reporting Policy

Risk Management Framework

Records Management, Archiving, Retention and Disposal Policy

Bridgewater Patient Privacy Notice

Bridgwater Children's Privacy Notice

Bridgewater Staff Privacy Notice

Equality and Diversity Policy

Mandatory Training and Induction Policy

Language Interpretation Policy

Reasonable Adjustments for Patients Policy

Safeguarding Children Policy

Safeguarding Adults Policy

Corporate Records (including Document Management) Policy

Equal Opportunities Policy

Policy and Procedure for the Development and Review of Policy and Procedural Documents

5 Roles and Responsibilities

5.1 Chief Executive Officer

The Chief Executive as the Accountable Officer has ultimate responsibility for this policy and ensures that the Trust complies with Government Legislation and with its responsibilities as a Data Controller under the UK GDPR.

5.2 Senior Information Risk Owner

The SIRO is the Board member who has overall responsibility for Information Risks within the Trust.

The SIRO will report to the Quality and Safety Committee on information risks. The SIRO in the Trust is the Director of Finance. The Deputy SIRO is Assistant Director of Information Technology (IT).

5.3 Data Protection Officer

The Data Protection Officer (DPO) has responsibility for informing and advising and monitoring compliance with data protection principles. The DPO for the Trust is held by the Trust Secretary. The DPO manages legal claims or potential legal claims from patients and should be informed if a SAR is part of a litigation claim against the Trust.

With the support of their office, the DPO will:

- Provide advice to the organisation and its employees on compliance obligations with data protection law
- Advise on when data protection impact assessments are required
- Monitor compliance with data protection law and organisational policies in relation to data protection law
- Co-operate with, and be the first point of contact for the Information Commissioner
- Be the first point of contact within the organisation for all data protection matters
- Be available to be contacted directly by data subjects
- Take into account information risk when performing the above
- Will be the key contact in the event of a data breach.

5.4 Caldicott Guardian

The Caldicott Guardian is the Board Member who has responsibility for overseeing the implementation of the laws that govern personal information and ensuring that good practice in relation to access and reuse is implemented within the Trust.

The Caldicott Guardian is the Trust champion in respect of the Caldicott Principles and as such is obligated to always make Caldicott decisions in the best interests of the patient. The Caldicott Guardian is the chief nurse. The deputy Caldicott Guardian is the deputy chief nurse.

5.5 Information Governance and Records Manager

The Information Governance (IG) and Records Manager is responsible for:

- Ensuring this policy and the processes to ensure compliance are in place
- Providing the Trust with IG expertise
- Supporting the Caldicott Guardian and SIRO with the management of risk and identified or potential threats to person identifiable information.

5.6 Director of People and Organisational Development

The Director of People and Organisational Development is responsible for ensuring there is a robust HR process for dealing with employee SARs.

5.7 Operational Managers/Departments Managers

Operational Managers and Department Managers will:

- Ensure their service/department has a procedure in place that instructs their staff on how to handle a SAR
- Understand how to records SARs on the appropriate SAR clinical system
- Monitor the SARs that come into their service/department and provide a second pair of eyes, usually another clinician to review copies of records before they are released to the requester
- Ensure staff are allowed time to participate in and complete designated mandatory Data Security Awareness Level 1 training
- Report non-compliance with this policy through the Trust risk management reporting system (Ulysses) and fully cooperate with any subsequent investigation.

5.8 All Staff

It is the responsibility of all staff to:

- Adhere to this policy
- Record the SAR onto the clinical system if it allows.
- To know where to access further support and SAR templates on the Hub
- Complete annual Data Security Awareness mandatory training
- Escalate to their manager/team leader any part of the document that is identified to be no longer relevant, requires revision or may present as a risk to patient or staff safety
- Access the most up to date document on the intranet
- Identify and make any specific requirements for the patient/family/carer, taking into consideration disability, language and cultural needs are identified.

5.9 Digital, Information Governance and Information Technology Group

The Digital, Information Governance, and Information Technology (DIGIT) group will:

- Review systems for SAR accessibility.

6 Equipment

SAR Template log

Printer

Photocopier

Black marker pen

Electronic Patient Record (EPR) system

7 Accessing own health, staff record or family member

Staff must submit a SAR verbally or in writing to the relevant service/department or email bchft.accesstorecords@nhs.net if they wish to access their health or staff record, or that of a family member.

Under no circumstances should a staff member access a record, even their own, without a legitimate purpose stated in Data Protection Act 2018 and UKGDPR.

8 Subject access requests

8.1 Living individuals

The Trust expects all departments and clinical services that handle SARs to have a documented local non-clinical standard operating procedure (LNCSOP) in place.

The Trust must comply with a SAR without undue delay and at the latest within one month of receiving the request. If the Trust breaches the deadline of one month, an incident must be raised using the online risk management reporting system (Ulysses), stating why it has breached the deadline.

The Trust can extend the time to respond by a further two months if the request is complex or the Trust has received a number of requests from the individual, e.g., other types of requests relating to individuals' rights.

The Trust will accept a request verbally or in writing, including emails and text messages from a data subject in the provision of subject access to health records or non-health records, e.g., HR records.

The Trust will make a standard access form available on the Trust website to the public to assist service users and on the Trust Intranet “The Hub” for staff. However, the data subject is not obliged to use the form. The request should be stored in the record, if a verbal request was made this should be added to the record.

As soon as a request is identified, staff must ensure that any routine data deletion or destruction processes are suspended with respect to the personal data of that individual. In addition, it is now a criminal offence to delete, destroy, alter or conceal personal data to frustrate a SAR (section 173 DPA 2018). Receipt of a SAR must be acknowledged within five working days of the request being received. The request should be acknowledged in the format received unless a preference is given.

The Trust will require applicants to provide proof of identity prior to access. Where an application is made on behalf of another service user, the Trust will confirm that the consent of the individual had been obtained prior to release.

Where an individual has not specified the information that they require, the Trust may ask the applicant to provide further information to refine the request.

Where an access request has previously been met and a subsequent identical or similar request is received, the Trust will assess if a reasonable time interval has elapsed before providing the information. This will vary depending on the type and frequency of contacts made with the data subject. Further advice can be obtained from the IG team.

The Trust can refuse to provide all, or part of the information were doing so would involve disproportionate effort. Where the request is disproportionate, the Trust should discuss with the requester and seek an amicable solution. Difficulties throughout the process (from finding, analysing, and providing the data) can be taken into account.

The Trust must be able to show that they have taken all reasonable steps to comply with the request and, as the Information Commissioners Office (ICO) Code notes, "*should be prepared to make extensive efforts to find and retrieve the requested information"* (ICO, 2017).

In addition, the Trust does not have to provide a person with a copy of their health and care records if it believes their SAR is "manifestly unfounded or excessive" or, should the Trust choose to respond, a reasonable fee can be charged for doing so.

SARs that fall into this category are likely to be repetitive (for example, regular requests for copies of records especially where there has been little or no change to the record since the previous request), aimed at disrupting the Trust or targeted against an individual.

Decisions about whether a SAR falls into this category must be taken on a case-by-case basis and staff should be able to justify your decision with evidence. ICO guidance on manifestly unfounded and excessive requests is available. Advice is always available on bchft.accesstorecords@nhs.net.

If the request is complex, the response time may be a maximum of three calendar months, starting from the day of receipt. Staff should be able to provide evidence of the time it will take. However, if part of the request can be provided it should be done so within the calendar month.

8.2 Exemptions

There are several exemptions that are set out under the Data Protection Act 2018 which allow information to be withheld from the individual that has made the request.

Some of the current exemptions include the following:

- It is believed disclosure of the information is likely to cause serious physical or mental harm to the individual or another person. If staff believe it is not of overall benefit to the patient to disclose their personal information or part of their personal information (and it is not required by law), they must seek advice from the IG team bchft.accesstorecords@nhs.net If staff decide not to disclose information, they must document in the patient's records their discussions and the reasons for deciding not to disclose. Staff must be able to justify their decision

- Confidential employment references provided by an employer in support of a person's application for employment are exempt from SARs

- Employers do not have to disclose information which relates to legal advice or legal proceedings as this is covered by legal professional privilege

- Personal data which relates to management information such as management forecasting.

8.3 Provision of copies/viewing health records

While we should disclose all information we hold, there may be information contained in the record that the DPA exempts us from disclosing. The health professional must consider whether it is appropriate to redact information prior to releasing copies of or viewing of health records.

For example:

- The names of the health professionals and social care professionals who have inputted into the care should be disclosed

- Third party information in the health record that is not the health or social care professional should be removed

- Information provided by another health professional or social care professional must remain, however, the health professional reviewing the record must consider whether it is appropriate to disclose the information and, if necessary, liaise with the individual who provided the information.

8.4 Assistance and support to the data subject

The service will, where required, make provision for a health care professional to respond to questions relating to any medical terminology in the health record during viewing or following release of copies.

On occasions, it may be suitable to arrange to sit with an individual and go through the record together; the service may provide a designated lay administrator to oversee the viewing of a health record where a health professional is not required.

Although the Trust discourages the use of some abbreviations, the health professional should include a list of abbreviations if the records contain abbreviations.

Support with understanding the record will be provided for data subjects where there is communication or information format needs related to disability or first language, for example, information in large print, signed or audio files, or translated information.

8.5 Children and young people under 18

Children have the same rights as adults over their personal data, even if a child is too young to understand the implications of their rights. Data about them is still their personal data and does not belong to anyone else, such as a parent or guardian. In the case of young children, these rights are likely to be exercised by those with parental responsibility for them.

Where an adult requests a child's data, proof of parental responsibility will be required. A note must be made on the health record stating these documents have been viewed, but there is no requirement to keep a copy of them and they should be confidentially destroyed.

Article 8 of the UK GDPR sets the age at which children can consent to the processing of their personal data in the context if offering an information society service (ISS) at **13 years old**. The Trust must respect the UK age limit when processing the personal data of UK based children.

A child who is capable of making a SAR can also ask someone to act on their behalf in the same way that that an adult can. For children who are not of sufficient age, maturity, or ability to make a request and for such children only, a person with parental responsibility can make a SAR. Where a child is competent, they are entitled to make or consent to a SAR to access their record.

9 Deceased individuals

When a patient or service user dies, staff may be asked for a copy of, or access to, their record. A family member, for example, might ask to see the record. These requests must be considered carefully. However, it is usually possible to agree to such requests in the appropriate circumstances

Access to Health Records Act 1990 regulates the processing, including the disclosure, of information about identifiable individuals that are deceased. The Access to Health Records Act 1990 states that only two groups of people may access the patient's health records:

- The executor has first rights to the patient's records, but if no executor was named, the patient's spouse or adult child can become the deceased personal representative

- Anyone with a claim arising out of the patient's death.

Evidence that an individual has the status of personal representative is required. This must be a letter of appointment from a probate court.

A note must be made on the record stating these documents have been viewed, but there is no requirement to keep a copy of them and they should be confidentially destroyed.

The personal representative for example, a spouse, need not give a reason for applying for access to a record. However, prior to releasing the record to the personal representative a health professional must go through the record to ensure the patient has not added a statement with instructions not to disclose all or part of the record to an individual.

Individuals, other than the personal representative, have a legal right of access under the Access to Health Records Act 1990 only where they can establish a claim arising from a patient's death. Their right is restricted to information "relevant to the claim". The decision as to whether a claim actually exists lies with the record holder. In cases where it is not clear whether a claim arises the Trust will seek legal advice.

If no entries, additions or amendments have been made to the record in the 40 calendar days prior to the date of application, we have 21 calendar days from the date of receiving the request to either grant or refuse the request to access the deceased person's record.

The Trust will require applicants to provide proof of identity prior to access, unless the individual picks the records up in person and their identification (ID) can be verified without ID.

There is no equivalent right of access to social care records, any input to the record by a social worker should be removed.

A deceased individual must be afforded confidentiality under the Common Law of Duty. Therefore, before disclosing records or any information about a deceased individual, staff must consider:

- If they are aware of any wishes (written or verbal) of the deceased individual relating to their information being shared
- If there is anything in the record which would either cause distress to the family or benefit them to know
- If there is any third-party information in the record, for example, information about other family members
- If there is anything in the record which if disclosed might cause harm to another person
- To explain any clinical abbreviations or terminology in the record, to help the person who has asked for a copy of the record understand it.

Requests to access records following an individual's death can be complex. It is important to consider each request on a case-by-case basis.

Requests may be made using the wrong terminology or legislation, such as asking for access under UK GDPR (General Data Protection Regulation) or the FOIA 2000 or may not mention any legislation. In these situations, staff should contact the requester to advise them about the correct process to apply for access and support them to follow this. Staff should not refuse the request outright because the requester has used the wrong legislation or access route.

For organisations subject to the FOIA, if a request is made but there is no legal right of access, they may need to issue a refusal notice, citing the appropriate exemptions under the FOIA.

9.1 Types of requests

Coroner - Coroners (or their offices) have a legal right to access the records or to other documents including reports internally and externally, of a deceased individual to support their inquests. The Trust must provide the information requested by the coroner.

Medical examiner – for example General Medical Council (GMC) and Nursing and Midwifery Council (NMC) may request the records of deceased people for independent scrutiny. There is a legal basis for health and care organisations to share relevant confidential patient information with medical examiners. This is covered by a section 251 approval following an application to the Confidentiality Advisory Group by NHS England.

Care Quality Commission (CQC) – the CQC has a legal right to access the records of deceased people, where required during its investigations. The CQC Code on Confidential Patient Information provides further information.
A personal representative of the estate of the deceased (a person holding the Grant of Probate or Letters of Administration) can request access to a health record. For example, a personal representative may need information about the deceased's care in a nursing home.

If the request for access to the health record is made by a personal representative, staff must consider withholding information if:

- The deceased expressly indicated they did not want parts of their record to be disclosed
- The record, if disclosed, would be likely to cause serious harm to another person
- The record of the deceased refers to another individual (who is not a treating healthcare professional)
- The record contains information provided by the patient, or resulting from an examination or treatment, which staff have reason to believe the patient would have felt particularly sensitive about and would not have expected to be disclosed.

Someone who has a claim arising from the death of the deceased can also request access to the health records of the deceased. If they do not have the authorisation of the personal representative, staff should request evidence of the nature and basis for their claim, and they should only disclose information which is relevant to the claim.

Police - the police may request records of deceased people as part of their investigations. Staff may consult the IG team or a senior member of staff regarding disclosure to ensure there is a legal basis for any disclosure and that the information shared is relevant to and necessary for the stated purpose. In most cases, to make a disclosure, staff will need to be satisfied that the public interest served by disclosure outweighs the public interest served by protecting the confidentiality of the individual and the public interest served by providing a confidential service to the wider public. Staff can refuse a request from the police if they are not satisfied that disclosure is relevant or necessary for the stated purpose.

For requests for deceased personal identifiable information from individuals not covered in this policy, staff must contact the IG team:

bchft.accesstorecords@nhs.net

10 Application by Solicitors, Police, Insurances Companies

Where a legal, financial or other professional or company requests access on behalf of a client they are representing, they must provide the signed consent of their client. The request will be dealt with in the same way as if it had come direct from the requestor or nominated person.

The Trust will rely on the legal representative or insurance company to obtain proof of identity of their client. The Data Subject's signed consent will be required.

If there is a reasonable doubt about the validity of the consent, the request will not be processed until the Trust is satisfied that it is a valid request. Further advice can be obtained from the IG team.

Where a request is made by a person acting under a Power of Attorney, a copy of the signed and valid document creating the power will be required.

A request made by the Police can either be with consent from the patient, which will be handled in the usual way or to investigate or prevent a crime. Many police forces have standard forms (often referred to as DP7 or DP9 - and previously known as "Section 29 forms") for requesting personal or confidential patient information.

Although the use of these forms is not mandated, they are the recommended way to obtain the information needed to decide whether the information should be disclosure. If, however, organisations are satisfied that they have the information needed to make a disclosure decision without using the forms, they can proceed on that basis. A request should be provided in writing and signed by a senior officer (usually Inspector or above like a Chief Inspector, Superintendent or Chief Superintendent).

10.1 Disclosures in absence of a statutory requirement

The Trust will consider applications for access where there is no statutory requirement to comply on a case-by-case basis and with due consideration to the rights of the data subject. The Trust recognises that in all cases the public interest in disclosure must outweigh the duty of confidentiality owed to the deceased before any disclosure is approved.

10.2 Timeframe for compliance

To comply with the UKGDPR and the DPA 2018, the Trust must provide the information within one calendar month, following the UKGDPR and the DPA 2018 of one calendar month, or as soon as is possible within the given timeframe.

If the request is complex, the Trust may need extra time to consider a request and can take up to an extra two months to respond.

If the extension is required, the Trust should let the requester know within one month that they need more time and why.

10.3 Request log

The service must maintain a secure log of all SARs for health records and non-health records to make provision for corporate monitoring reports. A template log can be downloaded for the SAR page on the Hub.

10.4 Amendments to health records

The Trust recognises that an opinion or judgment recorded by a health professional, whether accurate or not, should not be deleted from a medical record.

Where a data subject requests amendments to information in a health record, a health professional will be consulted. Amendments will be made where both parties agree but the original information will be left visible. A written explanation must be added to the record with the date time and signature of the person authorising the amendment.

Where a health professional considers disputed information to be accurate, the Trust will ensure that a note recording the service user's disagreement is added to the record. Information may only be deleted from a health record with the express permission of the Caldicott Guardian.

10.5 Service users living abroad

The Trust will provide previous service users who have left the UK with rights of access under UKGDPR, where the records of treatment are still held by the Trust. Extra security measure such as encryption and safe haven solutions to protect the information when being transferred should be put in place. Staff should contact the IG team if they are asked to transfer personal data outside the UK.

10.6 Freedom of Information Act 2000

The Trust will consider any requests for information which constitutes personal information to be exempt from disclosure under the FOIA 2000 if:

- Disclosure would contravene Data Protection Act 2018 principles
- Where information has been provided in confidence
- Where a duty of confidentially is owed to the deceased.

10.7 Access to Medical Reports Act 1988

The Trust will consider applications to view insurance or employment Medical Reports with regard to the Access to Medical Reports Act 1988.

10.8 Fees

The Trust will not charge for complying with a SAR unless the request is 'manifestly unfounded or excessive.' The Trust may charge a reasonable administrative-cost fee if further copies are requested.

Excessive requests: if a request is 'manifestly unfounded or excessive the Trust can charge a fee or refuse to respond but will need to be able to provide evidence of how the conclusion that the request is manifestly unfounded or excessive was reached.

Electronic access: it must be possible to make requests electronically (e.g., by email). Where a request is made electronically, the information should be provided in a commonly used electronic form, unless otherwise requested by the individual.

10.9 Emails

Employees often request access to personal data about them contained within e-mails between third parties (e.g., other employees and managers).

To determine whether these e-mails contain personal data about the requesting employee, the Trusts IT department need to conduct key word searches of the e-mail platform. This will typically throw up thousands of search results that require sifting through to determine whether or not the results returned include "personal data" about the requesting employee and, if so, whether an exemption from disclosure could be applied.

This problem can be substantially mitigated by the use of sensible data retention for emails. A Trust that retains ten years' worth of e-mail data will have substantially more emails to sift through than one that retains only a single year's worth of emails.

The Trust stance is emails should be kept for no longer than 12 months.

10.10 Employee subject access requests

How the Trust manages the employment records plays a huge part in dealing with an employee SAR successfully. The HR department will have a process for employee SARs including:

- Having a list of the type of documents that are likely to be held in a HR record along with the retention periods and which staff can access
- Auditing the HR record regularly to ensure its contents are appropriate for a HR record
- Signposting staff for Occupational Health SARs.

There should be no surprises for the employee when they submit a SAR.

11 Ensuring the information is provided securely

Health information and employment information is special category data under GDPR article 9 and should be subject to extra security measures when being sent to the requester.

- Staff must first establish the requesters' identity
- Staff must add [SECURE] to the subject box of the email when sending information securely to the requester.
- To post the information securely to the requester, staff must ensure:
    - They have enclosed a covering letter
    - The envelope displays a return address
    - The envelope is marked 'Private & Confidential'
    - The envelope is sealed appropriately
    - The envelope is posted using recorded delivery in order that its delivery can be tracked.
- The patient or staff member may ask to collect the information by hand, in which case, ID must be asked for.

Appropriate ID is any of the usual documents, such as password, utility bill with their address on. If this is not available, it is reasonable for staff to ask the data subject a series of questions only the individual would know the answers to.

12 Consultation

Key individuals/groups involved in the development of the document to ensure it is fit for purpose once approved.

Name	Designation
Mary Corkery	Policy Officer
Jim Eatwell/Kristina Brayford West/Sara Wilson	Safeguarding collated response
Ruth Besford	Equality and Inclusion Manager
Digital, Information Governance and Information Technology Group (DIGIT)	Membership comments Jan McCartney Sharon Ormesher Sandra Alderson

Name	Designation
Corporate Clinical Policy Group	
Trust Board	

13 Dissemination and implementation

13.1 Dissemination

The senior IG officer will disseminate this policy to associate borough directors for disseminating to managers and onward dissemination to staff.

The policy will be made available on the Trust Intranet (the Hub) and published in the team brief.

13.2 Implementation

Managers will ensure this policy is followed by all staff.

All Trust staff will be made aware of their personal and organisational responsibilities regarding health records through the Trust health records training program and local induction and monitoring audits.

Instruction and direction will be provided via a number of sources, including:

- LNCSOPs
- Annual mandatory training
- Policies and procedures
- Staff bulletin
- Team brief
- Team meetings and via line manager
- Corporate emails.

New employees will be made aware of this policy through the induction process.

14 Process for monitoring compliance and effectiveness

Process for reviewing compliance and effectiveness i.e., audit, review, survey, incident reporting	Responsible	Frequency of monitoring	Assurance group
Health record keeping audit program and the clinical audit programme Quality of information both for electronic and paper health records will be monitored through a suite of reporting channels, both internally and externally to the Trust. Examples of the monitoring requirements are relevant IG Toolkit, commissioning requested information both for performance and quality aspects and national and local clinical audits.	IG and Records Manager	Continuous	DIGIT

15 Standards/key performance indicators

Key Performance Indicator	Evidence Required	Frequency	Committee or responsible person
NHS Digital Data Protection and Security Toolkit (DSPT)	Number of SAR compliant in the time scale	Quarterly	DIGIT

16 References

Access to Health Records Act 1990 c.23 [online]. Available at: https://www.legislation.gov.uk/ukpga/1990/23/contents

Access to Medical Reports Act 1988 c.28 [online] Available at: https://www.legislation.gov.uk/ukpga/1988/28/contents

Children's Act 2004 c.11 [online] Available at: https://www.legislation.gov.uk/ukpga/2004/31/section/11

Data Protection Act 2018 Chapter 3 c.45 online] Available at: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Department of Health (2003) NHS Code of Practice Confidentiality [online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

Freedom of Information Act 2000 c.14 [online] Available at: https://www.legislation.gov.uk/ukpga/2000/36/contents

Gender Recognition Act 2004 c. 7 [online] Available at: https://www.legislation.gov.uk/ukpga/2004/7/contents

Information Commissioners Office (ICO) (2017) Subject Access Code of Practice version1.2 [online] Available at: https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf

NHS England (2022) Access to health records and care records of deceased people [online] Available at: https://transform.england.nhs.uk/information-governance/guidance/access-to-the-health-and-care-records-of-deceased-people/

Records Management Code of Practice for Health and Social Care (2016) [online] Available at: https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/

UK General Data Protection Regulation c.15 [online] Available at: https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/