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** |
| **Approving Committee** | **Corporate Clinical Policy Group** |
| **Date First Approved** | **May 2018** |
| **Last Full Review Date** | **June 2021** |
| **Next Full Review Date** | **June 2023** |
| **Policy Author** | **Senior Information Governance Officer** |
| **Version Number** | **2.0** |

| | |
|---|---|
| **Applicable Statutory, Legal or National Best Practice Requirements** | Access to Health Records Act (1990)<br>Access to Medical Reports Act (1988)<br>Data Protection Act (2018)<br>UK General Data Protection Regulation<br>Freedom of Information Act (2000)<br>Children's Act (1989)<br>Department of Health (2010) Guidance for Access to Health Records Requests<br>Information Commissioners Office (ICO) (2017) Subject Access Code of Practice<br>Records Management Code of Practice for Health and Social Care (2016)<br>Gender Recognition Act (2004) |

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<br><br>May 2018<br><br>May 2018<br>May 2018 | Jan McCartney<br><br>Policy Approval Group<br>J. McCartney<br>S. Arkwright | New document combining IG/Pol/008 and IG/Proc/002<br>Approved subject to amendments and chair approval<br>Amendments completed<br>Approved by chair action |
| 1.1 | March 21 | Jackie McKay | Reviewed |
| 1.2 | April 21 | M. Corkery<br>S Ramsdale<br>Halton Bronze Command | Comments made |
| 1.3 | April 21 | J. McKay | Updated following comments |
| 1.4 | April 21 | M. Corkery | Comments made |
| 1.5 | April 21 | J. McKay | Sent to Digit with no comments made.<br>Comments made by Halton Bronze Team. |
| 1.6 | June 21 | Corporate Clinical Policy Group | Approved subject to minor amendments and final chair approval. |
| 1.7 | June 21 | J. McKay | Amendments completed |
| 2.0 | June 21 | S. Arkwright | Approved by chair action |

| | | |
|---|---|---|
| **Does this policy impact/potentially impact on?**<br><br>• **Staff**<br>• **Patients**<br>• **Family Members**<br>• **Carers**<br>• **Communities** | **Yes** | **Please contact the Trust's Equality & Inclusion Manager at:**<br><br>**Email: ruth.besford@nhs.net** |
| | **No**<br><br>**x** | **Please sign and date below:**<br><br>**Name:**<br>**Email Address:**<br>**Date:** |

**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.

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 subject access request 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:

| | |
|---|---|
| The 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.<br><br>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 of the Data Subject to have the right to access to their own personal data. |
| 3rd 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.<br><br>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 European individual's data without being granted an Adequacy decision by the EU. |
| Freedom of Information Act (2000) | An Act to make provision for the disclosure of information held by Public Authorities.<br><br>Personal data of the applicant is exempt under section 40(1) of the Freedom of Information Act (2000); these requests will instead be dealt with as a Subject Access Request under the UK General Data Protection Regulations UKGDPR.<br><br>Personal data of another person is exempt under section 40(2) of the Freedom of Information Act (2000) if disclosure would breach one of the General Data Protection Regulations principles.<br><br>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.<br><br>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).<br><br>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.<br><br>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. |

# 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

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 |

## 4 Other Relevant Procedural Documents

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

Information Governance Policy

Data Protection 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

Making Adjustments for Patients with Disabilities and Language Needs Policy

Safeguarding Children Policy

Corporate Records (including Document Management) Policy

Equal Opportunities Policy

Freedom of Information and Environmental Information Regulation Policy

# 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 Senior Information Risk Owner (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 any subject access request 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 and Records Manager is responsible for ensuring that this policy and the processes to ensure compliance are in place. They provide the Trust with IG expertise and will support 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 Human Resources (HR) process for dealing with employee subject access requests.

### 5.7 Clinical Managers/Departments Managers

Clinical Managers and Department Managers will:

- Ensure their service/department has a procedure in place that instructs their staff on how to handle a subject access request
- Monitor the subject access requests 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
- To know where to access further support and SAR templates on the Hub

- Complete annual Data Security Awareness mandatory training
- Escalate to their Clinical 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:

- Monitor compliance with this policy on behalf of the Trust
- Report on the management and accountability arrangement for IG
- Provide assurance to the Board through the Trusts sub committees.

## 6 Equipment List

- SAR Template log
- Printer
- Photocopier
- Black Marker Pen

## 7 Accessing Own Health, Staff Record or Family Member

Staff must submit a subject access request verbally or in writing to the relevant service/department or email bchft.foi@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 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 subject access requests to have a documented procedure 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.

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 subject access request 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, unless the individual picks the records up in person and their identification can be verified without identification (ID). 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 subject access request is “manifestly unfounded or excessive” or, should the Trust choose to respond, a reasonable fee can be charged for doing so. Subject access requests 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 you 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.IG@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 your 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

The Trust will require the health professional to consider the following prior to releasing copies of or viewing of health records:

- Third party information in the health record that is not the health or social care professional is removed unless consent sought

- If it is reasonable to disclose without the consent of the health or social care professional party.

### 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.

A child who is capable of making a subject access request 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 subject access request. Where a child is competent, they are entitled to make or consent to a SAR to access their record. Children aged over 16 years are presumed to be competent.

Children under 16 in England, Wales and Northern Ireland must demonstrate that they have sufficient understanding of what is proposed in order to be entitled to make or consent to an SAR. In Scotland, a person aged 12 or over is presumed to be of sufficient age and maturity to be able to exercise their data protection rights, unless the contrary is shown. This presumption does not apply in England and Wales or in Northern Ireland, where competence is assessed depending upon the level of understanding of the child, but it does indicate an approach that will be reasonable in many cases. A child should not be considered to be competent if it is evident that he or she is acting against their own best interests.

The Trust acknowledges that the law regards young people aged 16 or 17 to be adults in respect to their rights to confidentiality. The Trust will pay due regard to children under the age of 16 who have the capacity and understanding to take decisions about their own treatment and access to records.

### 8.6 Deceased Individuals

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.

Proving status as a personal representative requires that a person must receive a letter of appointment from a probate court and provide it as evidence to the health professional. 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".

There is less clarity regarding which individuals may have a claim arising out of the patient's death. Whilst this is accepted to encompass those with a financial claim, determining who these individuals are and whether there are any other types of claim is not straightforward. 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.

### 8.7 Information Provided to Other Organisations

Where the Trust has legitimately shared patient information with another NHS organisation and that organisation maintains its own records, the Trust considers that it is reasonable for the information to be disclosed as part of a subject access request made directly to that organisation.

### 8.8 Application by Solicitors, Police, Insurances Companies or Attorney

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 under DPA Schedule 2 part 1 (2), which is relating to a police investigation into a crime. Staff must ask the Police Officer to provide a completed Schedule 2.1.2 form, which will outline the reason for the request and what information they require. Staff should contact the IG team for advice (bchft.ig@nhs.net) if they are unsure how to proceed with a request for information for the Police.

### 8.9 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.

### 8.10 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.

### 8.11 Request Log

The service must maintain a secure log of all subject access requests 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.

### 8.12 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.

### 8.13 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.

The Trust must not provide original health records for transfer abroad; a copy or summary of treatment will be provided upon request. Staff should contact the IG team if they are asked to transfer personal data outside the UK.

### 8.14 Freedom of Information Act 2000

The Trust will consider any requests for information which constitutes personal information to be exempt from disclosure under the Freedom of Information Act (2000) if:

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

### 8.15 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).

### 8.16 Fees

**The Trust** will not charge for complying with a subject access request 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.

### 8.17 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 e-mails.

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

### 8.18 Employee Subject Access Requests

How the Trust manages the employment records plays a huge part in dealing with an employee subject access request successfully. The HR department will have a process for employee subject access requests 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 subject access requests

There should be no surprises for the employee when they submit a subject access request.

## 9 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, identity (ID) should 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 you to ask the data subject a series of questions only the individual would know the answers to.

## 10 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 | Named Nurse Safeguarding Adults/Adults Safeguarding Lead |
| Mike Baker | Assistant Director of Communications |
| Ruth Besford | Equality and Inclusion Manager |
| Razi Nazir | Knowledge and Library Services Manager |
| Sarah Wilson | Head of Safeguarding |
| Karen Worthington | Acting Borough Director Oldham Children's Services / Interim Operational Director |
| Susan Burton | Director of Nursing Warrington |

| Name | Designation |
|---|---|
| Barry Hutton | Director of Dental Network |
| Andy Shakeshaft | Halton Bronze Command |
| Digital, Information Governance and Information Technology | Membership |
| Corporate Clinical Policy Group | |

# 11 Dissemination and Implementation

## 11.1 Dissemination

The Senior IG Officer will disseminate this policy to Borough Directors for disseminating to Managers and onward dissemination to staff. The policy will be made available on the Trust Intranet (the Hub).

## 11.2 Implementation

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:

- Local Non-Clinical Standard Operating Procedures (LNCSOP's)
- 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.

# 12 Process for Monitoring Compliance and Effectiveness

The core aspects outlined within the policy are monitored through the Trusts health record keeping audit program and the clinical audit programme.

Quality of information both for electronic and paper health records are 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.

## 13 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 |

## 14 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 1989 [online] Available at: https://www.legislation.gov.uk/ukpga/1989/41/contents

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

Department of Health (2010) Guidance for Access to Health Records Requests [online] Available at: http://webarchive.nationalarchives.gov.uk/20130103005001/http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_112916

Freedom of Information Act 2000 (FOIA) [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

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 [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/