	TRUST WIDE DOCUMENT
	Policy
DOCUMENT TITLE	**Subject Access Policy – Access to records for citizens**
DOCUMENT NUMBER	**ELHT/C134 v3.0**
DOCUMENT REPLACES	**ELHT/ C134 V2.1**
LEAD EXECUTIVE DIRECTOR DGM	**Director of Finance/ SIRO**
AUTHOR(S)	**Head of Information Governance- Data Protection Officer and Information Governance Manager**

TARGET AUDIENCE:	All Trust Personnel
DOCUMENT PURPOSE	To safeguard the security of the Trust's information assets by ensuring availability and preserving integrity and confidentially.
To be read in conjunction with	• Information Governance Policy • Confidentiality of Personal Information Policy • Freedom of Information policy
SUPPORTING REFERENCES	• DSP Toolkit • Data Protection Act 2018 • GDPR • Health Records Act 1990

CONSULTATION		
	Committee/Group	**Date**
Consultation	Information Governance Steering Group (IGSC)	May 2022
Approval Committee	Information Governance Steering Group (IGSC)	May 2022
Document approved date	August 2022	
NEXT REVIEW DATE	May 2025	
AMENDMENTS	• Access to records – Deceased patients' guidance • Revision of fees • Caldicott review • Employee reference information • Additional rights • Record retention • Enforcement • Police DP1 Guidance	

Contents

1. Introduction

As a data controller, the Trust has a legal obligation to comply with all appropriate legislation in respect of disclosure and access to personal data.

The main legislation giving rights of access to personal information include:

- **The Data Protection Act 2018 (DPA)** - rights for living individuals to access their own records. The right can also be exercised by an authorised representative on the individual's behalf. The DPA is not just confined to health records. It applies equally to all relevant records relating to living individuals.
- **The Access to Health Records Act 1990 (AHRA)** - rights of access to deceased service user health records by specified persons.
- **The Medical Reports Act 1988 (MRA)** - right for individuals to have access to reports, relating to themselves, provided by medical practitioners for employment or insurance purposes.
- **General Data Protection Regulation 2018 (GDPR).**

In addition, there are a range of 'statutes' and 'gateways' that permit or require the Trust to disclose the personal information it holds.

1.1. Purpose

This policy has been produced with the intention of promoting good practice and consistency of dealing with requests from individuals for access to personal data, including other organisations/bodies. It has been developed to ensure that East Lancashire Hospital trust (ELHT) complies with its duties as a data controller and provides access in accordance with the law and good practice.

1.2. Scope

This policy covers the requirements of the – DPA, AHRA and MRA in respect of data subjects and their authorised representatives, including disclosures within the scope of these and other 'Acts' which compel or permit the Trust to disclose personal data, i.e. court orders, requests from the police and so on.

Personal data can be data held in electronic form or in a 'relevant filing system'. It applies no matter what media the information is stored in. Paper records count as a relevant filing system for the DPA if they are held in a 'sufficiently systematic, structured way'. If paper records are held in no particular order, (e.g., an unindexed file), they may not be subject to the right of access.

For example:

- manually stored paper data, including data held in offsite storage.
- electronically stored records, e.g., email, network.
- tapes held on CCTV and other visual recordings.
- other electronic media, CD-ROM/DVDs, memory sticks, audio recordings.
- clinical services e.g., Health records.
- corporate services e.g., customer care, complaints, investigations, claims, and incidents.

2. Definitions

Data Controller	Person who, (either jointly or in common with other persons), determines the purposes for which and the manner in which any personal data are to be processed. The data controller for ELHT is the Trust itself rather than an individual within the organisation.
Data Processor	Is an individual, (other than an employee of the data controller), or organisation, who processes personal information whilst undertaking a business activity or service on behalf of the Data Controller, under contract.
Data Subject	Means an individual who is the subject of personal data.
Health Professional	For the purpose of the Data Protection Act, a registered health professional can be one of the following people: • a medical practitioner - this could be a GP, consultant or hospital doctor. • a dentist. • an optician. • a pharmaceutical chemist. • a nurse, midwife or health visitor. • an osteopath. • a chiropractor. • a clinical psychologist, child psychotherapist or speech therapist. • a music therapist. • a scientist employed by a health service body as head of department. • anyone registered as a member of a profession to which the Health Professionals Order 2001.
Health Record	Data Protection legislation defines a 'health record' as a record consisting of information about the physical or mental health or condition of an identifiable individual made by or on behalf of a health professional in connection with the care of that individual.
Parental Responsibility	As defined by the Children's Act 1989, means that all the rights, duties, powers, responsibility and authority which by law a parent of a child has in relation to the child and his/her property.
Personal Data	For information to be personal data, it must relate to a living individual and allow that individual to be identified from it, (either on its own or along with other information likely to come into the organisation's possession).
Processing	Obtaining, recording or holding information, or carrying out any operation or set of operations on that data.
Recipient	Any person to whom the data are disclosed.
Relevant Filing System	Any set of information relating to individuals to the extent that, although the information is not processed by means of

	equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.
Sensitive Data	Defined in the DPA chapter 2 (35) (8) as personal data consisting of information relating to the data subject with regard to racial or ethnic origin; political opinions; religious beliefs or other beliefs of a similar nature; trade union membership; genetic data and biometric data for the purpose of uniquely identifying individual; physical or mental health or condition; sexual life; the commission or alleged commission by the data subject of any offence; or any proceedings for any offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.
Subject Access Coordinator	Administrator who processes subject access requests on behalf of the data controller (the Trust).
Subject Access Request (SAR)	Section 45 of the DPA and Article 15 of GDPR, sets out an individual's right to see copies of the personal data an organisation holds about them, why this information is held, and to whom it may be disclosed.
Third Party	Means any person other than – (a) the data subject, (b) the data controller, or (c) any data processor or other person authorised to process data for the data controller or processor.

3. Duties

3.1. Board/Lead Committee

The Information Governance Steering Group (IGSG) is responsible for providing scrutiny and review of this document prior to approval.

The IGSG will monitor and oversee the implementation of this policy.

3.2. Chief Executive

The Chief Executive is responsible for ensuring that ELHT implements an access to records policy which is fit for purpose and complies with all relevant legislation. The Chief Executive delegates executive responsibility to the Director of Finance and Informatics

3.3. Executive Directors

3.3.1 Director of Finance and Informatics

The Director of Finance and informatics has lead responsibility for formulating the Trust approach to subject access and access to records, incorporating policy and process

development. To include approval, compliance with, monitoring and review of any documents produced.

The Director of Finance and informatics delegates policy and process development to the Head of Information Governance and operational responsibility to Line Managers/ Business Managers.

3.3.2 Associate Medical Director

The Associate Medical Director is the Caldicott Guardian. They are responsible for protecting the confidentiality of service user information and enabling information sharing. The Caldicott Guardian may be consulted to advise on complex disclosure cases.

3.4. Managers

3.4.1 Data Protection Officer

The Head of Information Governance is the Data Protection Officer and will manage complaints received via the ICO.

3.4.2 Head of Information Governance

The Head of Information Governance has been appointed to write and review the access to records policy.

They will report performance monitoring data to IGSG on the handling of SARs received and processed. The reporting should include compliance with turnaround times.

3.4.3 Communications Manager

The communications team must monitor the Trust's social media accounts and be able to forward requests received in this way to the appropriate person for processing.

3.5. Employees

3.5.1 Information Governance (IG) Team

The IG Team will provide professional advice and support to all employees in relation to disclosure requests and information sharing, in particular requests from the police and court where consent of the data subject has not been provided.

3.5.2 Designated Administration Staff

There are designated administration staff in place who are responsible for the administration and processing of access to records requests. For the purposes of this policy, they will be known as 'subject access coordinators. The following departments

process their own requests Radiology and MSK

They will ensure that:

- All requests are appropriate, and the consent and identity of the applicant is verified
- Communications are sent to the applicant throughout the life of the request, from its receipt until the release of the information
- Requests are recorded and processed in a legally compliant and confidential manner
- Potential problems are escalated back to their operational manager
- Health professionals are consulted to identify information that may cause serious harm- were applicable (please see exemptions).
- Advice is sought where appropriate from health professionals, the Caldicott Guardian and the IG Team
- Consent forms and associated documentation, including copies of disclosure files are held securely and confidentially and will be retained in line with the Trust's retention policy.
- There is a robust password process in place which includes the retrieval of any password protected documents.

3.5.3 All Other Staff

Employees must ensure they understand the requirements of this policy and in particular must be able to:

- identify a subject access or other request for personal data if received.
- know where and who to re-direct it to, and
- pay regard to the time limits imposed by the legislation by forwarding promptly.

Employees must not respond to access to records requests themselves.

4. Processes and Procedures

4.1 The Data Protection Act and Subject Access Rights – living individuals

The DPA regulates the processing, including the disclosure, of information about identifiable living individuals. Subject to specified exemptions the Act requires data controllers (the Trust) to comply with the seven 'GDPR principles' set out in Article 5. Data Protection Act 2018.

The Data Protection Act gives individuals (known as data subjects), or their authorised representative, the right to apply to see certain personal data held about them. These rights are known as 'subject access rights' and are contained in Article 15 of GDPR.

Appendix 1 contains further information about who can make a request.

4.1.1 Making a request

An individual may exercise this right by making a request in writing. However, where an individual is unable to make a written request, it is the Department of Health's view that in serving the interest of service users it can be made verbally, with the details recorded on

the individual's file.

The Trust may require the data subject to supply further information which will allow identification of the relevant records and to confirm their identity.

Appendix 2 contains further information about the identification required.

An emailed request is as valid as one sent in hard copy. Requests may also be received via social media or the Trust website.

If a request does not mention the DPA specifically or even say that it is a subject access request, it is nevertheless valid.

A request is valid even if it has not been sent directly to the person who normally deals with such requests. It is important that all employees can recognise a request and can forward it to the relevant area in accordance with the Trust's SAR process.

Requests for copies of CCTV footage should be responded to in line with the Trust CCTV policy.

4.1.2 Recording the request

On receipt, all requests must be recorded on DATIX. The receiving date is the date received into the Trust, not the date received into the team dealing with the request. Requests that are received late must be recorded on DATIX as an incident.

DATIX must be updated at each stage of the request, on the day the action is taken.

4.1.3 Clarifying the request

Before responding to a SAR, the Trust may ask the requester for information it reasonably needs to find the personal data covered by the request. The Trust is not obliged to comply with the SAR until the information has been received.

The Trust cannot require the data subject (applicant) to narrow the scope of their request, but merely to provide additional details that will help the subject access coordinator locate the requested information. If an applicant asks for 'all the information you hold' about them, they are entitled to do that. The Trust may ask the applicant to provide information about the context in which information about them may have been processed, and about the likely dates when processing occurred, if this will help the subject access coordinator deal with the request.

The type of information it might be reasonable for the subject access coordinator to ask for includes, where personal data is held in electronic form, information as to the type of electronic data being sought, (application form, letter, email etc.), and roughly when the data was created. This may help to identify whether the information sought is likely to have been deleted or archived (either printed off and held in a manual data archive or removed from the 'live' electronic data systems and held in an electronic archive).

4.1.4 Responding to the request

In response to a subject access request the Trust must provide the following information:

a) Confirmation as to whether or not information relating to the data subject is being processed.
b) A description of the personal data, the purposes for which it is being processed, the likely recipients and, if appropriate, the source of the data.
c) A copy of the information relating to the data subject which the data controller has in permanent form (unless it is not possible, or to do so would cause the Trust 'disproportionate effort'); and
d) additional information which may be required to make sense of the information (such as a list of acronyms).

Appendix 3 contains further information on locating information.

Time Limit
The Trust must respond promptly to any subject access requests, within a maximum of 1 calendar month from receipt of the requests or any further information which has been requested to confirm the applicant's identity or to locate the data.

Where the data controller:

a) reasonably requires further information in order to satisfy itself as to the identity of the person making a subject access request and to locate the information which that person seeks; and
b) has informed him of that requirement,
c) the data controller is not obliged to comply with the request unless supplied with that further information.

Although the DPA states 1 calendar month to comply, a government commitment requires that for health records, requests should normally be handled within 21 days.

A letter acknowledging receipt of the request must be sent to the applicant within 2 working days of receipt of the request.

In exceptional circumstances if it is not possible to comply within the 1 calendar month period then the applicant must be informed.

You can extend the time to respond by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their request and explain why the extension is necessary. These should be assessed by the IQA team on a case-by-case basis.

To note: If a request has to be re-directed internally, the one calendar month time limit begins on the date the request was received by the Trust and not the date received by the processing team.

Fees
In most cases you cannot charge a fee for a subject access request. However, if the request is found to be manifestly unfounded or excessive you may charge a 'reasonable fee' for the administration costs of complying with the request.

You can also charge a reasonable fee if an individual requests further copies of their data following a request. You must base the fee on the administration costs of providing further copies.

4.1.5 Special Rules for Health Records

Separate provisions exist in relation to requests for health records in order to avoid disclosing material in inappropriate circumstances. Consultation by the data controller with the 'appropriate health professional' is required.

- Consulting with an appropriate health professional for the following requests: Deceased Patients, Data Subject and Police requests.

- The appropriate health professional, as defined in DPA schedule 3, part 2, must be consulted and give their written permission to release health information. They are responsible for making decisions to limit or deny access to health information.
- The health professional who is currently or was most recently responsible for the diagnosis, care or treatment of the data subject in connection with the matters to which the data relates.

- Where there is more than one such health professional, the health professional who is the most suitable to provide an opinion on the question.

  The exceptions to this are where the Caldicott Guardian, DPO and SIRO have agreed that the SAR Coordinators will remove all third-party information prior to release.

- **Situations where information may be limited or denied**
  In consulting with the appropriate health professional, the Data Protection Act 2018 enables the Trust to limit or deny access to an individual's health record where the information released may cause serious harm to the physical or mental health or condition of the service user, or any other person.

  Any person who is not an appropriate health professional must not withhold information covered by this exemption. Information identified for disclosure must be screened by the appropriate health professional who must highlight to the SAR coordinator any information to be withheld with accompanying justification for withholding the information from the applicant or data subject.

  The Data Protection Act does not define 'serious harm', however, it is considered that it would mean life threatening and/or traumatic, and from which recovery, whether physical or psychological, may reasonably be expected to be difficult or impossible.

  In the case of Access to Health Records Act, in addition to screening for serious harm, if the deceased person had indicated that they did not wish information to be disclosed, or the record contains information that the deceased person expected to remain confidential, then it should remain so, unless there is an overriding public interest in disclosing.

Where information is withheld there is no requirement to tell the applicant or data subject that the information has not been released.

4.1.6 Exemptions

The DPA recognises that in some circumstances the Trust might have a legitimate reason for not complying with a SAR, so it provides a number of exemptions from the duty to do so. Where an exemption applies to the facts of a particular request, the Trust may refuse to provide all or some of the information requested, depending on the circumstances. On receipt of a request these exemptions will be considered on a case-by-case basis.

The exemptions include:

- if the individual makes repeated requests to access the same or similar information – this would excuse the Trust from responding to **vexatious requests** (see 4.8.1).
- where the data **includes information about another person** who has not consented to the disclosure of that information, unless 'it is reasonable in all the circumstances to disclose the information without the consent of the individual'. A balancing of the interests of the two individuals is required in this situation (see 4.8.2).
- where the information is a **reference given in confidence** by the Trust to a third party for the purpose of educating, employing or training the data subject or in relation to services provided by the data subject (see 4.8.3).
- where the information relates to a **management forecast** and its release will prejudice the Trust's ability to conduct its business or activity.
- where the information relates to **negotiations between the Trust and the data subject**, the disclosure of which may prejudice those negotiations.
- where a claim to **legal professional privilege** could be made in respect of the information in legal proceedings.

The DPA does not explain what is meant by 'likely to prejudice'. However, the Information Commissioner's view is that it requires there to be a substantial chance (rather than a mere risk) that complying with the SAR would noticeably damage the discharge of the function concerned.
Exemptions | ICO

4.1.7 Repeated or unreasonable requests

Where an access request has previously been met, the Act permits that a subsequent identical or similar request does not have to be fulfilled unless a reasonable time interval has elapsed between.

The DPA does not limit the number of requests an individual can make to any organisation. However, it does allow some discretion when dealing with requests that are made at unreasonable intervals.

The Trust will not be obliged to comply with an identical or similar request to one already dealt with, unless a reasonable interval has elapsed between the first request and any subsequent ones.

In determining whether a request has been made at reasonable intervals, the following will be considered:

- the nature of the data – this could include considering whether it is particularly sensitive.
- the purposes of the processing – this could include whether the processing is likely to cause detriment (harm) to the requester;
- how often the data is altered – if information is unlikely to have changed between requests a request may be refused.

Section 95 of the DPA states that the '…information to be supplied pursuant to a request under section 94 must be supplied by reference to the data in question at the time when the request is received except that it may take account of any amendment or deletion made between that time and the time when the information is supplied, being an amendment or deletion that would have been made regardless of the receipt of the request'. If there has been a previous request or requests, and the information has been added to or amended since then, when answering an access request the Trust is required to provide a full response to the request: not merely supply information that is new or has been amended since the last request. It is acceptable to negotiate with the requester to ask them to restrict the scope of their request to the new or updated information; but if they insist upon a full response then all information should be supplied.

If, for these reasons, the Trust is not obliged to provide the information requested and decides not to do so, this must be explained to the requester.

4.1.8 Third Party Information

The basic rule
As data controller, the Trust may find that in complying with a subject access request, it will disclose information relating to an individual other than the data subject who can be identified from that information, including the situation where the information enables that other individual to be identified as the source of information. The DPA sets out only two circumstances in which the data controller is obliged to comply with the subject access request in such circumstances, namely:

- where the other individual has consented to the disclosure of the information; or
- where it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

So, although the Trust may sometimes be able to disclose information relating to a third party, a decision needs to be made as to whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights in respect of their own personal data. If the other person consents to you disclosing the information about them, it would be unreasonable not to do so. However, if there is no such consent, you must decide whether to disclose the information anyway.

The Trust will make decisions about disclosing third-party information on a case-by-case basis and not apply a blanket policy of withholding it. For the avoidance of doubt, the Trust cannot refuse to provide subject access to personal data about an individual simply because the data was obtained from a third party.

In line with the Data Protection Act 2018, the Trust will not withhold the names of health professionals who have compiled or contributed to the health records or who have been involved in the care of the service user.

Three-step approach to dealing with information about third-parties
To assist with decision making whether to disclose information relating to a third-party individual, it helps to follow the three-step process described below:

- **Step 1 – Does the request require the disclosure of information that identifies a third party?**
  The Trust will need to consider whether it is possible to comply with the request without revealing information that relates to and identifies a third-party individual. In doing so, it should take into account the information to be disclosed and any information the Trust reasonably believes the person making the request may have, or may get hold of, that would identify the third-party individual.

  As the DPA requires that the Trust provide information rather than documents, it may be possible to delete names or edit documents if the third-party information does not form part of the requested information. However, if it is impossible to separate the third-party information from that requested and still comply with the request, the following steps need to be considered.

- **Step 2 – Has the third-party individual consented?**
  In practice, the clearest basis for justifying the disclosure of third-party information in response to a SAR is that the third party has given their consent. It is therefore good practice to ask relevant third parties for consent to the disclosure of their personal data in response to a SAR. However, the Trust is not obliged to try to get consent and, in some circumstances, it will clearly be reasonable to disclose without trying to get consent, such as where the information concerned will be known to the requester anyway. Indeed, it may not always be appropriate to try to get consent, for instance if to do so would inevitably involve a disclosure of personal data about the requester to the third party.

- **Step 3 – Would it be reasonable in all the circumstances to disclose without consent?**
  In practice, it may sometimes be difficult to get third party consent, e.g. the third party might refuse consent or might be difficult to find. If so, the Trust must consider whether it is 'reasonable in all the circumstances' to disclose the information about the third party anyway. The DPA provides a non-exhaustive list of factors to be taken into account when making this decision. These include:

  - the type of information that would be disclosed
  - any duty of confidentiality owed to the other individual
  - any steps taken by the controller with a view to seeking the consent of the other individual
  - whether the other individual is capable of giving consent
  - any express refusal of consent by the other individual

Confidentiality
Confidentiality is one of the factors that must be taken into account when deciding whether to disclose information about a third party without their consent. A duty of confidence arises where information that is not generally available to the public (that is, genuinely 'confidential' information) has been disclosed with the expectation it will remain confidential. This expectation might result from the relationship between the parties. For example, the following relationships would generally carry with them a duty of confidence in relation to information disclosed.

- Medical (doctor and service user)
- Employment (employer and employee)
- Legal (solicitor and client)
- Financial (bank and customer)
- Caring (counsellor and client)

However, confidentiality should not always be assumed. For example, a duty of confidence does not arise merely because a letter is marked 'confidential' (although this marking may indicate an expectation of confidence). It may be that the information in such a letter is widely available elsewhere (and so does not have the 'necessary quality of confidence'), or there may be other factors, such as the public interest, which mean that an obligation of confidence does not arise.

In most cases where a duty of confidence does exist, it will usually be reasonable to withhold third party information unless the Trust has obtained the third-party individual's consent to disclose it.

Other relevant factors
In addition to the factors listed in the DPA, the following points are likely to be relevant to a decision about whether it is reasonable to disclose information about a third party in response to a SAR.

- **Information generally known to the individual making the request.** If the third-party information has previously been provided to the individual making the request, is already known by them, or is generally available to the public, it will be more likely to be reasonable for you to disclose that information. It follows that third-party information relating to a member of staff (acting in the course of their duties), who is well known to the individual making the request through their previous dealings, would be more likely to be disclosed than information relating to an otherwise anonymous private individual.

- **Circumstances relating to the individual making the request.** The importance of the information to the requester is also a relevant factor. The need to preserve confidentiality for a third party must be weighed against the requester's right to access information about his or her life. Therefore, depending on the significance of the information to the requester, it may be appropriate to disclose it even where the third party has withheld consent.

- **Health, educational and social work records.** Special rules govern subject access to health, educational and social-work records. In practice, these rules mean that relevant information about health, education or social work professionals, (acting in their professional capacities), should usually be disclosed in response to a SAR.

Responding to the request

Whether it is decide to disclose information about a third party in response to a SAR or to withhold it, the Trust will need to respond to the requester. If the third party has given their consent to disclosure of information about them or if the Trust is satisfied that it is reasonable in all the circumstances to disclose it without consent, the information should be provided in the same way as any other information provided in response to the SAR. If consent of the third party has not been obtained and the Trust is not satisfied that it would be reasonable in all the circumstances to disclose the third-party information, then it should be withheld. However, the Trust is still obliged to communicate as much of the information requested as possible without disclosing the third-party individual's identity. Depending on the circumstances, it may be possible to provide some information, having edited or 'redacted' it to remove information that would identify the third-party individual. The Trust must be able to justify its decision to disclose or withhold information about a third party, so it is good practice to keep a record of any decisions made, and why. For example, it would be sensible to note why the Trust chose not to seek consent or why it was inappropriate to do so in the circumstances.

4.1.9 Confidential references

The Trust may give or receive references about an individual, e.g., in connection with their employment. Such references are often given 'in confidence', but that fact alone does not mean the personal data included in the reference is exempt from subject access.

The DPA distinguishes between references the Trust gives and references the Trust receives.

References given are exempt from subject access if you give them in confidence and for the purposes of an individual's education, training or employment or the provision of a service by them.

References received from a third party are not exempt from subject access. If you receive a SAR relating to such a reference, you must apply the usual principles about subject access to decide whether to provide some or all of the information contained in the reference

4.1.10 Supplying information to the applicant

Information supplied to the applicant must contain a marking of 'data subject copy'. This then becomes the responsibility of the data subject to maintain the confidentiality of the information disclosed. Pages should be numbered and the number of pages of information supplied should be recorded in DATIX (notepad).

Information that must be supplied
The focus of a subject access request (SAR) is usually the supply of a copy of the requester's personal data. However, subject access entitles an individual to more than just a copy of their personal data. An individual is also entitled to be:

- told whether any personal data is being processed – so, if you hold no personal data about the requester, you must still respond to let them know this;
- given a description being processed, and whether it will be given to any other organisations or people; and
- given details of the details of the source of the data (if known).

This information might be contained in the copy of the personal data supplied. If it is not, it should be given at the point of supplying the personal data in response to the SAR.

The right to a description of other organisations or people to whom personal information may be given is a right to this information in general terms; it is not a right to receive the names of those organisations or people.

Before supplying any information in response to a SAR, the Trust should check that it has the requester's correct postal or email address (or both).

Explaining the information supplied
The DPA requires that the information supplied to the individual is in intelligible form. At its most basic, this means the information should be understandable by the average person. However, the DPA does not require you to ensure that the information is provided in a form that is intelligible to the particular individual making the request.

Disproportionate effort
There are two situations in which the obligation to supply the requester with a copy of the relevant information 'in permanent form' does not apply. The first is where the requester agrees to another arrangement, and the second is where the supply of such a copy is impossible or would involve disproportionate effort.

The DPA does not define 'disproportionate effort' (section 95 (2)), but case law has determined that there is scope for assessing whether, in the circumstances of a particular case, complying with a request by supplying a copy of the requested information in permanent form would result in so much work or expense as to outweigh the requester's right of access to their personal data.

Furthermore, case law has determined in assessing whether complying with a SAR would involve disproportionate effort, the Trust may take into account difficulties which occur throughout the process of complying with the request, including any difficulties encountered in finding the requested information.

In order to apply the exception, the burden of proof is on the Trust as data controller to show that all reasonable steps have been taken to comply with the SAR, and that it would be disproportionate in all the circumstances of the case for the Trust to take further steps.

In deciding whether to claim this exemption, the Trust must engage with the applicant about the information they require in order to determine an alternative way of satisfying the request if necessary.

Form in which the information must be supplied

Once the personal data relevant to the request has been located and retrieved, it must be communicated to the requester in intelligible form.

In most cases, this information must be communicated to the requester by supplying him or her with a copy of it in permanent form. You may comply with this requirement by supplying a photocopy or print-out of the relevant information.

Where the data subject makes a request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

Subject access provides a right to see the information contained in personal data, rather than a right to see copies of the documents that include that information. The Trust may therefore provide the information in the form of transcripts of relevant documents (or of sections of documents that contain the personal data), or by providing a print-out of the relevant information from Trust computer systems.

Unless otherwise agreed with the applicant, the Trust's preference will be to supply information in paper format and eventually electronic format. Any information sent electronically or on mobile media must be encrypted. Information sent by post must be sent recorded delivery. The information must be protected in an envelope marked 'to be opened by addressee only' and 'private and confidential' with the return address clearly written or stamped on the reverse. Any information collected in person must be signed for with the receipt being retained with the case file. Proof of ID must be obtained from the person collecting the information to ensure it is not disclosed to an unauthorised person. Information must not be supplied by Fax.

4.1.11 Record retention

Subject access requests and information released under the Access to Health Records Act must be retained for 3 years. Records of all other requests for personal information must be kept for 6 years. This is in accordance with the Records Management Code of Practice for Health and Social Care 2016 (RMCoP). The RMCoP must always be consulted before any information is destroyed to ensure that these retention periods are still current. It can be accessed by clicking on the following link: http://systems.digital.nhs.uk/infogov/iga/rmcop16718.pdf.

Reports released under the Medical Reports Act must be retained for at least 6 months following its supply to the employer/insurer. During this period service users continue to have a right of access for which the Trust may charge a reasonable fee for a copy.

4.1.12 Additional rights for individuals

Right to restrict processing
If an individual believes that the Trust is processing personal data in a way that causes, or is likely to cause, substantial unwarranted damage or substantial unwarranted distress to them or another, the individual has the right to send a notice requiring the Trust, within a reasonable time, to stop the processing.
This right to serve a notice applies whether the individual objects to the processing taking place at all, or whether the objection relates specifically to processing for a particular purpose or in a particular way.

The applicant would need to write to the Trust Data Protection Officer and quote section

10 (although they may not do so) and give the specific reasons as to why holding or using the data is causing or is likely to cause substantial damage or distress. This is known as a Section 10 Notice.

The DPA does not define what is meant by unwarranted and substantial damage or distress. However, in most cases:

- substantial damage would be financial loss or physical harm; and
- substantial distress would be a level of upset, emotional or mental pain that goes beyond annoyance, irritation, strong dislike, or a feeling that the processing is morally abhorrent.

The Trust must, within 21 days, respond to the individual stating either that their request has been complied with, or if the request cannot be complied with, the response must give an explanation as to why the request cannot be met.

An individual is not entitled to serve notice if any of the following conditions for processing apply:

- they have given a valid consent to the processing (although consent may be withdrawn);
- the processing is necessary for the taking of steps, at the data subject's request, with a view to entering into a contract, or the processing is necessary for the performance of a contract to which the data subject is a party.
- the processing is necessary for any compliance with any legal obligation to which the Trust is subject, other than an obligation imposed by contract.
- the processing is necessary to protect the individual's vital interests (i.e., it is a life-or-death situation).

While the DPA 2018 repeals the DPA 1998, it does not repeal it in its entirety. The provisions under the 1998 Act which relate to processing of personal data for purposes of national security, defence and international relations of the State will remain effective. The Act will also continue to apply to any complaint or investigation under section 10 of the Acts relating to enforcement of the Acts.

DPA - inaccurate information in records

Informal resolution

Where a data subject believes that information held by the Trust is inaccurate, they should firstly discuss their concerns with the record holder or in the case of health records their health professional.

If the situation cannot be resolved informally, or in the case of a health record the service user is not currently under the care of a health professional they should be advised to submit a formal complaint by writing to:

Customer Relations Team,
East Lancashire Hospitals Trust,
Haslingden Road, Blackburn, BB2 3HH.

Where information is proven inaccurate, data subjects have the right to have it rectified or removed. In most cases, original information will not be completely removed from a record. This is in order to show, for example, medical history, a record of care, or why a particular course of action was taken. Where possible, amended information should be recorded alongside the original.

In situations where the record holder or health professional maintains information recorded is correct, or is a matter of opinion, and there is no factual evidence to the contrary, the data subject should be allowed to supplement the record with their own statement.

For health records, an 'Alert' must be recorded on the clinical information system, to make it clear to those accessing it, that the accuracy of the record has been challenged. The existence of any supplementary information must be cross referenced within the 'Alert Reason' field to ensure it can be located easily. Supplementary statements written by the service user should be addressed to the appropriate health professional, or in the case of a formal complaint the investigating officer. They will be responsible for recording an alert, noting the dispute and attaching the statement / letter to the service user record.

Complainants who remain dissatisfied at the end of the local resolution stage will be advised to apply to the court for an order that the Trust rectifies, blocks, erases or destroys the inaccurate information.

Court Process
Individuals have the right to go to court to request an order where the court is satisfied that an organisation holds data about that individual which are inaccurate. The court may order the Trust to correct, destroy or block access to the data.

The court may order the data controller to notify third parties to whom the incorrect data have been disclosed of the correction. This only applies where it is reasonably practicable for the Trust to do so.

If the court considers that these requirements have been complied with the court may, as an alternative, order the data be supplemented by a court approved statement of true facts. The ICO could serve an equivalent enforcement notice.

Compensation
Individuals have rights to compensation if they suffer damage, or damage and distress because the Trust has breached any of the requirement of the DPA.

4.2 Access to Health Records of the Deceased (AHRA)

The Access to Health Records Act (AHRA) 1990 provides certain individuals with a right of access to the health records of a deceased individual. These individuals are defined under Section 3(1)(f) of that Act as, 'the patient's personal representative and any person who may have a claim arising out of the patient's death'. A personal representative is the executor or administrator of the deceased person's estate.

4.3 Access to Medical Reports (MRA)

The Access to Medical Reports Act 1988 governs access to medical reports made by a medical practitioner who is or has been responsible for the clinical care of the service user, for insurance or employment purposes.

Reports prepared by other medical practitioners, such as those contracted by the employer or insurance company, are not covered by the Act. Reports prepared by such medical practitioners are covered by the Data Protection Act 2018.

A person cannot ask a service user's medical practitioner for a medical report on him/her for insurance or employment reasons without the service user's knowledge and consent. Service users have the option of declining to give consent for a report about them to be written.

4.4 Other requests

Requests can be received from other organisations or statutory bodies who may have a right of access to service user health records.

Appendix 1 contains further information about the most frequent applicants.

Any requests received from organisations or statutory bodies not contained in Appendix 1 does not mean that the request is not valid.

If the request does not include details of the legislation that permits the Trust to provide the applicant with access to records, and the subject access coordinator is unsure as to whether the Trust is legally obliged or legally permitted to provide information, then the applicant should be asked to provide this information.

4.5 Administrative Process

The Trust has designated administration staff in key locations across the Trust who are responsible for receiving, recording and processing requests for personal information. See Appendix 4.

A Flowchart of the administrative process for responding to requests can be found at Appendix 5.

4.6 Complaints relating to the administration of requests

4.6.1 Complaints made to the Trust

If an applicant is unhappy with the outcome of their request for access to information, the applicant should be encouraged to go through the following channels:

- An informal meeting with the health professional (for client requests) or member of Human Resources staff (for employee requests) to resolve the complaint locally.

- If the situation cannot be resolved informally, the applicant should be advised to submit a formal complaint by writing to ELHT complaints department

Following receipt of the complaint a review will take place.

Where access to a deceased persons medical record does not meet the legal requirements for release and a complaint is made, the requestor should be asked their reason for access to the medical records and a Caldicott review can take place. The Caldicott Guardian will make a decision based on information contained in the record, reason for request, expectations or notes made by the person in the medical records e.g., if the patient made a note to state that they did not wish for their family members etc. to have access to their medical records this will be upheld by the Trust.

4.6.2 Complaints made to the Information Commissioner's Office

Any notification of refusal to disclose personal data should be given as soon as practicable and in writing, even if the decision has also been given verbally. The Trust should record the reasons for its decision and explain these to the data subject.

If the Trust decides not to disclose some or all of the personal information, when explaining their reasons to the applicant, they should distinguish between reliance on an exemption, and failure or inability to obtain the consent of another person whose identity would be disclosed, or such a person's refusal to consent and the reason for such refusal.

In the event of the Trust refusing access the individual may, if they so wish, take up the matter with the Information Commissioner. The Information Commissioner may be contacted using any of the following methods.

POST: Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF.
TELEPHONE: 01625 545745
E-MAIL: mail@ico.gsi.gov.uk

4.7 Enforcement

4.7.1 The Information Commissioner's enforcement powers

Anyone who believes they are directly affected by the processing of personal data may ask the Information Commissioner's Office (ICO) to assess whether it is likely or unlikely that such processing complies with the Data Protection Act 2018 (DPA). This is called a compliance assessment. If the ICO assessment shows that it is likely that an organisation has failed to comply with the DPA (or is failing to do so), they may ask it to take steps to comply with the data protection principles. Where appropriate, the ICO may order the organisation to do so. However, the ICO has no power to award compensation to individuals – only the courts can do this.

The Information Commissioner may serve an enforcement notice if she is satisfied that an organisation has failed to comply with the subject access provisions. An enforcement notice may require an organisation to take specified steps to comply with its obligations in this regard. Failure to comply with an enforcement notice is a criminal offence. The Information Commissioner will not necessarily serve an enforcement notice simply because an organisation has failed to comply with the subject access provisions. Before serving a notice, she has to consider whether the contravention has caused or is likely to cause any person damage or distress. She can serve a notice even though there has been no damage or distress, but it must be reasonable, in all the circumstances, for her to do so. She will not require organisations to take unreasonable or disproportionate steps to comply with the law on subject access.

The Information Commissioner has a statutory power to impose a financial penalty on an organisation if she is satisfied that the organisation has committed a serious breach of the DPA that is likely to cause substantial damage or distress.

4.7.2 Enforcement by court order

If the Trust fails to comply with a subject access request (SAR), the applicant may apply for a court order requiring the Trust to comply. It is a matter for the court to decide, in each particular case, whether to make such an order.

The Trust may only refuse to comply if a relevant exemption under the DPA applies in the particular circumstances of the request.

4.8 Compensation

If an individual suffers damage because the Trust has breached the DPA – including, by failing to comply with a SAR – they are entitled to claim compensation from the organisation. This right can only be enforced through the courts. The DPA allows the Trust to defend a claim.

5. Training Requirements

All subject access coordinators must receive DATIX training on how to record subject access and access to records requests.

All subject access coordinators must complete annual Access to Health Records training available via NHS Digital.

All staff must have an awareness of requests for personal information and must know who to pass requests on to if they receive one. Training will be delivered via induction training, annual Information Governance online mandatory training, desktop notifications, Messenger articles or other publications to raise awareness.

6. Monitoring

Measuring and monitoring compliance with the effective implementation of this procedural document is best practice and a key strand of its successful delivery. Hence, the author(s) of this procedural document has/have clearly set out how compliance with its appropriate implementation will be measured or monitored. This also includes the timescale, tool(s)/methodology and frequency as well as the responsible committee/group for monitoring its compliance and gaining assurance.

Minimum Requirement	Frequency	Process for monitoring	Evidence	Responsible Individual(s)	Response Committee(s)
Requests completed within the 1 calendar month legal time limit	Bi-Monthly	DATIX report	Report	IG Manager	IGSG

7. Resource/Implementation Issues

Effective implementation of the Access to Records Policy is reliant on the availability of trained subject access coordinators.

8. Risk Issues

The Data Security and Protection Toolkit is an online self-assessment tool that enables organisations to measure and publish their performance against the National Data Guardian's ten data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practicing good data security and that personal information is handled correctly.

All employees need to be able to identify and re-direct the different types of access requests that may be received. Failure to respond to requests appropriately could lead to a breach of service user/ data subject confidentiality and/or intervention from the ICO. The ICO may take enforcement measures or fine the Trust. A data subject may also make a claim against the Trust for compensation.

The Trust must comply with requests made under the Data Protection Act in line with this document. Failure to do so may result in action from the Information Commissioner's Office, and action against the Trust.

9. Requirements, Supporting Documents and References

9.1. Requirements

Other	Data Security and Protection Toolkit https://www.dsptoolkit.nhs.uk/
	Her Majesty's Government Legislation including: • The Data Protection Act (1998) • The Freedom of Information Act (2000) • The Public Records Act (1958) • The Access to Health Records Act (1990) • The Medical Reports Act (1988) • General Data Protection Regulation (2018) Further details available at: http://www.legislation.gov.uk/

9.2. Supporting Documents

9.3. References

- ICO: Subject Access Code of Practice (V1.2 2017) https://ico.org.uk/media/for-organisations/documents/1065/subject-access-code-of-practice.pdf
- Information Governance Alliance (2016): Records Management Code of Practice for Health and Social Care 2016. Available at: Codes of practice for handling information in health and care - NHS Digital
- Department of Health: Guidance for Access to Health Records Requests (2010) http://www.nhs.uk/chq/Documents/Guidance%20for%20Access%20to%20Health%20Records%20Requests.pdf
- The National Archives (2011). Access to NHS records transferred to places of deposit under the Public Records Act. Available at: http://www.nationalarchives.gov.uk/documents/

10. Subject Expert and Feedback

Advice and support queries in relation to this document should be sent to the author.
Deborah Tonkin
Head of Information Governance and DPO
IG-issues@elht.nhs.uk

11. Review

This document will be reviewed in five years, or sooner in the light of organisational, legislative or other changes.

Appendix 1
Who Can Make A Request

The standard position is that requests for access to records are made by the data subject or their authorised representative with accompanying valid consent. This section lists the most frequent applicants (although the list is not exhaustive). In certain circumstances requests may be received from other organisations or statutory bodies without the accompanying consent of the data subject. This list includes those applicants and gives guidance as to where it may be appropriate to provide records without consent.

1. Service user Access to Health Records

1.1 Formal Access
Subject to the exemptions, competent service users may apply for access to their own Record. It is not necessary for service users to give reasons as to why they wish to access their records.

All requests will be dealt with by a member of staff within the local Subject Access team. See Appendix 4.

1.2 Informal Access
Wherever possible, in response to a verbal request by the client, informal access should be allowed by the appropriate health professional to the parts of the health records for which they have responsibility.

Informal requests by the service user to view health records may be dealt with immediately (e.g. during a consultation provided the notes are available), by the appropriate health professional, or if this is not possible, an appointment can be made for the service user to view the notes.

Service users cannot have direct access to Trust clinical systems. In these cases, the relevant parts of the record should be printed out and shown to the service user. The service user must not be provided with a copy to take away with them.

The health professional must review the record to decide if access can be permitted to all or part of the record and must always consider whether it is necessary to apply any of the exemptions.

2. Employee Access to Personnel Records

Employees or former employees may wish to request access to information such as personnel files, emails and grievance files.
All requests will be dealt with by a member of staff within the Human Resources Department. See Appendix 4.

2.1 Employment references
If the Trust provides a confidential employment reference about an employee or ex-employee to a prospective new employer, the Trust can refuse to disclose that reference to the employee if he or she requests to see it. However, if an employee or ex-employee requests to see a reference provided to the Trust by their old employer in respect of a job application, the Trust is not obliged to comply with the employee's request unless either

the author of the reference has consented to its disclosure, or it is reasonable in all the circumstances to comply with the request without the author's consent.

In determining whether it is reasonable to comply with the request without the author's consent, the Trust must consider:

- Any duty of confidentiality owed to the author
- Any steps taken with a view to seeking the author's consent.
- Whether the author is capable of giving consent.
- And any express refusal of consent by the author.

In any event, this does not excuse the Trust from disclosing as much of the reference as is possible without revealing the identity of the author, whether by the omission of the author's name or other identifying particulars.

Request for copies of references should be addressed to the Human Resources Department. See Appendix 4.

3. Data Subject Access to other Personal Data

Individuals may wish to make a subject access request for information held about them other than information held in health records.

3.1 Information held in complaint files

Individuals are also entitled to access information held about themselves in complaints records. Requests could come from service users, the friends or relatives of service users, or employees of the Trust (both former and current). All requests of this nature should be directed to the Trust's complaints department to be processed.

Complaint files can be complex, often consisting of a mixture of information that is the complainant's personal data, is third party personal data and that is not personal data at all. Third party personal data cannot be disclosed if it would be unfair to do so or if disclosure is reasonable in all the circumstances to do so. Each document may need to be considered for release rather than the file.

Complaint files will often contain information recording an individual's opinion of something or another. However, for an opinion to be personal data, it must both identify an individual and relate to him or her.

It can be difficult to determine whether an opinion:

- relates to the person who holds it,
- relates to the person or issue the opinion is of, or both.

When attempting to determine whether an opinion relates to the person holding it this calls for careful judgement based on the nature of the information, the context in which it is held and the purpose for which it is used. If in doubt, contact the Information Governance team for advice.

Requests for access to complaint files should be logged on DATIX and processed in the same way as requests for access to health records. All records should be reviewed, and any exemptions should be applied as appropriate, including the removal of third party information.

The Information Commissioner's Office has issued guidance on the following:

- Access to Information held in Complaints files

ICO : Information held in complaint files

4. Solicitor or Third Party acting on behalf of the data subject

The DPA does not prevent an individual making a subject access request via a third party. Often, this will be a solicitor acting on behalf of a client, but it could simply be that an individual wants someone else to act for them. In these cases, the subject access coordinator dealing with the request will need to be satisfied that the third party making the request is entitled to act on behalf of the individual. It is the third party's responsibility to provide evidence of this entitlement. For written consent to be considered valid it should be less than 6 months old.

Requests must be received in writing and must contain enough information to enable the Trust to identify the person whose information is being requested.

If the request states that action is intended against the Trust the subject access coordinator must immediately notify the Legal Department. If the request states that no claim is intended against the Trust, the usual process can be followed.

If the subject access coordinator believes that an individual may not understand what information would be disclosed to a third party who has made a SAR on their behalf, the response may be sent directly to the individual rather than to the third party. The individual may then choose to share the information with the third party after having had a chance to review it.

All requests will be dealt with by a member of staff within the local Subject Access team. See Appendix 4.

5. Independent Mental Health Advocate (IMHA)

Service users subject to certain aspects of the Mental Health Act 1983 have statutory access to an Independent Mental Health Advocate (IMHA). IMHAs exist to help and support service users to understand and exercise their legal rights. IMHAs are available to most detained service users as well as service users on supervised community treatment or guardianship.

IMHAs have certain rights of access to service user records under the Mental Health Act 1983. The Department of Health has produced guidance on this subject. This can be viewed by clicking on the following link:
http://webarchive.nationalarchives.gov.uk/+/dh.gov.uk/en/healthcare/mentalhealth/informationonthementalhealthact/dh_091895

All requests will be dealt with by a member of staff within the local Subject Access team. See Appendix 4.

6. Lasting Power of Attorney (LPA)

These were established by the Mental Capacity Act 2005 and set out decisions that

people can authorise others to make on their behalf. An LPA may be put in place for managing property and affairs (including financial matters or for personal welfare - including health care and consent to treatment) for those who lack capacity to make such decisions. The LPA may include restrictions and conditions as to areas where the attorney does not have power to act on or when the LPA and or conditions apply.

Proof of the lasting power attorney must be supplied by producing the original lasting power of attorney. All documents must be returned to the applicant by recorded delivery to the address supplied. Failure to produce this document within 20 days of request will mean the discontinuation of the request.

The LPA must have been registered with the Office of the Public Guardian for it to be valid.

Persons who do not have this power would not normally be able to make a valid subject access request on their behalf.

There is a section on this area in the NHS Code of Practice of Confidentiality on page 31 under the heading *where patients are unable to give consent.* Please see link below: https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

All requests will be dealt with by a member of staff within the local Subject Access team. See Appendix 4.

7. Court of Protection

An attorney appointed by the Court of Protection would have, under general powers, authority to request access to records on behalf of an individual.

All requests will be dealt with by a member of staff within the local Subject Access team. See Appendix 4.

8. Next of kin / relative

Despite the widespread use of ‘next of kin’ this is not defined, nor does it have formal legal status. A next of kin or relative cannot give or withhold their consent to the sharing of information on a service user’s behalf. A next of kin or relative has no rights of access to health records.

It may be decided that disclosure of information or access to records is in the best interests of the service user. These decisions are outside of the scope of this policy.

9. Members of Parliament and Councillors

Under the provisions of the Data Protection Act 2018 (Processing of Sensitive Personal Data) (Elected Representatives) elected representatives, i.e., Members of Parliament, local authority councillors and mayors can request health information about their constituents.

All requests will be dealt with by a member of staff within the local Subject Access team. See Appendix 4.

10. Children and young people

Even if a child is too young to understand the implications of subject access rights, data about them is still their personal data and does not belong to anyone else, such as a parent or guardian. 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, in the case of a health record, the appropriate health professional will need to consider whether the child is mature enough to understand their rights. If the health professional is confident that the child can understand their rights, the Trust should respond to the child rather than the parent. 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, among other things:

- 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.

Children who are aged 13 or over are generally expected to have the capacity to give or withhold their consent to the release of information from their health record.

All requests will be dealt with by a member of staff within the local Subject Access team. See Appendix 4.

11. Parents requesting children's records

Parents may have access to their children's records if this is not contrary to a competent child's wishes.

For children under 18, any person with parental responsibility may apply for access to the records. Not all parents have parental responsibility. In relation to children born after 1 December 2003 (England and Wales), 15 April 2002 (Northern Ireland) and 4 May 2006 (Scotland), both biological parents have parental responsibility if they are registered on a child's birth certificate.

In relation to children born before these dates, a child's biological father will only automatically acquire parental responsibility if the parents were married at the time of the child's birth or at some time thereafter.

If the parents have never been married, only the mother automatically has parental

responsibility, but the father may acquire that status by order or agreement.

Neither parent loses parental responsibility on divorce.

Where more than one person has parental responsibility, each may independently exercise rights of access.

Where a child has been formally adopted, the adoptive parents are the child's legal parents and automatically acquire parental responsibility.

In some circumstances people other than parents acquire parental responsibility, for example by the appointment of a guardian or on the order of a court.

A local authority acquires parental responsibility (shared with the parents) while the child is the subject of a care or supervision order.

If there is doubt about whether the person giving or withholding consent to access has parental responsibility, legal advice should be sought.

The Trust is entitled to refuse access to a parent, or an individual with parental responsibility where the information contained in the child's records is likely to cause serious harm to the child, or another person.

All requests will be dealt with by a member of staff within the local Subject Access team. See Appendix 4.

12. Deceased - Personal Representative of the deceased

The personal representative is the only person who has an unqualified right of access to a deceased service user's record and need give no reason for applying for access to a record.

The requester should provide enough proof to satisfy the data controller of their identity. This would include probate documents and personal identification.

All requests will be dealt with by a member of staff within the local Subject Access team. See Appendix 4.

13. Deceased - Applications in relation to a claim under AHRA

Individuals have a legal right of access under the Access to Health Records Act (AHRA) only where they can establish a claim arising from a service user's death.

There is less clarity regarding which individuals may have a claim arising out of the service user'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 record holder should seek legal advice.

Where an application is being made on the basis of a claim arising from the deceased's death, applicants must provide evidence to support their claim in the form of a solicitors letter.

All requests will be dealt with by a member of staff within the Subject Access team. See Appendix 4.

14. Access to Medical Reports

The Access to Medical Reports Act 1988 governs access to medical reports made by a health professional who is or has been responsible for the clinical care of the service user, for insurance or employment purposes. Reports prepared by other health professionals, such as those contracted by the employer or insurance company, are covered by the Data Protection Act 2018.

A person cannot ask a service user's health professional for a medical report about him/her for insurance or employment reasons without the service user's knowledge and consent. Service users can decline to give consent for a report about them to be written.

The service user can apply for access to the report at any time before it is supplied to the employer/insurer, subject to certain exemptions which allow the health professional to withhold access (discussed below). The health professional should not supply the report until this access has been provided, unless 21 days have passed since the service user has communicated with the doctor about making arrangements to see the report. Access incorporates enabling the service user to attend to view the report or providing the service user with a copy of the report.

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

A health professional may make a reasonable charge for supplying the service user with a copy of the report.

Health professionals must retain a copy of the report for at least 6 months following its supply to the employer/insurer. During this period service users continue to have a right of access for which the medical practitioner may charge a reasonable fee for a copy.

Withholding access to the report

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

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

All requests will be dealt with by a member of staff within the local Subject Access team.

See Appendix 4.

15. Mental Health Tribunals

The solicitor acting on behalf of the service user may request copies of health records, these requests will be accompanied by the service user consent and will be dealt with by a member of staff within the local Subject Access team. See Appendix 4.

16. Audit trail information

Audit Trail Information details who has accessed an individual's records. Applicants should make a formal request for access to this information which must be provided in a suitable form so that it is intelligible and easily understood.

Some statutes place a strict requirement on the Trust to disclose information. Care should be taken however to only disclose the information required to comply with and fulfil the purpose of the law. If the health professional has reason to believe that complying with a statutory obligation to disclose information would cause serious harm to the service user or another person, they should seek legal advice.

17. Court Order / Affidavit

There are many scenarios surrounding Courts and access to health records and advice should always be sought if a member of staff receives a request for records where there is any doubt as to how to deal with the request. If the matter is complicated, then the Trust will have the opportunity to seek legal advice.

Often disclosure of medical records of the alleged victim of, or witness to, a crime is requested by the alleged perpetrator's defence lawyers, and occasionally by the Crown Prosecution Service or prosecution team. Initial refusal by the appropriate health professional to release such records will usually be met by a witness summons being issued by the court, (under the Criminal procedure (Attendance of Witnesses) Act 1965) in the Crown Court. The defence legal team are only entitled to have access to confidential material that is relevant to the matters in issue in the criminal trial. They are not entitled to trawl through a service user/victim's entire psychiatric history seeking material for cross-examination.

Prior to the applicant (defence/prosecution) requesting a court order to be served on the Trust they should issue the Trust with an affidavit and copy of the application notice to answer within 7 days (crown court rules 1982). This gives the Trust a period of time to decide whether the records should be disclosed or whether it would not be in the best interests of the service user, or the third parties mentioned within the notes, to disclose the whole record(s) to the court. If the service user does not consent to disclosure, the appropriate health professional remains obliged to refuse disclosure on the grounds of confidentiality. The Trust can then either write to court setting out the reasons why it is felt a summons should not be issued or the Trust can attend the hearing for the summons, (legal representation would be required if this is the case).

If the Trust is not issued with the affidavit, it may be served with a summons to produce the records to the court on a specific date. Failure to comply with the order may be contempt of court, and therefore a very serious matter. A Court Order will usually require a health professional or subject access coordinator to produce health records to the court,

and in these circumstances, they should not be handed over to the police, defence or prosecution.

It is essential that all original records the Trust holds relating to the service user are taken to the court or in the case of electronic records the court will require a hard copy, unless otherwise agreed.

Where information is disclosed under court order, those who disclose it will usually have a complete defence to any allegation that they have breached confidentiality, but the order must be interpreted correctly, and information only be disclosed in accordance with the terms of the order.

However, even though the court has ordered production of the notes the appropriate health professional should still review the notes for anything that may harm the service user or any other person. It may then be necessary for the Trust to seek legal representation if it is felt it would not be in the best interests of the service user, or the third parties mentioned within the notes, to disclose the whole record(s) to the court.

If an affidavit or court order is issued to the Trust, it must immediately be telephoned through and then forwarded to the local Subject Access team to be dealt with. See Appendix 4.

18. Coroner

Under the Coroners and Justice Act 2009 following the death of a service user the coroner may request disclosure of any information considered relevant and necessary to their investigations.

Normally a copy of the records should be provided however Coroners are entitled to request original records. It they do, then copies of the records must be retained by the Trust. Coroners normally give sufficient notice for copies to be made but have the power to seize records at short notice, which may leave little or no time to take copies.

All endeavors must be made to take a copy of the notes, however if this is not the case a note must be made of the person seizing the records, their identity checked, and their contact details taken (as in many cases it is the police acting on behalf of the coroner). If the Police are acting on behalf of the coroner, they must complete a data protection form – each force has their own form.

All requests will be dealt with by a member of staff within the local Subject Access team. See Appendix 4.

19. Criminal Cases Review Commission (CCRC)

If a request to access records is received from the CCRC then this must be complied with as under section 17(2) of the Criminal Appeal Act 1995, the Trust is required to do so.

All requests will be dealt with by a member of staff within the local Subject Access team. See Appendix 4.

There are a number of legal gateways which allow the Trust to override confidentiality and release information. Gaining consent and the implications of gaining consent should

always be considered.

If a request for information is received from a government department, agency or public authority, and it is not clear if the organisation requesting the information is permitted to do so, then the subject access coordinator should ask the requesting person to state which legal gateway it is that allows the Trust to disclose the relevant information to that organisation. This can then be checked before any information is released.

20. Police

If the application for personal information e.g., copy of health records, is accompanied by the written consent from the data subject, the request can be processed as though it was from the data subject themselves. If it is unclear whether the data subject would know the extent of the information to be disclosed, then they must be contacted before proceeding.

In the absence of consent the Trust is permitted to release information to the police in a number of circumstances, however gaining consent should always be considered unless to do so will prejudice the enquiry.

21.1 Section 29 request, GDPR Article 6 (DP1 forms)

The Police may seek personal information under an exemption of the Data Protection Act 2018. Schedule 11-part 4(2) exemption is used when making enquires which are concerned with:

a) the prevention and detection of crime or
b) the apprehension or prosecution of offenders.

Disclosing in connection with a serious crime:

Disclosing information to help prevent, detect or prosecute serious crime may sometimes be justified to protect the public. Although there is no absolute definition of serious crime, Section 116 of the Police and Criminal Evidence Act 1984 identifies some serious arrestable offences which include:

- treason.
- murder
- manslaughter.
- rape.
- kidnapping.
- high jacking.
- certain sexual offences.
- causing an explosion.
- certain firearm offences.
- taking of hostages.
- causing death by reckless driving;
- offences under prevention of terrorism legislation.

Also, making a threat which if carried out would be likely to lead to:

- a serious threat to the security of the state or to public order,

- serious interference with the administration of justice or with the investigation of an offence,
- death or serious injury.

Process for releasing information:

In all circumstances, the Police must fill in a Data Protection Form before any information can be released. Every Police Force has its own form. The form must contain as much detail as possible about the information that is being requested, and why it is necessary to support the prevention, detection or prosecution of a serious crime. The form must be signed by an officer of the rank of Inspector or above.

While the Trust is permitted to release information, it is not legally obliged to do so. Request should be considered in the first instance by the Data Protection Officer and by an appropriate health professional.

What to consider when deciding whether or not it is appropriate to disclose:

- have the police indicated that informing the individual about the disclosure would prejudice their enquiry? if not, the individual should be informed of any disclosure.
- without disclosure, would the task of preventing, detecting or prosecuting the crime be seriously prejudiced or delayed?
- is the information limited to what is strictly relevant to a specific investigation? ('phishing trips' for non-specific information, not related to a specific incident are not the basis for disclosure of personal data).

During normal office hours, (8am to 4pm Monday to Friday), the local Subject Access team must be contacted to log and process requests. The Information Governance Team will also be available for advice during these hours.

If a request is received out of normal office hours, staff should always establish if the request is of an urgent nature. If it is not, the Police should be advised to contact the appropriate Subject Access team and forward the Data Protection form to them during normal office hours.

If a request made out of hours is urgent, staff should contact their on-call senior manager for advice and authorisation to release or withhold information. The Police must still fill out and submit a Data Protection Form before any information can be released.

The decision to release information to the Police must always be made by a health professional. All requests must be logged by the local Subject Access team.

Staff should not feel pressurised or intimidated into giving information just because the police have requested it, it is perfectly reasonable to ask why the information is needed and exactly what is required before deciding whether it is appropriate for information to be released.

In addition to the Police, other organisations may request information relying on this exemption because they have a crime prevention or law enforcement function.

21. Crime and Disorder Act 1998 – section 115

Information may be required on an individual if there is a need for strategic cross-organisational planning to detect, prevent or reduce crime and disorder that an individual may be involved in.

While the Trust is permitted to release information, it is not legally obliged to do so. The requirements of the DPA and common law duty of confidentiality must still be met. Requests should be considered by an appropriate health professional.

22. Multi Agency Public Protection (MAPPA)

Section 325 Criminal Justice Act 2003 establishes a duty to co-operate with the Responsible Authority for Multi Agency Public Protection Arrangements (MAPPA). MAPPA assesses and manages the risks posed by violent and sexual offenders who may cause serious harm to the public. Co-operation may include the sharing of information, but any information shared must comply with other legal responsibilities such as the Data Protection Act 2018 and the Common Law Duty of Confidentiality.

23. Children and young people - requests about

Under section 47 of the Children Act (1989) releasing information to other agencies is permitted in order to make all necessary enquiries to decide whether action needs to be taken to safeguard or promote a child's welfare. In such a situation, firstly confirm it is a section 47 enquiry and then release relevant information, unless 'to do so would be unreasonable in the circumstances of the case'. The Trust does not have to gain consent of the parent or child or inform them.

24. Professional bodies (GMC, HCPC, NMC)

During fitness to practice proceedings it is sometimes necessary for the professional bodies to request disclosure of service user records.

When a request is received from the professional body information cannot be released unless service user consent has been obtained. The consent may be provided with the request if the referral has come directly from a service user, if not it may need to be obtained by the Trust.

The service user should be given full information about how the professional body may use the records, and in particular, should be told that it may be necessary to disclose the records to the practitioner concerned and their representatives. The consent from the service user should be clear about what the service user does and doesn't consent to.

Disclosure of service user records will also be lawful without the service user's consent where the disclosure is necessary for the professional body to fulfil its statutory function. In order for disclosure to be necessary, the professional body must be satisfied that, without it they would not be able to establish the full seriousness of the allegations and the professional would not be able to have a fair hearing.

These requests will be dealt with by Clinical Governance in line with clinical professional standards.

25. Ombudsman (Health, Prison)

The Parliamentary and Health Service Ombudsman carries out independent investigations in complaints made by, or on behalf of, people who claim to have suffered injustice or hardship because of poor treatment or service provided by the NHS. In the case of the Prisons and Probation Ombudsman they investigate complaints and deaths of prisoners in custody.

Both have powers to request copies of health records and any other information that will allow them to investigate a complaint.

26. Department of Work and Pensions (DWP)

The DWP may request medical reports or copies of health records in order to assess benefit claims. These should be provided free of charge, with a target timescale of 10 working days from receipt to providing the information.

The service user will have given their consent to DWP to enable access to their records as part of their application for benefit.

Appendix 2
Identification

Confirming the requester's identity

The applicant should provide enough proof to satisfy the Trust of their identity and to enable the subject access coordinator to locate the information required.

If this information is not contained in the original request the subject access coordinator will seek proof as required. Where requests are made by an authorised representative the Trust should be satisfied that the individual has given consent to the release of their information.

For health records, requests from current clients with an ongoing relationship with a health professional, confirmation of identity can be obtained from the appropriate clinician.

Suitable Documentation

Where there is any doubt, proof of identity will be required. Forms of ID must include one copy of proof of identity and one copy of proof of address as follows:

Proof of Identity	Proof of Address
In order to be acceptable, this document must meet the following criteria: 1. it is not expired and is issued by an acceptable source. 2. it contains a photograph affixed by the issuing agency; and 3. it contains a signature as that on the request. There are many ways to meet this requirement, including: • passport • driving licence • EU identity card • student identity card • work pass	Generally, documents meeting this requirement will show the following characteristics: 1. the document is system generated, although tenancy agreements and/or correspondence from a solicitor can also be accepted; also, correspondence from an agency in the UK, such as HMRC can be accepted. 2. the document has a date and is current, usually issued in the last 6 months, but longer periods may apply in some cases, TV License for example 3. the document shows the same name and address as given on the request 4. the document is from an acceptable source and clearly shows that the person has an account or customer identification registered in their name. 5. the document is <u>not</u> a bill for a mobile telephone; and 6. it is not the same document presented as proof of identity. Examples include: • utility bill, • DWP letter

Appendix 3

Locating information

'Personal data' can be data held in electronic form or in a 'relevant filing system'. Paper records count as a relevant filing system for the DPA if they are held in a sufficiently systematic, structured way. If paper records are held in no particular order, they may not be subject to the right of access.

Information held in electronic records

In most cases, information stored in electronic form can easily be found and retrieved. Electronic records may still be 'held' for the purposes of subject access even if the information has been:

- Archived to storage
- Copied to back-up files
- Deleted.

Archived information and back-up records

Any information that the Trust has retained but has removed from 'live' systems should be provided in response to a SAR. If requested, the applicant should be asked to provide enough context about their request to enable the Trust to make a targeted search. Electronic archive and back-up systems may make the information more difficult to locate, however every effort should be made to locate the information requested in order to respond to the SAR request.

Deleted information

Information is 'deleted' when the Trust tries to permanently discard it and has no intention of ever trying to access it again.

The Information Commissioner's view is that, if the Trust deletes personal data held in electronic form by removing it (as far as possible) from its computer systems, the fact that expensive technical expertise might enable it to be recreated does not mean that the Trust must go to such efforts to respond to a SAR. The Commissioner would not seek to take enforcement action against an organisation that has failed to use extreme measures to recreate previously 'deleted' personal data held in electronic form. The Commissioner does not require organisations to expend time and effort reconstituting information that they have deleted as part of their general records management.

Information contained in emails

The contents of an email should not be regarded as deleted merely because it has been moved to a user's 'Deleted items' folder.

Any information that the Trust has retained, i.e. archived emails, should be provided in response to a SAR. If requested, the applicant should be asked to provide enough context about their request to enable the Trust to make a targeted search. Electronic archive and back-up systems may make the information more difficult to locate, however every effort should be made to locate the information requested in order to respond to the SAR request.

Information stored on personal computer equipment

The Trust does not allow employees to hold information about service users, customers, contacts, or other employees on their own devices or in private email accounts. Private email must not be used for communicating Trust business.

Other records

If the Trust holds information about the requester in other media (e.g. in paper files), a decision will need to be made whether it is covered by the right of subject access. Whether the information is personal data accessible via the right of subject access will depend primarily on whether the non-electronic records are held in a 'relevant filing system' and also on whether the requester has given the Trust enough context to enable location of the information.

Amending data following receipt of a SAR

The DPA specifies that a SAR relates to the data held at the time the request was received. However, in many cases, routine use of the data may result in it being amended or even deleted while the Trust is dealing with the request. It is acceptable for the Trust to supply the information held when sending out a response, even if this is different to that held when the Trust received the request.

It is not acceptable to amend or delete the data if the Trust would not otherwise have done so in order not to supply the information.

Appendix 4

Flowchart Administrative Process

NB: see section 4.1.4 of the Access to Records Policy for required response timescales.

Appendix 5

Equality Impact Assessment Screening Form

Department/Function	Information Governance Department			
Lead Assessor	Head of Information Governance/Data Protection Officer			
What is being assessed?	Impact of document on equality			
Date of assessment	08/06/2022			
What groups have you consulted with? Include details of involvement in the Equality Impact Assessment process.	Equality of Access to Health Group	☐	Staff Side Colleagues	☐
	Service Users	☐	Staff Inclusion Network/s	☒
	Personal Fair Diverse Champions	☐	Other (Inc. external orgs)	☒
	Please give details: Information Governance Steering Group			

1) What is the impact on the following equality groups?

Positive:	**Negative:**	**Neutral:**
➢ Advance Equality of opportunity ➢ Foster good relations between different groups ➢ Address explicit needs of Equality target groups	➢ Unlawful discrimination, harassment and victimisation ➢ Failure to address explicit needs of Equality target groups	➢ It is quite acceptable for the assessment to come out as Neutral Impact. ➢ Be sure you can justify this decision with clear reasons and evidence if you are challenged

Equality Groups	**Impact (Positive / Negative / Neutral)**	**Comments** ➢ Provide brief description of the positive / negative impact identified benefits to the equality group. ➢ Is any impact identified intended or legal?
Race (All ethnic groups)	Neutral	
Disability (Including physical and mental impairments)	Neutral	
Sex	Neutral	
Gender reassignment	Neutral	
Religion or Belief	Neutral	
Sexual orientation	Neutral	
Age	Neutral	
Marriage and Civil Partnership	Neutral	
Pregnancy and maternity	Neutral	
Other (e.g. caring, human rights)	Neutral	

2) In what ways does any impact identified contribute to or hinder promoting equality and diversity across the organisation?	N\A

3) If your assessment identifies a negative impact on Equality Groups you must develop an action plan **to avoid discrimination and ensure opportunities for promoting equality diversity and inclusion are maximised.** ➢ This should include where it has been identified that further work will be undertaken to further explore ➢ the impact on equality groups ➢ This should be reviewed annually.

Action Plan Summary

Action	**Lead**	**Timescale**
None		