<table>
<thead>
<tr>
<th>DOCUMENT TITLE:</th>
<th>Subject Access Request Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOCUMENT NUMBER:</td>
<td>ELHT/C134 V2.1</td>
</tr>
<tr>
<td>DOCUMENT REPLACES</td>
<td>ELHT/ C134 V2.0</td>
</tr>
<tr>
<td>LEAD EXECUTIVE DIRECTOR DGM</td>
<td>Director of Finance/ SIRO</td>
</tr>
<tr>
<td>AUTHOR(S):</td>
<td>Freedom of Information / Subject Access Lead</td>
</tr>
<tr>
<td>TARGET AUDIENCE:</td>
<td>All Trust Personnel</td>
</tr>
<tr>
<td>DOCUMENT PURPOSE</td>
<td>To safeguard the security of the Trust’s information assets by ensuring availability and preserving integrity and confidentially.</td>
</tr>
</tbody>
</table>
| To be read in conjunction with | • SAR procedures clinical notes (MR21).  
• Information Governance Policy |
| SUPPORTING REFERENCES | • DSP Toolkit  
• Data Protection Act 2018  
• GDPR  
• Health Records Act 1990 |

### CONSULTATION

<table>
<thead>
<tr>
<th>Committee/Group</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consultation</td>
<td>Information Governance Steering Group (IGSC)</td>
</tr>
<tr>
<td>Approval Committee</td>
<td>Information Governance Steering Group (IGSC)</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Ratification date at Policy Council:</td>
<td>26\textsuperscript{th} February 2019</td>
</tr>
<tr>
<td>NEXT REVIEW DATE:</td>
<td>February 2022</td>
</tr>
<tr>
<td>AMENDMENTS:</td>
<td>V 2.1 Added information for Radiology duplicate image fees</td>
</tr>
<tr>
<td></td>
<td>V 2.0 Update for removal of fees and new GDPR/DPA 2018</td>
</tr>
</tbody>
</table>
Table of Contents
1 Introduction ........................................................................................................................................... 4
2 Responsibilities and Definitions ........................................................................................................ 5
3 Recognising a Subject Access Request (SAR) .................................................................................... 5
4 Rights of Access .................................................................................................................................. 6
  4.1 Exemptions .................................................................................................................................... 6
  4.1.2 Child Protection Concerns ......................................................................................................... 7
  4.1.3 Wishes of Deceased Patients ..................................................................................................... 7
  4.1.4 Repeat of Earlier Request ........................................................................................................... 7
  4.2 Requests from parties other than the subject .................................................................................. 7
  4.2.2 Requests for access by other organisations ................................................................................. 8
    4.2.2.1 Solicitor .................................................................................................................................. 8
    4.2.2.2 Court Order .......................................................................................................................... 8
    4.2.2.3 Department of Work and Pensions ......................................................................................... 8
    4.2.2.4 Police .................................................................................................................................... 8
    4.2.2.5 Research Organisations ....................................................................................................... 9
  4.2.3 Parental Responsibility ............................................................................................................... 9
  4.3 Individuals living abroad ................................................................................................................. 11
  4.4 Information relating to the deceased ................................................................................................ 11
  4.5 Third party disclosure ..................................................................................................................... 11
  4.6 Joint Records .................................................................................................................................. 11
5 Subject Access Request Process ......................................................................................................... 11
6 Fees ..................................................................................................................................................... 13
7 Accessibility ......................................................................................................................................... 14
8 Timescales .......................................................................................................................................... 14
9 Complaints ......................................................................................................................................... 15
10 Training and Awareness .................................................................................................................... 15
11 Dissemination ................................................................................................................................... 16
12 Further Information ............................................................................................................................ 16
Appendix 1 - Responsibilities and Definitions ..................................................................................... 17
Appendix 2 - Request for Access to Personal Information Form .......................................................... 20
Appendix 3 - Request for Access to Personal Information Form for employee records/notes ......... 24
Appendix 4 - ID Checklist ..................................................................................................................... 28
Appendix 5 - Agreement to disclosure of Records form ..................................................................... 30
Appendix 6 - Subject Access Request Process Flow Map .................................................................. 31
Appendix 7 - Subject Access Request Process Flow Map .................................................................. 32
SUBJECT ACCESS REQUESTS

1 Introduction

1.1 The Data Protection Act 2018 gives every living person (or their authorised representative) the right to request access to information held about them by an organisation irrespective of when it was compiled.

Access to deceased patient’s information is governed by the Access to Health Records Act 1990.

1.2 A record can be computerised (electronic) and / or manual form (paper files). It may include such documentation as hand written notes, letters to and from other professionals, reports, imaging records, printouts, photographs, DVD and sound recordings.

1.3 Subject Access requests relating to the Trust will normally be for access to view and / or to request copies of the following types of records which the Trust process. These are:

- Health Care Records held by the Health Records Team
- HR records and other related HR documents for staff held by Human Resources
- Complaints / Incidents information held by the Quality and Safety Unit
- Information held by the Safeguarding Team
- Internal correspondence about a staff member could be requested under the Data Protection Act 2018 as a subject access request.

It is important that all staff bear in mind when compiling records that the content could be requested under the Data Protection Act 2018 as a subject access request, and ensure that records they create are written in a way that would be appropriate to disclose.

This procedure informs staff how requests for access to information about an individual are dealt with and how the Trust respond to such requests. It explains the process by which patients; members of the public; staff; legal representatives and 3rd parties can request the information.

This procedure is designed to reflect best practice in handling requests for information about an individual. Full implementation of this policy will enable the organisation to:

- Comply with legal obligations under the Data Protection Act 2018
- Increase levels of trust and confidence by being open with individuals about the information that is held about them
- Provide better customer care
- Improve transparency of organisational activities in line with public policy requirements
- Enable individuals to verify that information held about them is accurate
2 Responsibilities and Definitions

Key responsibilities and definitions are set out in Appendix 1.

2.1 Employees responsibilities

Heads of Service and Managers are responsible for ensuring that information is disclosable under the requirements of the Data Protection Act, and for ensuring that requests for information are provided in a timely fashion. All employees, whether permanent, temporary or contract, should be aware of this policy and adhere to the principles set out. They should all be aware of how to access this policy and where to seek further advice about this policy.

Employees should also note that access to your own health and personnel records should always be via a subject access request. Accessing your own records in any other way will be considered a breach of your duty of confidentiality. If clarification is required please contact the Information Governance department.

3 Recognising a Subject Access Request (SAR)

3.1 A Subject Access Request (SAR) is any request made by an individual or an individual’s representative (see Rights of Access section) for information held by the Trust about that individual.

3.2 A SAR must be made in writing, however, the requestor does not need to mention the Data Protection Act or state that they are making a SAR for their request to be valid. They may even refer to other legislation, for example, the Freedom of Information Act 2000, but their request should still be treated according to this policy. The “Request for Access to personal information form” which can be provided to a requestor to submit a subject access request. A copy of this can be found in the appendix.

3.3 A SAR can be made via any of, but not exclusively, the following methods:

- Email
- Fax
- Post
- Social media, via Trust Facebook or Twitter accounts
- Corporate website

SARs made online must be treated like any other SAR when they are received, however, the Trust will not provide personal information via social media channels.
4 Rights of Access

Under the Data Protection Act 2018, any living person, who is the subject of personal information held and processed by the Trust, has a right to request access to that information. This is a legal right, subject to given exemptions below. They also have the right to an explanation of any terms they may not understand (such as technical language or terminology) and the right to ask that any inaccurate information is corrected, and to request a copy of those corrections.

Subject access provides a right for the subject to see / view their own personal data as well as to request copies of these.

An individual does not have the right to access information recorded about someone else, unless they are an authorised representative, or have parental responsibility.

The Trust is not required to respond to requests for information unless it is provided with sufficient details to enable the location of information to be identified, and to satisfy itself as to the identity of the individual making the request. The request must also be written. Verbal requests for information held about an individual are not valid subject access requests, however, if an informal request is made verbally to a member of staff it is reasonable that the requestor be provided with the information they require. If the member of staff is unsure, further guidance can be sought from the Information Governance Team.

4.1 Exemptions

4.1.1 Disclosure Might Cause Harm / Third Party Information

Under the Data Protection (Subject Access Modification) Health Order 2000, the Trust has the right to deny access to all or part of records (if this applies) if one of the following conditions applies:

If, in the opinion of the healthcare professional / Head of Service, access would disclose information likely to cause serious harm to the physical or mental health or condition of the patient or any other person (for example, a child in a child protection case)

If giving access would disclose information which identifies a third party (unless the individual concerned has given consent).

Those who make the disclosure decision (e.g. healthcare professionals / Head of Service) must carefully consider, and be prepared to justify, any decisions to disclose or withhold information. The Caldicott Guardian and Data Protection Officer must be advised if there appear to be any grounds for withholding information.

If information has been withheld, the Trust is free to advise applicants of the grounds on which information has been withheld – but they are not obliged to
do so. For example, the Trust may not wish to volunteer the fact that Information has been withheld if they believe that such a disclosure would cause undue distress, or if it might jeopardise a child protection investigation.

4.1.2 Child Protection Concerns

There may be situations in which access to all or part of a child’s health records can be refused – for example, where there are ongoing child protection issues, or where releasing information may put a child or young person at risk of harm. In these cases, advice must be sought from the appropriate managers and child protection professionals, as well as the Caldicott Guardian, before releasing any information.

4.1.3 Wishes of Deceased Patients

Health records relating to deceased people do not carry a common law duty of confidentiality. However, it is the policy of the Department of Health and the General Medical Council (GMC) that records relating to the deceased person should be treated with the same level of confidentiality as those relating to living people. For example, if the record contains a note made at the patient’s request that they did not want a particular individual to know the details of their illness or their care, then no access should be granted to that individual. In addition, the record holder has the right to deny or restrict access if it felt that disclosure would cause serious harm to the physical or mental health of any other person, or would identify a third person.

Identity checks regarding the deceased patients legal representative / executor of will would need be satisfied to ensure the correct recipient has access / copies of any records.

4.1.4 Repeat of Earlier Request

Access to personal information can be refused where an access request has previously been granted. The Data Protection Act permits record holders not to respond to a subsequent identical or similar request unless a reasonable interval has elapsed since the previous compliance. In determining whether a reasonable interval has elapsed, record holders should consider:

- The nature of the information
- How often it is altered
- The reason for its processing
- Whether the reason for the request(s) is also relevant

4.2 Requests from parties other than the subject

4.2.1 Requests for Access to Records Made by a Patient Representative

Any person can authorise a representative to access information held about them on their behalf. This must be done in writing, with confirmation of the representative’s identity and relationship to the patient.

Representatives able to provide evidence that they are acting under a Power
of Attorney or a Court of Protection Order will be granted access to information held about an individual.

Where an individual who is physically or mentally disabled and unable to provide written consent for a representative to seek access on their behalf, the Trust will give the individual as much assistance as possible, in order to ascertain whether consent has been granted by other means to the representative.

4.2.2 Requests for access by other organisations
Various external organisations and agencies may request information held about an individual. In almost all cases, staff must not share any information unless they have consent from the individual. Examples of requests from other agencies are listed below:

4.2.2.1 Solicitor

Solicitors may apply to see information held about their client, but informed, explicit and signed consent must first have been obtained from the individual before a copy of the information is released. The solicitor should be given access only to the information and explanation that would otherwise have been made available to the individual, subject to the restrictions stated above.

4.2.2.2 Court Order

A Court may order disclosure information (e.g. under the Civil Procedure Rules, the Data Protection Act 2018). Unlike a request from a solicitor, a Court Order should be obeyed unless there is a robust justification to challenge it, in which case the Trust may challenge the order through the Court. The Court’s decision is law, unless the Trust decides to appeal the order and take the case to a higher Court in an attempt to override the Court’s decision.

Courts and Coroners are entitled to request original records. If they do, 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 Court Orders or documents appertaining to or alluding to be a Court Order should be forwarded immediately to the Information Governance Lead and the Quality and Safety Unit.

4.2.2.3 Department of Work and Pensions

The Data Protection Act 2018 allows (but does not require) personal data to be disclosed to assist in the assessment or collection of any tax or duty. Any request by the Department of Work and Pensions for access to any information held about an individual must be accompanied by the relevant form.

4.2.2.4 Police

The Data Protection Act 2018 allows (but does not require) personal data to be disclosed to assist in the prevention or detection of crime and the
apprehension of prosecution of offenders.

The individual should be asked (if possible) for their informed, explicit and signed consent to disclose the information, unless this would prejudice the enquiry or court case. **Any request by the Police for access to information held about an individual must be accompanied by the relevant consent form (DP2) and / or a letter detailing the information required from the Chief Superintendent of the requesting police force.**

The Crime and Disorder Act 1998 also allows (but does not require) the Trust to disclose information to the police, local authority, probation service, or health authority for the purposes of preventing crime and disorder. For the Trust to consider releasing any information without consent, the access request must relate to a serious crime in line with the Crime and Disorder Act 1998 (for example, murder or rape), otherwise the Police should be asked to obtain a Court Order or written approved signed consent (see above regarding Court Orders).

All such requests from the Police should be in writing and forwarded immediately to the Quality and Safety Unit and Information Governance Lead.

### 4.2.2.5 Research Organisations

Although research is considered an important factor in improving healthcare, the Information Commissioner does not consider it an essential element in the provision of healthcare.

If personal identifiable or pseudonymised information is required, informed, explicit and signed consent must be obtained. Service users are generally aware and supportive of research, but it is not reasonable to assume that they are aware of, or likely to consent to, each and every research subject or proposal.

If it is sufficient for the purposes of the research to use anonymised data, consent is not required, but patients should be informed by posters and/or leaflets how their information may be shared.

### 4.2.3 Parental Responsibility

Parents, or those with parental responsibility, will generally have the right to apply for access to information held about a child, although disclosure may be refused if the child is deemed competent as “Gillick competent” (see below) and refuses to give consent.

Parental responsibility is defined in the Children Act 1989 as ‘all the rights, duties, powers, responsibilities and authority which by law a parent of a child has in relation to the child and his/her property’.

Married parents both have parental responsibility, unless a Court Order has removed that status from any party. A separated or divorced parent who no longer lives with the child has parental responsibility unless a Court has removed that status from either party.
Parental responsibility endures if the child is in care or custody. It is lost, however, if the child is adopted.

If the parents are not married, only the mother automatically has parental responsibility. The father may acquire it in the following ways:

- Registering the birth, along with the mother, as the child’s father (for children born after 1st December 2003)
- Formal agreement with the mother (Section 4 of the Children Act 1989) – agreement can then only be brought to an end by a Court
- Marrying the mother
- Obtaining a court order
- Obtaining a residence order

In practice, parental responsibilities would include:

- Safeguarding a child’s health, development and welfare
- Financially supporting the child
- Maintaining direct and regular contact with the child

Parental responsibility can also be acquired:

- Through appointment as the child’s guardian
- By way of a residence order from the Court
- By anyone having an Adoption Order made in their favour

Through Section 2(9) Children Act 1989 – “A person who has parental responsibility for a child may not surrender or transfer any part of that responsibility to another but may arrange for some or all of it to be met by one or more persons acting on his behalf”.

A Local Authority can acquire parental responsibility by:

- Emergency protection order (local authority)
- Interim or Full Care orders (local authority)

In this case the parents do not lose parental responsibility but the local authority can limit the extent to which a person exercises their parental responsibility.

Where, in the view of a health professional, the child is not capable of understanding the application for access to records, the Trust is entitled to deny access as being against their best interests.

Legally, young people aged 16 and 17 are regarded to be adults for the purposes of consent to treatment and the right to confidentiality. As such, if a person of this age wishes any information about them to be treated as confidential this wish should be respected and they have the right to deny parental access to information held about them.
4.3 **Individuals living abroad**

A request for access to information held about an individual made from outside the UK will be treated in the same way as a request made from within the UK. People living outside of the UK have the same rights of access to information an organisation holds about them as UK residents do.

4.4 **Information relating to the deceased**

Applications for access to health records of the deceased are made under the Access to Health Records Act 1990. Records made after 1st November 1991 can be made available to a patient representative, executor or administrator. Any person with a claim arising from the death of a patient has a right of access to information specifically relating to the claim.

Requests for access to General Practitioner records where the patient is deceased are handled by NHS England – Primary Care Support Services. Any such application for access received by the Trust will be forwarded to NHS England – Primary Care Support Services to be processed.

NHS England – Primary Care Support Services will obtain the record from storage, copy it and send to the NHS England Area Team to be reviewed.

4.5 **Third party disclosure**

Where records contain information that relates to an identifiable third party, that information may not be released unless:

- The third party is a health professional who has compiled or contributed to a health record, or who has been involved in the care of the individual.
- The third party, who is not a health professional, gives their written consent to the disclosure of that information.
- It is reasonable to dispense with the third party’s consent (taking into account the duty of confidentiality owed to the other individual, any steps taken to seek his/her consent, whether he/she is capable of giving consent and whether consent has been expressly refused).

4.6 **Joint Records**

Where joint records are held, the relevant organisations must be informed of the access request and agree who will lead the disclosure process. However, requests for joint records should not have to be made to both organisations. Either organisation can provide the information requested provided the applicant is informed that the information is jointly held.

The term ‘joint records’ does not include records that contain information provided by one organisation to the other. While the information held by each organisation might be similar, they cannot be considered as joint records. In such cases a separate application must be made to each authority.

5 **Subject Access Request Process**
5.1 **Receipt of request** – Requests for information held about an individual must be directed to the appropriate department i.e. Human Resources for non-clinical records or Health Records Access team for clinical records and casenotes. The requests will be acknowledged and logged. They will also notify the requestor of the next steps. The requestor may be asked to complete a form to better enable the Trust to locate the relevant information. The relevant department will forward the appropriate form to the requestor, see the Appendix 2. Note requests for estates will require completion of a form which will be provided by the estates department if required.

5.2 **Confirmation of identity / further clarification and / or fees payable** – If ID and clarification of a subject access request has not already been provided, the requestor will be asked to provide 2 forms of ID, one of which must be a photo ID and the other confirmation of address - see appendix for full list of ID that may be provided. ID can be photocopied and posted to the Trust or it can be scanned and emailed to the Trust.

**Member of staff ID checks** – Human Resources needs to check the identity of anyone making a subject access request to ensure information is only given to the person entitled to it. In the first instance, check with the member of staff’s line manager that the member of staff who has submitted a request is who they say they are. If they are then you do not need to collate 2 forms of ID. Also check if there are any other circumstances which you need to be aware of pertaining to the request.

If any fees are payable in cases of excessive or repeated requests for the same information - the relevant department will notify the requestor of the amount and details of how to pay. If the requestor is not the subject, written confirmation that the requestor is authorised to act on behalf of the subject is required.

5.3 **Confirmation – Once the ID /clarification / fees have been received**, the relevant department will confirm this to the requestor and notify them that their request will be responded to within one calendar month. The Trust can extend the deadline by up to two months (so up to three months in total) where requests are particularly ‘complex or numerous.’ If this is the case, the data subject must be contacted within one month of making their request and informed why an extension is necessary. This period begins from the date that the ID/clarification/fees are received. The requestor will be informed if there will be any deviation from this timeframe, however, such deviation should be an exception and be escalated to the Data Protection Officer prior to informing the requestor.

5.4 **Collating** – The relevant department will contact and ask the appropriate Head of Service (or delegated authority within the department(s) for the required information as requested in the Subject Access Request. This may also involve an initial meeting with the relevant department to go through the request if this is required. The department who hold the information must return the required information by the deadline provided and / or a further meeting is arranged with the Head of Service (or delegated person) to
review and check the information. This review checks to see if there is any information which may be subject to an exemption and / or if consent is required to be collated from a third party.

The information must be reviewed / received by the given deadline to ensure the calendar month timeframe is not breached. The Head of Service will be asked to complete the “Agreement to Disclosure of Records Form” to ensure they have provided all of the information requested.

5.5 **Response** – The finalised response will be collated together with the information retrieved from the department(s) and / or a statement that the Trust does not hold the information requested or that an exemption applies. A written response will be sent back to the requestor. This will be via email, unless the requestor has specified another method by which they wish to receive the response (e.g. post). The Trust will only provide information via channels that are secure. When hard copies of information are posted, they will be sealed securely and sent by recorded delivery.

5.6 **Logging** – After the response has been sent to the requestor the SAR will be considered closed and the log will be updated.

5.7 **Monitoring and Reporting** - The Information Governance Steering Group will routinely monitor the number of requests received and any issues relating to them, such as difficulty obtaining information, internal reviews and complaints.

6 **Fees**

No fees will be charged unless the request is manifestly unfounded or excessive, in particular because they are repetitive. In this case the Trust has agreed that the following charges will apply:

50 sheets and under - £0.50 per sheet, plus £20 Admin fee, plus postage costs

Anything above this will be as follows: £0.25 per sheet, plus £20 hourly admin fee, plus postage costs.

Radiology images will be charged a fee of £25 for each duplicate request.
7 Accessibility

7.1 Every effort will be made to provide the requestor with information in an accessible format. Requests for information in large print, translated or audio format will be considered on a case by case basis, and may not necessarily be met. However, the Trust will help individuals to understand information where possible.

7.2 The Data Protection Act 2018 requires that information is provided in an ‘intelligible form’. The Trust is not required to translate information or decipher poorly handwritten notes, but best practice would be to help individuals where there are barriers to understanding the information.

7.3 If information is coded, and it is not possible for people outside of the organisation to understand to coded information, the Trust is required to provide access to the code.

8 Timescales

8.1 The Trust will respond to requests for access to information held about an individual within one calendar month. The Trust can extend the deadline by up to two months (so up to three months in total) where requests are particularly ‘complex or numerous.’ If this is the case, the data subject must be contacted within one month of making their request and informed why an extension is necessary.

8.2 When there is a fee applicable, the Trust will inform the applicant of this on receipt of the request and inform the applicant of the amount to be paid. The Trust is not required to provide the information requested until the fee has been paid.

8.3 If the application does not include sufficient information to identify the person making the request or to locate the information (see 4.3), that information should be sought promptly and the month period begins when it is supplied.
9 Complaints

9.1 If an individual or their representative is not satisfied with the outcome of their request, for example, if they feel information has been withheld or recorded incorrectly, or that they have not been allowed sufficient time to view the information, they should be informed of the options available to them to take further action.

9.2 In the first instance, the individual should be encouraged to attend an informal meeting with a view to addressing and resolving the issues locally.

9.3 An individual also has the option to escalate the matter to the Trust Data Protection Officer for review.

9.4 An individual can escalate the matter to the ICO using the following contact details:

The Information Commissioner’s Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545 745
E-mail: mail@ico.gsi.gov.uk

9.5 An individual may wish to seek legal independent advice to progress resolution of their concerns. In all cases, wherever possible, local resolution should be sought. However, the individual has the right to pursue any of these channels at any time and may wish to pursue several actions simultaneously.

10 Training and Awareness

10.1 Specific awareness training will be considered for staff who are identified as holding information that could be subject to a subject access request. This includes the following teams:

- Human Resources
- Safeguarding Lead
- Incidents / Complaints Lead

10.2 All staff will be made aware of subject access and the requirements of the Trust to respond within the statutory timeframe.
11 Dissemination
11.1 The policy will be disseminated to all departments and can be accessed on the intranet.

12 Further Information
12.1 Further information or advice on the content or application of this policy is available from:

- Information Governance Lead
- Caldicott Guardian
- The Information Commissioner's Office (see Escalation Procedure section for full details)
Appendix 1 - Responsibilities and Definitions

1. Data Controller.

Under the Data Protection Act 2018, the Trust is a data controller. That is, the organisation (or person) that determines the purposes for which and the manner in which any personal data about individuals are processed.

2. Personal Identifiable Information

The Data Protection Act (DPA) 2018 and General Data Protection Regulation (GDPR), defines personal data as “data which relates to a living individual who can be identified a) from those data or b) from those data and other information which is in the possession of, or likely to come into possession of Data Controller”. This includes an expression of opinion. Personal data includes: name, address, date of birth, national insurance number, credit card no, passport no, blood group, DNA, Biometric data, sexual preference, destination of air travel, medical history, geographical location, last time and place credit card used. At least one condition from Article 6, (GDPR) must be met before this information can be released.

3. Special Classes of Data

At least one condition from Article 9, GDPR must be met before this information can be released. Sensitive data is classified as: Race or Ethnic origin, Political Opinion, Religious or other beliefs, Trade Union, Physical or Mental Health issues (i.e. health record files), Sex life, Commission of Offences, Criminal Proceedings.

4. Summary of (Personal Data) and Article 9, GDPR Conditions (special classes of data)

<table>
<thead>
<tr>
<th>Article 6 (GDPR) – at least one condition needs to be met:</th>
<th>Article 9 (GDPR) – at least one condition needs to be met:</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Consent of the data subject</td>
<td>(1) Explicit consent of the data subject</td>
</tr>
<tr>
<td>(2) Contractual necessity</td>
<td>(2) Vital interests of the data subject</td>
</tr>
<tr>
<td>(3) Non contractual legal obligation</td>
<td>(3) Charity or not for profit bodies</td>
</tr>
<tr>
<td>(4) Vital interests of the data subject</td>
<td>(4) Data manifestly made public by data subject</td>
</tr>
<tr>
<td>(5) Public Interest or in exercise of official authority</td>
<td>(5) Legal claims</td>
</tr>
<tr>
<td>(6) Legitimate interest of the data Controller</td>
<td>(6) Substantial public interest</td>
</tr>
<tr>
<td></td>
<td>(7) Health and Social Care</td>
</tr>
<tr>
<td></td>
<td>(8) Public Health</td>
</tr>
<tr>
<td></td>
<td>(9) Historical, statistical or scientific purpose</td>
</tr>
<tr>
<td></td>
<td>Order by Secretary of State (I.E. Data Protection</td>
</tr>
<tr>
<td></td>
<td>Subject Access Modification (Health) Order 2000</td>
</tr>
<tr>
<td></td>
<td>(SI2000/413))</td>
</tr>
</tbody>
</table>

DPA also allows where processing is by order by Secretary of State or Courts
Third Party Information

The Data Protection Act 2018 states third party means “any person other than the data subject, the Data Controller or any data processor or other person authorised to process data for the controller or processor”

Generally speaking third party information has two components:

A. The first one is that it can be any individual who is identifiable from the records who is not the applicant. Note that this does not apply to healthcare professionals.

B. The second is that in an organisation context, a third party is any organisation / agency which is not the Trust, i.e. where the Trust holds information from other organisations, those other organisations remain organisationally responsible for their own records as the “data controller” and constitute third parties.

Data Subject

According to the Data Protection Act 2018, the data subject is a living individual (not an organisation) who is the subject of the personal data.

Information Governance Lead

The Data Protection Officer has a duty to ensure that the requirements of the Data Protection Act 2018 are upheld and the Chief Executive through the Senior Information Risk Owner has overall responsibility for implementation of this policy.

Caldicott Guardian

The Caldicott Guardian is responsible for ensuring that the organisation is compliant with the confidentiality requirements of the Data Protection Act 2018.

Senior Information Risk Owner

Responsibility for management of compliance with Data Protection legislation.

Health Records Manager.

Responsibility for the implementation of and compliance with this policy and SAR procedures for access to clinical records

Head of Human Resources

Responsibility for the implementation of and compliance with this policy and SAR procedures for access to staff and related non-clinical records
12. Information Governance Lead/ Data Protection Officer

Has responsibility for:

Specialist advice regarding “information rights”,
Assuring compliance with the procedure,
That staff are supported to understand their responsibilities and
That appropriate mechanisms are in place to deal with any Data Protection
issues which may arise within the Trust.

13. Employees

Heads of Service and Managers are responsible for ensuring that information
is disclosable under the requirements of the Data Protection Act, and for
ensuring that requests for information are provided in a timely fashion. All
employees, whether permanent, temporary or contract, should be aware of
this policy and adhere to the principles set out. They should all be aware of
how to access this policy and where to seek further advice about this policy.
Employees should also note that access to your own health and personnel
records should always be via a subject access request. Accessing your own
records in any other way will be considered a breach of your duty of
confidentiality. If clarification is required please contact the Information
Governance department.

14. Approval Responsibility

The Policy Council and Information Governance Steering Group are
responsible for approving this procedure and forwarding to other relevant
groups for information.
Appendix 2 - Request for Access to Personal Information Form

Application for Access to Your Records
(Data Protection Act 2018 and other relevant legislation)
Please read accompanying notes prior to completing this form

Section 1 – Patient Details

<table>
<thead>
<tr>
<th>Surname</th>
<th>If the patient’s name/address was different at the time of the treatment(s) for the record requested, please provide details below.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forename (s)</td>
<td></td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Postcode</td>
<td></td>
</tr>
<tr>
<td>Contact Tel No.</td>
<td></td>
</tr>
</tbody>
</table>

Section 2 – Applicant Details (if different from the above)

<table>
<thead>
<tr>
<th>Surname</th>
<th>Forename (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date of Birth</td>
<td>Address</td>
</tr>
<tr>
<td>Contact Tel No.</td>
<td>Postcode</td>
</tr>
</tbody>
</table>

Please tick (✓) which of the following applies:

☐ I am the patient (Please enclose a photocopy of proof I.D).

☐ I am the parent requesting these records on behalf of my child (Please enclose a photocopy of proof of parental responsibility i.e. parental responsibility order issued by the court or a photocopy of child’s full birth certificate).

☐ I have been asked to act by the patient/client and attach the patient/client’s written authorisation (If the patient is unable to provide written authorisation, please enclose a photocopy of proof power attorney/court order).

☐ I am requesting the records of a deceased patient (please enclose proof of appointment under Will or Grant of Probate).
Section 3 – Information Requested

<table>
<thead>
<tr>
<th>Type of Request:</th>
</tr>
</thead>
<tbody>
<tr>
<td>I wish to view the records personally at the trust [ ]</td>
</tr>
<tr>
<td>I wish to have a photocopy of the notes sent to me [ ]</td>
</tr>
</tbody>
</table>

Please provide details of specific records you wish to view

<table>
<thead>
<tr>
<th>Date Attended</th>
<th>Hospital or Location</th>
<th>Ward or Clinic or speciality</th>
<th>Consultant or Health Professional</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please provide any other information i.e. reason for attendance, nature of treatment or illness

Section 4 - Authorisation - If the named applicant is acting on your behalf please complete.

I hereby authorise East Lancashire Hospitals NHS Trust to release personal health data relating to me to ........................................................................................................................................................................................................................................................................

Signature.................................................................. Date............................................

Section 5 – Declaration

☐ I have read the attached notes and understand that a fee may be required prior to the release of any information.

☐ I have provided all the information and supporting documentation as outline in the checklist below.

Applicant Signature: ................................................................. Date: .........................

*Please note Health Records will only be disclosed with the consultants consent*
Application to Health Records Request form Checklist (Please tick ✓ to confirm)

- Have you correctly completed the personal details in section 1
- Have you signed and dated the declaration.
- Have you included signed consent from the patient (if required)
- Have you enclosed photocopies of the proof of identification/authorisation documents? (We require proof of identity AND address).
- Have you provided as much information as possible about the exact information you require.
- Have you read the attached information (see page 4)

Failure to correctly complete the form and provide supporting information may result in the application being returned to you, which will delay the process.

Guidance notes for Application to Health Records Request Form

Your Rights
The Data Protection Act 2018, allows you to find out what information about you is held on computer and in certain manual records. This is known as “right of subject access”. As the ‘holder’ of your records the Trust is known as the ‘data controller’, and the patient/employee is known as the ‘data subject’ under the Act. The Act supersedes the previous rights of access for living patients under the Access to Health Records Act 1990.

Terms & Conditions
You are entitled to receive a copy but should note that a charge will usually be made for repeat requests or those considered obviously excessive. You should also be aware that in certain circumstances your right to see some details in your health records may be limited in your own interest or for other reasons. The Trust has a written procedure which allows patients (data subjects) to access their health records.

Any information you have supplied in making this request will be treated in confidence. It will only be used for the purpose of carrying out the search for your information in accordance with the Data Protection Act. The Trust is only responsible for providing information which is held by us.

If your request indicates the release of information to a Third Party (e.g. a solicitor, insurance company or relative) a signed certified consent must be attached to the request form or other relevant proof of entitlement provided.

Proof of Identity
East Lancashire Hospitals NHS Trust has a duty to keep information secure and will only provide information to you if we are satisfied that you are the person entitled to receive it. Your application must be certified. The individual certifying your application must not be a family member. All applicants must provide a photocopy of proof of identity (driving license, passport, or birth certificate) AND a photocopy of proof of address (utility bill or bank statement). Please note you must provide copies of BOTH of these documents in order for us to process your request.
Fees

There are no fees for subject access requests unless requests are manifestly unfounded or excessive, in particular because they are repetitive. In this case the costs will be:

- 50 sheets and under - £0.50 per sheet, plus £20 Admin fee, plus postage costs

Anything above this will be as follows:

- £0.25 per sheet, plus £20 hourly admin fee, plus postage costs

Radiology images will be charged a fee of £25 for each duplicate request.

DO NOT SEND PAYMENT NOW, WE WILL SEND YOU AN INVOICE ONCE THE TOTAL PRICE HAS BEEN CALCULATED.

Notes

- You do not need to give a reason to access your health records.
- Please provide as much information as possible.
- Please ensure that all information provided is accurate and up to date.
- Once all the relevant information has been received, the Trust has up to 40 calendar days in which to respond to your request.
- If access has recently been given, access may not be given until a reasonable time interval has elapsed. What is reasonable depends on the nature of the information, the purposes for which is processed and when it was altered or added to.
- There is no minimum age for applications. Children can apply for their own records provided they are capable of understanding the nature of the request.
- A parent or guardian can only apply on the child’s behalf if (a) the child has given consent (b) the child is too young to have the understanding to make the request. Please note that a parent does not have legal right of access to their child’s records.
- We can only supply East Lancashire NHS Trust records to you.

Please return all completed forms to:

Access and Requests Office
Health Records Department
Burnley General Hospital
Casterton Avenue
Burnley
Lancashire
BB10 2PQ

Further information can be obtained by telephone on (01282) 803031 or 803032
Appendix 3 - Request for Access to Personal Information Form for employee records/notes

Application for Access to Employee Records/Notes.
(Data Protection Act 2018 and other relevant legislation)
Please read accompanying notes prior to completing this form

Section 1 – Staff Details

<table>
<thead>
<tr>
<th>Surname</th>
<th>If the name/address was different at the time of employment for the record requested, please provide details below.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forename(s)</td>
<td></td>
</tr>
<tr>
<td>Date of Birth</td>
<td></td>
</tr>
<tr>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>Postcode</td>
<td></td>
</tr>
<tr>
<td>Contact Tel No.</td>
<td></td>
</tr>
</tbody>
</table>

Section 2 – Applicant Details (if different from the above)

<table>
<thead>
<tr>
<th>Surname</th>
<th>Forename(s)</th>
<th>Date of Birth</th>
<th>Address</th>
<th>Contact Tel No.</th>
<th>Postcode</th>
</tr>
</thead>
</table>

Please tick (✔) which of the following applies:

☐ I am the member of staff whose record is being requested (Please enclose a photocopy of proof I.D.)

☐ I am the member of staff to whom notes being requested pertain to (Please enclose a photocopy of proof I.D.)

☐ I have been asked to act by the staff member/client and attach the written authorisation (If the member of staff is unable to provide written authorisation, please enclose a photocopy of proof power attorney/court order).
Section 3 – Information Requested

<table>
<thead>
<tr>
<th>Type of Request:</th>
</tr>
</thead>
<tbody>
<tr>
<td>I wish to view the records personally at the trust ☐</td>
</tr>
</tbody>
</table>

Please provide details of specific records you wish to view

Please provide any other information

Section 4 - Authorisation - If the named applicant is acting on your behalf please complete.

I hereby authorise East Lancashire Hospitals NHS Trust to release personal health data relating to me to ………………………………………………………………………………………………………………………………………

Signature……………………………………………… Date………………………………………………

Section 5 – Declaration

☐ I have read the attached notes and understand that a fee may be required prior to the release of any information.

☐ I have provided all the information and supporting documentation as outline in the checklist below.

Applicant Signature: …………………………………………… Date: ………………………

Application to Records Request form Checklist (Please tick ✓ to confirm)

☐ Have you correctly completed the personal details in section 1

☐ Have you signed and dated the declaration.

☐ Have you included signed consent from the staff member (if required)

☐ Have you enclosed photocopies of the proof of identification/authorisation documents? (We require proof of identity AND address).

☐ Have you provided as much information as possible about the exact information you require.

☐ Have you read the attached information

Failure to correctly complete the form and provide supporting information may result in the application being returned to you, which will delay the process.
Guidance notes for Application to Records Request Form

Your Rights
The Data Protection Act 2018, which came into force on 1 March 2000, allows you to find out what information about you is held on computer and in certain manual records. This is known as “right of subject access”. As the ‘holder’ of your records the Trust is known as the ‘data controller’, and the patient/employee is known as the ‘data subject’ under the Act. The Act supersedes the previous rights of access for living patients under the Access to Health Records Act 1990.

Terms & Conditions
You are entitled to receive a copy but should note that a charge will usually be made. You should also be aware that in certain circumstances your right to see some details in your health records may be limited in your own interest or for other reasons. The Trust has a written procedure which allows patients (data subjects) to access their health records.

Any information you have supplied in making this request will be treated in confidence. It will only be used for the purpose of carrying out the search for your information in accordance with the Data Protection Act 2018. The Trust is only responsible for providing information which is held by us.

If your request indicates the release of information to a Third Party (e.g. a solicitor, insurance company or relative) a signed certified consent must be attached to the request form or other relevant proof of entitlement provided.

Proof of Identity
East Lancashire Hospitals NHS Trust has a duty to keep information secure and will only provide information to you if we are satisfied that you are the person entitled to receive it. Your application must be certified. The individual certifying your application must not be a family member. All applicants must provide a photocopy of proof of identity (driving license, passport, or birth certificate) AND a photocopy of proof of address (utility bill or bank statement). Please note you must provide copies of BOTH of these documents in order for us to process your request.

Fees
To provide copies:

Current members of staff will not be charged for access to their records or notes pertaining to them. There will be a charge for repeat requests and requests considered excessive

- 50 sheets and under
  - £0.50 per sheet, plus £20 Admin fee, plus postage costs

Anything above this will be as follows:
- £0.25 per sheet, plus £20 hourly admin fee, plus postage costs

DO NOT SEND PAYMENT NOW, WE WILL SEND YOU AN INVOICE ONCE THE TOTAL PRICE HAS BEEN CALCULATED.

Notes
- You do not need to give a reason to access your records.
- Please provide as much information as possible.
- Please ensure that all information provided is accurate and up to date.
- Once all the relevant information has been received, the Trust has up to 40 calendar days in which to respond to your request.
- If access has recently been given, access may not be given until a reasonable time interval has elapsed. What is reasonable depends on the nature of the information, the purposes for which it is processed and when it was altered or added to.
- We can only supply East Lancashire NHS Trust records to you.
Please return all completed forms to:

Employee Relations Teams
Human Resources
Park View Offices
Royal Blackburn Teaching Hospital
Haslingden Road
Blackburn
BB2 3HH

Tel: 01254 732977 or internal ext 82977  Email: employee.relations@elht.nhs.uk
Appendix 4 - ID Checklist

Acceptable ID documents for Subject Access Requests

To make a Subject Access Request for yourself, you will be asked to provide two forms of ID documentation, one being proof of identity and one to confirm your address, before any information will be released.

All forms of acceptable documentation are listed in the tables below. Please note, ONE document from each of the tables below should be provided (please send copies not originals): Please tick against the documents you have provided.

PROOF OF IDENTITY

Acceptable Photo Personal Identity Documents

- Current UK (Channel Islands, Isle of Man or Irish) passport or EU/other nationalities passports
- Passports of non-EU nationals containing UK stamps, a visa or a UK residence permit showing the immigration status of the holder in the UK *
- Current UK (or EU/other nationalities) Photo-card Driving Licence (providing that the person checking is confident that non-UK Photo-card Driving Licences are genuine
- A national ID card and/or other valid documentation relating to immigration status and permission to work *

Any documents not listed above are not acceptable forms of identification e.g. organisational ID card.

Acceptable Non-Photo Personal Identity Documents

- Full UK Birth Certificate – issued within 6 weeks of birth
- Current Full Driving Licence (old version); (Provisional Driving Licences are not acceptable)
- Residence permit issued by Home Office to EU Nationals on inspection of own-country passport
- Adoption Certificate
- Marriage/Civil Partnership certificate
- Divorce or annulment papers
- Police registration document
- Certificate of employment in HM Forces
- Current benefit book or card or original notification letter from the Department of Work and Pension (DWP) confirming legal right to benefit
- Most recent HM Revenue and Customs (previously Inland Revenue) tax notification
- Current firearms certificate
- Application Registration Card (ARC) issued to people seeking asylum in the UK (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms)
- GV3 form issued to people who want to travel in the UK without valid travel documents
- Home Office letter IS KOS EX or KOS EX2
- Building industry sub-contractors certificate issued by HM Revenues and Customs (previously Inland Revenue)

CONFIRMATION OF ADDRESS

To confirm the address, the following documents are acceptable:
Recent utility bill or certificate from a supplier of utilities confirming the arrangement to pay for the services on pre-payment terms (note: mobile telephone bills should not be accepted as they can be sent to different addresses). Utility bills in joint names are permissible*

<table>
<thead>
<tr>
<th>Document Type</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local authority tax bill (valid for current year)*</td>
<td></td>
</tr>
<tr>
<td>Current UK photo-card driving licence (if not already presented as a personal ID document)</td>
<td></td>
</tr>
<tr>
<td>Current Full UK driving licence (old version) (if not already presented as a personal ID document)</td>
<td></td>
</tr>
<tr>
<td>Bank, building society or credit union statement or passbook containing current address</td>
<td></td>
</tr>
<tr>
<td>Most recent mortgage statement from a recognised lender*</td>
<td></td>
</tr>
<tr>
<td>Current local council rent card or tenancy agreement</td>
<td></td>
</tr>
<tr>
<td>Current benefit book or card or original notification letter from Department of Work and Pensions (DWP) confirming the rights to benefit</td>
<td></td>
</tr>
<tr>
<td>Confirmation from an electoral register search that a person of that name lives at the claimed address*</td>
<td></td>
</tr>
<tr>
<td>Court Order*</td>
<td></td>
</tr>
</tbody>
</table>

* The date on these documents should be within the last 6 months (unless there is a good reason for it not to be e.g. clear evidence that the person was not living in the UK for 6 months or more) and they must contain the name and address of the applicant
Appendix 5- Agreement to disclosure of Records form

This form must be retained with a copy of the documents to be released.

Documents must not be released directly to the applicant

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Applicant’s Full Name</td>
</tr>
<tr>
<td></td>
<td>..........................................................................................................................</td>
</tr>
<tr>
<td>2.</td>
<td>Applicant’s Date of Birth</td>
</tr>
<tr>
<td></td>
<td>..........................................................................................................................</td>
</tr>
<tr>
<td>3.</td>
<td>Applicant’s Current Address</td>
</tr>
<tr>
<td></td>
<td>..........................................................................................................................</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AUTHORISER’S DECLARATION – Please tick relevant box or boxes</td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>I agree to the attached records being released to the above named person or the person’s named representative</td>
</tr>
<tr>
<td>2.</td>
<td>Part or whole of the records have been withheld on the grounds that:</td>
</tr>
<tr>
<td></td>
<td>a. Disclosure is likely to cause serious harm to the physical or mental health of the person or of another individual</td>
</tr>
<tr>
<td></td>
<td>b. Access would disclose information relating to, or provided by, a third party who has not consented to their information being disclosed</td>
</tr>
<tr>
<td></td>
<td>c. The record contains information the person expressly stated must not be released</td>
</tr>
<tr>
<td></td>
<td>d. The person is under 16 and I do not think he / she fully understands what an application to see their records means</td>
</tr>
</tbody>
</table>

Staff Name: ...........................................................................................................

Post held: ..................................................................................................................

Signature: ..................................................................................................................

Date: .........................................................................................................................
Appendix 7- Subject Access Request Process Flow Map

Procedure for managing continuing healthcare Subject Access Requests

The details of the SAR to be logged on the SAR Logbook

Staff to inform the relevant department immediately when a SAR is received.

Department to acknowledge receipt of SAR to applicant

Use Acknowledgement Letter and Acceptable ID documents for Subject Access doc (if required)

Department to check if sufficient info received, 2 forms of ID and/or to clarify request

Department to inform applicant that ID and / or further clarification is required

Clock Stops

Clarity given within 10 working days (clock stops until info received)

Yes

Clarification given within 10 working days (clock stops until info received)

Deadline

No

Fee received within 10 working days (clock stops until received)

Yes

Department to inform applicant of the fee to be charged. Use fee letter template.

Yes

Yes

Records and disclosure proforma returned?

Escalate to Caldicott Guardian

Close SAR and logged closed date on SAR Logbook

Department to arrange with service for collation of records

Arrange secure transfer or collation of info for SAR

Head of Service to complete Agreement to Disclosure of Records Form

Yes

Check the information – Does an exemption apply?

Yes

Department to redact information due to exemption or obtain consent to disclose 3rd party information – Use Response letter with no information provided template

Close SAR and logged closed date on SAR Logbook

Department to inform of SAR

Department to inform of fee

Department to inform of records

No

No

No

No

No

Yes

No