East London
NHS Foundation Trust

Access to Records Policy

Version number:	1.4
Consultation Groups:	Information Governance Steering Group
Approved by (Sponsor Group):	Information Governance Steering Group
Ratified by:	Quality Committee
Date ratified:	September 2019
Name and Job Title of author:	Ari Garboggini, Information Governance Manager
Executive Director Lead:	Mason Fitzgerald, Director of Planning &
Implementation Date:	August 2019
Last Review Date:	September 2019
Next Review Date:	July 2022

Services	**Applicable to**
Trustwide	√

Version Control Summary

Version	Date	Author	Status	Comment
1.0	14.10.11	Head of Information Governance	Final	New policy incorporating previous Access to Health Records policy, Access to Non Health Records policy and Newham PCT Information Disclosure Guidelines
1.1	23.04.13	Head of Information Governance	Final	Section 9.6 (Fees) strengthened
1.2	15.01.15	Information Governance Assets Manager	Final	Minor amendments for consistency of job role titles and addition of monitoring, reference and additional documents sections in line with Trust Policy template
1.3	08.11.18	Information Rights Manager		Policy reviewed to incorporate the GDPR/Data Protection Act 2018. Also some procedural change regarding SAR to HR.
1.4	02.07.19	Information Governance Manager		Policy reviewed to incorporate the ICO audit actions (updating third parties about inaccuracies corrected; procedure for deleting information; acknowledge verbal requests as valid option).

Contents

1.0 Introduction

Individuals have a right to apply for access to their personal information, and in some cases, information held about other people. This policy ensures individuals can exercise this right.

2.0 Purpose

This policy sets out who may apply for access, their rights, relevant legislation, responsibilities and the subject access requests handling process. This policy will be on the Trust's intranet under Information Governance.

3.0 Duties

The Associate Director of Information Governance (who is the Data Protection Officer) is responsible for protecting the confidentiality of a patient and service-user information and enabling appropriate information-sharing and has overall responsibility for ensuring adherence to this policy. A Data Protection Officer is a legal requirement under Article 37 of the General Data Protection Regulation. The Data Protection Officer monitors internal compliance with data protection matters, provides advice and information on data protection obligations, acts as a contact point for data subjects and the Information Commissioner's Office. The Data Protection Officer is independent and has direct communication with the Board.

The Information Rights Manager will oversee the systems and procedures that support the implementation of this policy, co-ordinate any subject access requests where it is unclear where the requester's personal information is located, and provide support and advice where the request is sensitive or complex. The Information Rights Manager will liaise with the Trust's Data Protection Officer when required.

Designated local Access to Records leads will have a system in place to respond to requests promptly, within agreed timescales, will identify any exemptions and third party information and will ensure the information is reviewed by an appropriate individual prior to its release.

Individuals responsible for reviewing and approving information for release in response to a subject access request will do so within in a timely manner that enables release of the information within statutory timeframes.

All individuals accessing personal information in response to a subject access request or for other purposes must understand and comply with the law, Confidentiality Code of Conduct and Trust information governance policies.

4.0 Rights of access to records containing the personal information of living individuals

Individuals have the right to be informed if the Trust holds personal data about them and in most circumstances to be given a copy of that data, irrespective of when it was compiled. The following sections set out the relevant legislation, who may apply for access, fees, time limits and an outline of the process Access to Records leads follow when dealing with subject access requests.

5.0 Who may apply for access

5.1 Access by an individual

The following individuals may apply for access:

- **Competent service users** - may apply for access to their own records subject to certain exemptions, or may authorise third parties such as lawyers, employers or insurance companies to do so on their behalf. It is not necessary to give a reason why.

- **Children and young people -** competent young people may apply for access to their own records. Legally there is no automatic presumption of capacity for individuals under the age of 16 so they must demonstrate they have sufficient understanding. Where in the view of the health professional a child is considered capable of making decisions about his/her medical treatment, his/her consent should be sought before a parent or other third party can be given access to the child's personal information. However, children aged 12 or over are generally expected to have the capacity to give or withhold consent to the release of information from their health records.

- **Staff, contractors, volunteers -** may apply for access to their own records. People currently working should contact their HR Adviser who will arrange access to the records. Ex-staff should contact their HR Adviser if known and the Information Governance Team will coordinate the process. If HR Adviser is not known, then the Information Rights Manager should be contacted.

5.2 Access by someone acting for an individual

- **Parents -** may have access to their children's records if this is not contrary to a competent child's wishes. Any person may apply for parental responsibility but not all parents automatically have parental responsibility. For children born after 1st December 2003 both biological parents have parental responsibility if they are registered on a child's birth certificate. For children born before this date, 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 sometime thereafter. If the parents have never been married only the mother has automatic 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 lives with one or other parents there is no obligation to inform the parent the child lives with if the other parent seeks access to the records of the child, providing the parent seeking access can demonstrate parental responsibility as outlined above.

  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 the appointment of a guardian or on the order of a court. A local authority acquires parental responsibility (shared with the parents) whilst a child is the subject of a care or supervision order.

  The Trust is entitled to refuse access to a parent or individual with parental responsibility if knowledge of the information contained in the child's record could cause serious harm to the child or another individual.

- **Next of kin -** the term 'next of kin' does not have a formal legal status. A next of kin has no rights of access to medical records and cannot give or withhold consent to the sharing of information on a patient's behalf.

- **Solicitors -** information can be released to solicitors provided the patient has given signed and valid consent to the disclosure. If there is any doubt that the patient understands the nature and extent of the information being disclosed, the health professional should discuss this with the patient prior to disclosure.

- **Solicitors acting for another party -** consent from the patient should be obtained prior to disclosing any information. If the patient refuses, or the health professional does not consider it appropriate to disclose, the solicitor may apply to the Court for an Order requiring disclosure. If a Court Order is received requiring the Trust to disclose information then the Information Rights Manager must be notified.

- **Individuals on behalf of adults who lack capacity -** an individual's mental capacity must be judged in relation to the particular decision being made. If the health professional believes the patient has the requisite capacity to give or withhold consent to the disclosure of information then their consent is necessary where a relative or third party requires access to their records.

  Where the patient does not have capacity, information may be shared with any individual authorised to make proxy decisions. The Mental Capacity Act contains powers to nominate individuals to make health and welfare decisions on behalf of incapacitated adults (see below). The Court of Protection can also appoint deputies for this purpose. This may entail giving access to relevant parts of a patient's medical records unless the health professional can demonstrate this would not be in the patient's best interests.

- **Power of Attorney –** there are two types of Power of Attorney:

  - An ordinary Power of Attorney (PoA) gives another person the power to act on an individual's behalf with regard to property or financial affairs. It does not include health matters and does not give a right of access to an individual's health record without the consent of that individual.

  - An Enduring Power of Attorney (EPA) does not extend to personal welfare and therefore does not give the right of access to health records of another individual.

  - A Lasting Power of Attorney (LPA) replaced the Enduring Power of Attorney in October 2007 as part of the Mental Capacity Act 2005. It relates either to property and affairs or to personal welfare. It can only be used in the event of an individual's mental incapacity and must be registered to take effect. Health information of another individual can only be disclosed where there is a Personal Welfare Power of Attorney. The Trust must be assured before disclosing health information that the individual lacks mental capacity.

- **Independent Mental Health Advocate (IMHA) -** a statutory form of advocacy that provides safeguards for certain qualifying individuals. An IMHA is entitled under the Mental Capacity Act 2005 to ask for access to the individual's health records and to make copies. No part of the record should be withheld from the IMHA.

5.3 Access to an individual's records by other agencies

- **Police -** if the police do not have a Court Order or warrant they may request voluntary disclosure of a patient's health records under Schedule 2 Part 1

Paragraph 2 of the Data Protection Act 2018. There is no obligation to disclose records to the police. They should usually only be disclosed where the patient has given consent or there is an overriding public interest.

Disclosure in the public interest is made to prevent a serious threat to public health, national security, the life of an individual or third party or to prevent or detect serious crime. Serious crime includes murder, manslaughter, rape, treason, serious fraud, state security and kidnapping or abuse of children or other vulnerable people. It does not include theft, minor fraud or damage to property. See also the section on other legislation and statutory requests.

- **Other NHS Trusts -** in most circumstances a patient should give consent for copies of medical records or a medical report to be sent to another Trust. This does not apply where the patient refuses consent and it is in the public interest to disclose the information, for example, when someone is at risk.

The advice of the Information Rights Manager should be sought where clarification is required or where a request may be sensitive or contentious.

5.4 Access to the records of deceased people

The only statutory right of access to the records of deceased patients is under the Access to Health Records Act 1990. The Act provides a small cohort of people with a statutory right to apply for access to information contained within a deceased person's record. These individuals are defined under Section 3(1)(f) of the 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 a deceased person's estate.

A personal representative has an unqualified right of access to a deceased person's record and need give no reason for applying for access. Other individuals have a right of access only where they can establish a claim arising from a patient's death. Only information directly related to the claim should be disclosed.

Requests must be responded to within one calendar month.

In some circumstances individuals who do not have a statutory right of access under the Act may request access to a deceased person's record, such as helping a relative to understand the cause of death or the actions taken to ease the patient's suffering. Whilst longstanding legal advice is that the duty of confidentiality extends beyond death, requests should be considered on a case by case basis, be proportionate, in the public interest and not simply rejected. Consideration should include any preference expressed by the deceased prior to death, the distress or detriment that any living individual might suffer following disclosure, any loss of privacy that might result and the impact on the deceased's reputation.

The advice of the Information to Rights Manager should be sought where clarification is required or where a request may be sensitive or contentious.

6.0 Relevant legislation

6.1 Data Protection Act 2018

Section 45 of the Data Protection Act 2018 gives living individuals or their authorised representative the right to apply for access to their personal data. It applies equally to all relevant records and is not confined to health records.

An individual who makes a written request is entitled to be:

- Told whether any personal data is being processed
- Given a description of the personal data, the reasons for its processing, and whether it will be shared with other individuals or agencies
- Given a copy of the information or to access it on Trust premises`
- Where available, given details of the source of the data

Requests must be responded to within one calendar month.

The Trust does not normally make a charge for individuals or third parties (such as solicitors) who make a subject access request. Please see more details on the Fees section.

6.2 Access to Health Records Act 1990

If an applicant requests access to the records of a deceased patient, the only right of access is under the Access to Health Records Act 1990. There is an ethical obligation to respect a patient's confidentiality beyond death. This is also set out in Section 41 of the Freedom of Information Act 2000.

The section on the 'Rights of access to the records of deceased people' explains this in detail.

6.3 Access to Medical Reports Act 1988

This Act governs access to medical reports written by a medical practitioner who is / has been responsible for the clinical care of a patient for insurance or employment purposes. A third party cannot ask for a medical report for employment or insurance reasons without the individual's knowledge and consent.

The individual can apply for access to the report at any time before it is supplied to the employer / insurer, subject to certain exemptions including where it would cause serious physical or mental harm to the individual or a third party or identify a third party who has not consented to the release of that information.

It should not be supplied to the employer / insurer until the individual has been given access unless 21 days have passed since the individual has communicated about making arrangements to see the report. Once access has been given it should not be supplied to the employer / insurer until the individual has consented. Individuals have the right to request in writing amendments to the report if any part is incorrect or the right to have attached a note of their views if the medical practitioner declines to amend the report. Individuals also have the right to refuse to consent to release of the report.

The Trust makes a charge for requests made under this Act. These charges are laid out in the Fees section.

6.4 Other legislation and statutory requests

- **Court Orders –** there is a legal duty to disclose information in response to an order of the Courts. The advice of the Information Rights Manager should be sought prior to disclosing information. These are usually urgent, are unequivocal and failure to respond can result in staff being subpoenaed to appear in Court. It is not necessary in most circumstances to seek the consent of the individual whose information is being requested. The Information Rights Manager will advise on a case by case basis.

- **Road Traffic Act 1988 –** when asked, there is a legal duty to provide the police with the name and address of a driver who is allegedly guilty of an offence under this Act. Clinical information should never be disclosed. There is no duty to advise the police when an individual is likely to attend an appointment at the Trust. It is not necessary to seek the consent of the individual whose information is being requested.

- **Prevention of Terrorism Act 1989 and Terrorism Act 2000 –** there is a legal duty to inform the police if information is known about terrorist activity, including personal information. It is not necessary to seek the consent of the individual and it may endanger safety if the consent of the individual is sought.

- **Police and Criminal Evidence Act –** the Trust may pass on information to the police if it is believed someone is at serious risk of harm or death. Serious arrestable offences include murder, rape, kidnapping and causing death by dangerous driving. They do not include minor offences such as theft. The Trust should consider whether it is appropriate to seek the consent of the individual prior to disclosure.

- **Children Act 1989, sections 17 and 47 –** the police or local authority may make enquiries when deciding whether to take action to safeguard a child's welfare. Consent does not have to be gained from the child or parents but it is good practice to do so if appropriate.

- **Crime and Disorder Act 1998, section 115 –** the Act provides for anti-social behaviour orders to be applied by the police or local authority against individuals aged ten or over. Section 115 of the Act permits the disclosure of personal information that may otherwise be prohibited. There is no duty to disclose. This means information given in confidence should not be disclosed unless there is a clear public interest in doing so as the conditions of the Data Protection Act 2018 and the common law duty of confidence apply.

7.0 Duty of confidence

All individuals within the Trust have a duty of confidence. This is included in employment and other contracts. This means any personal information given or received in confidence for one purpose should not be used for a different purpose without the consent of that individual or their representative unless there is a legal duty to do so.

8.0 General procedure for dealing with subject access requests

8.1 Receipt and appraisal of new requests

All requests for access to personal information should be forwarded to the local Access to Records Lead, who will ensure appropriate consent from the individual who is the subject of the request, has been received.

Once appropriate consent has been received, the Access to Records Lead will co-ordinate the process and ensure the disclosure is made within the relevant timescale. This applies to requests for access to the personal information of both staff and service users.

A list of Access to Records Leads is available from the Information Governance Team.

The process below should be followed by Access to Records Leads. All individuals have a duty to pass any requests promptly to the relevant lead for action.

Access to Records leads should seek the advice of the Information Rights Manager where clarification is required or a request may be sensitive or contentious.

8.2 Dealing with general requests and queries

Where general requests for information are received, or it is unclear which Access to Records lead should be contacted, the Information Rights Manager's team will undertake the following actions:

- **Requests from staff / contractors / volunteers not currently working in the Trust –** ensure relevant identification is received, acknowledge receipt to requestor and subsequently liaise with HR, who will provide the information requested to the Information Rights Manager. The Information Rights Manager will then co-ordinate the request and provide all disclosable requested information. This is not limited to HR records and dependent on the request, may include the co-ordination of emails, minutes of meetings etc.

- **Requests from patients where it is unclear where care was received –** perform a search on RiO or ask other electronic clinical systems owners to check to see if the patient can be identified, acknowledge the request with the requester (advising where the care was received and who to contact) and pass to the relevant Access to Records lead. Where care has been received in more than one Directorate and the requester wishes to receive all their personal information, the Access to Records lead where care was last received will co-ordinate the process

- **General requests from the police / other agencies -** perform a search on RiO or ask other electronic clinical systems owners to check to see if the patient can be identified then advise the police / other agency who should be contacted for access to the records if there is a just reason for disclosure.

9.0 Guidance for Access to Records leads

9.1 Reasons for requiring access

There is no obligation for an individual or third party acting on behalf of an individual to state why access to their personal information is required.

It is helpful to encourage individuals to state what information is required, especially where it relates only to a particular episode of care or period of employment. The form at Appendices 1 - 2 can be used for this purpose.

9.2 Intended litigation

Solicitors or anyone acting in a legal capacity must confirm if litigation is intended against the Trust. The Information Rights Manager and Associate Director of Legal Affairs must always be notified by the Access to Records lead where litigation is intended. This must be within five days of receipt of the request and before any disclosure takes place.

9.3 Confirming identity

The Trust must satisfy itself as to the identity of the person making the request to ensure information is released only to the data subject or to a third party with the data subject's consent. The clock does not start until identification has been confirmed.

All requests can be in writing or verbal and must be accompanied by proof of identity. Applications should be accompanied by photocopies of two different official documents which between them provide sufficient information to prove the name, date of birth, current address and signature of the individual whose personal information is sought. For example, driving licence, medical card, birth certificate, passport, bank statement (with financial information redacted) utility bill.

The form on the information governance forms page on the intranet can be used for this purpose.

Personal representatives of deceased people are required to provide evidence of their right to act in this capacity.

The Trust will refuse to comply with a request until identification has been confirmed. This may, however, be waived in extenuating circumstances where there is absolutely no doubt regarding the identity of the applicant. Service users currently admitted to a ward do not need to provide identity whilst receiving inpatient care. Discretion may also be used where a service user receiving community care makes a face to face request to the individual currently providing their ELFT care. The individual proving care must be assured the service user genuinely wants access to their records and is not being unduly influenced by their family, carers or friends.

The police, Courts and other agencies acting in an official capacity are not required to provide proof of identity.

9.4 Consent

Where a third party applies for access to the records of an individual, the individual must give explicit (written) consent.

There is no legal time limit after which consent to disclose becomes invalid. However, if there has been a significant interval between the time written consent was provided and the time the request was made, it is good practice to confirm the data subject is still willing to agree to the disclosure. This is particularly important if the request is made via a solicitor or insurance company, where it is believed the individual may now have a different view, or where the capacity to consent may have changed.

Applications from Solicitors will be accepted without identification documentation providing the request is received on headed notepaper and is supported by the signed consent of the data subject.

Applications from other Third Parties will be accepted providing the identity of the data subject is confirmed, as above, signed consent is given by the data subject and the Third Party can evidence a valid name, address and relationship to the data subject.

Consent to disclose to the police and other agencies is not always necessary. The advice of the Information Rights Manager should be sought prior to disclosure.

9.5 Processing and responding to requests

The flowchart in Section 10 should be followed by Access to Records leads when processing requests.

The relevant requests templates on the information governance forms page on the intranet can be used for this purpose.

The relevant letter templates on the intranet should be used by Access to Records leads when responding to requests for disclosure of personal information.

The following principles apply:

- All requests can be verbal or in writing
- Appropriate consent should be obtained prior to releasing the information. The clock stops until valid consent is received
- Local Access to Records leads should co-ordinate the subject access process
- Services should clearly display information advising service users how to obtain copies of their records
- In exceptional circumstances information may be withheld from a service user. This is usually where it would identify a third party who has not consented to the release of their information or where release might affect the rights and freedoms of the service user or other individuals. Please ensure that a copy of what was withheld (redacted) is kept in the relevant network drive.
- The Responsible Clinician or lead care co-ordinator must make the decision to refuse access to records. This should be clearly documented in the records. The service user should be notified in writing of the decision. Care should be taken that third party information is not inadvertently released in writing to the service user

9.6 Fees

The subject cannot be charged for copies of records unless the request is 'manifestly unfounded, excessive or repetitive'. You could then charge a reasonable fee. There is currently no agreed definition of what constitutes a manifestly unfounded or excessive request, or what a reasonable fee is. This type of request will be rare. If in doubt, please contact the Information Rights Manager. Third parties requesting access on behalf of service users/patients cannot be charged either.

9.7 Response targets

The following response times apply:

- One calendar month under the Data Protection Act 2018/GDPR for the records of living or deceased people.

- All requests should be acknowledged within five working days of receipt.

Note that the clock stops until any clarification/information sought is received.

-

9.8 Minimum periods between requests for access

Where a request has previously been complied with there is no obligation to give access again until a reasonable period has elapsed. Reasonableness depends on the nature of the information, whether it has been updated, and to some extent, the reason for the request.

Contact the Information Rights Manager for further advice.

9.9 Approval from an appropriate health professional

All disclosures from patients' health records must be approved by:

- The patient's Responsible Clinician or the lead Health Care Professional
- A professional nominated by the locality clinical director where the above person has left the Trust

The Responsible Clinician Approval form on the intranet should be completed by the health professional and forwarded to the Access to Records lead before any information is disclosed to the patient or representative.

9.10 What must be disclosed

All records (subject to the caveats outlined in 'Grounds for refusing disclosure') relating to the physical or mental health of an individual should potentially be disclosed in response to a request for access to health records. This includes all paper and electronic records including X-rays, ECGs, complaints, incident investigation files etc.

Staff, ex staff, volunteers etc are entitled to be given a copy of any personal information about them. This is not limited to information contained in their HR record and may include emails, reports, minutes of meetings etc.

Applicants are entitled to be given a copy of the records or alternatively to view them on Trust premises if preferred. Copies of records disclosed must be stapled together in relevant sections and where appropriate include section tabs and a front cover.

9.11 Grounds for refusing disclosure

Information should not be disclosed if:

- Disclosure would be likely to cause harm, damage or distress to the physical or mental health of the data subject or another individual
- Disclosure would identify another individual who has not given permission for the information to be released. This does not apply to health professionals caring for the patient or individuals acting in a work context

- A third party agency has expressly not consented to disclosure of the information
- There is a duty of confidence to the individual. This includes where the information was given in the expectation it would not be disclosed to the person making the request or an individual has expressly stated it should not be disclosed to a particular individual. It also applies to the records of a young person where the young person is considered competent to make their own decisions and to information relating to an incapacitated person
- The information is subject to legal professional privilege (such as an independent report written for the purposes of litigation)
- The information is restricted by order of the Courts
- The request is vexatious. Seek the advice of the Information Rights Manager prior to responding to the request
- The information is not kept in a structured filing system i.e. there is no logical way of retrieving it. Seek the advice of the Information Rights Manager prior to responding to the request
- Where applicants have a claim arising out of a patient's death, access can only be given to the part of the record that is relevant to the claim
- If the Responsible Clinician / HCP states they would prefer to counsel the applicant prior to releasing the information. In this case the Access to Health Records lead should write to the applicant to offer an appointment

It is not necessary to advise why information is withheld. However, where information is partially redacted in response to the above points there is an obligation to disclose the remainder of the records.

9.12 Explanation of medical terms

Any terminology that might be unintelligible to the requester should be explained. As levels of understanding vary, applicants should always be advised to contact the Trust if anything is unclear or an explanation is required.

9.13 Correcting inaccurate information

Individuals have the right to seek correction of information they believe is inaccurate. Where the Trust does not accept the individual's opinion the opinion must still be recorded.

Requests must be made in writing, clearly state what needs amending and what it should be amended to. Service users and other individuals seeking correction are not permitted to alter their own records as the Trust has a responsibility to maintain them to professional standards. In the case of electronic records, service users and unauthorised individuals are not permitted to access electronic systems to make amendments as they do not have an authorised Trust log in

Factual inaccuracies (such as the wrong date of birth) may be corrected. Note that the information originally supplied should not be erased as it must be available as part of the original record.

Clinical opinion, whether accurate or not, and observations may not be amended or destroyed as they form an important part of the service user's care. Information supplied by third parties should also not be amended. In these instances the service user's opinion should be noted on the record.

In the case of health records, retention of relevant information is essential for understanding decisions that were made at the time and to audit the quality of care.

Individuals have the right to be supplied with a copy of the correction or appended note.

Third parties must be notified so that they can also update/correct their records. Individuals have the right to challenge the Trust's decision through its complaints process, and ultimately via the Office of the Information Commissioner. If an individual asks for the deletion or erasure of information the Trust holds about them, the Information Governance Department must be notified and it will consider these requests on a case by case basis so the Trust meets its obligations under article 17 of the GDPR. Third parties involved in the records must be notified about any deletions.

10. Monitoring

Access to Records Leads will provide statistics on volume and compliance status of subject access requests to the Information Rights Manager, who will then report to the Information Governance Steering Group.

11. References

The following can be found at *www.**legislation**.gov.uk*

Access to Health Records Act 1990
Data Protection Act 2018
Access to Medical Records Act 1988
Road Traffic Act 1988
Prevention of Terrorism Act 1989 and 2000
Police & Criminal Evidence Act
Children's Acts 1989
Crime & Disorder Act 1998 section 115

12. Associated Documents

Health Records Policy
Non Health Records Policy
Information Governance Strategy
Information Governance and IMT Security Policy

To be sent with all disclosures

In accordance with Article 15 of the General Data Protection Regulation we are providing you with this general information about your personal data.

We process and share your personal data in line with the Health & Social Care Act 2015, Data Protection Act 2018 and the General Data Protection Regulation.

We process your personal data to help provide you with the best possible healthcare. We share it for health and social care purposes. Not sharing information may lead to a clinical risk, safeguarding concerns or concerns about your care and may have an impact of the care we or our partners can provide. Where it supports your care we may also share your information with education and voluntary and private sector agencies. We also receive information about you from other health, social care and other agencies, and from individuals such as your carers or family. In most circumstances we do not share information about you with other individuals unless you have given us your consent.

We process basic information about you (name, address and contact details). We also process special category personal data. This is your health information. If we need it to care for you we may process other special category personal data such as your religious beliefs or sexual preferences.

We keep your personal information according to the NHS Records Management Code of Practice https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

If you think the information we hold about you is incorrect please state this in writing to elft.information.governance@nhs.net. We are able to change incorrect factual information. We are not able to change clinical opinions. If you think these are wrong, set out ahy you think this and we will add it to your clinical record.

We do not use automated decision making to make any decisions about you.

We do not send your personal data to another country or to any international organisations.

You have the right to complain about the way we process your personal data. You can contact your clinical team, speak to our PALS team at elft.palsandcomplaints@nhs.net, or contact our Data Protection Officer at elft.dpo@nhs.net.

If we are unable to resolve your concern you have the right to complain to the Information Commissioner. Call their helpline on 0303 123 1113 (local rate – calls to this number cost the same as calls to 01 or 02 numbers). Or see the ICO website https://ico.org.uk/

13. Procedure flowchart for Access to Records leads