Access to Records Policy

Version number:	1.8
Consultation Groups	Information Governance Steering Group
Approved by (Sponsor Group)	Information Governance Steering Group
Date approved	28th August 2024
Ratified by:	Quality Committee
Date ratified:	27th November 2024.
Name of originator/author:	Information Governance Manager – Bedfordshire & Luton and London
Executive Director lead:	Chief Quality Officer
Implementation Date:	November 2024
Last Review Date	August 2024
Next Review date:	August 2027

Services	Applicable
Trust wide	X
Mental Health and LD	
Community Health Services	

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).
1.5	20.09.21	Information Governance Manager		Policy reviewed to incorporate Transfer of Care requests from other NHS organisations, procedure reviewed due to staff changes
1.6	12.04.22	Information Governance Manager – Information Rights		Policy reviewed to reflect The Data Protection Act 2018 and remove references to GDPR. Additional references made where requests for information from other agencies have been received. Rights to rectification and erasure have been expanded on to include where these requests should go to. Reference to responding to an Access to Health Records Request in one month has been changed to 21

				calendar days.
1.7	19.06.23	Data Protection Officer		Staff subject access requests process strengthened
1.8	13.08.24	Information Governance Managers		Policy reviewed to reflect new team structure (remove references to Information Rights Manager and include new Senior Information Governance Managers (Systems and Compliance), and London & Bedfordshire & Luton Information Governance Manager roles). Procedure for processing CCTV footage requests has also been clarified.

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 Section 69 of The Data Protection Act 2018. 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 Senior Information Governance Managers have overall operational responsibility for the Trust's information governance function, managing the work of the information governance team, ensuring information governance is proactive and effective in supporting best practice for ELFT staff and best care for ELFT's service users.

The Information Governance Managers (London and Bedfordshire & Luton) will, under the direction of the Senior Information Governance Manager – Systems, 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 Governance Managers will liaise with the Trust's Data Protection Officer when required.

The Information Rights Coordinator will support the local Access to Records leads, manage a caseload of complex requests and track the performance of the Information Governance Team through the collation of performance statistics from Access to Records leads across the Trust.

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 –**

  Individuals currently employed by the Trust should contact their local People & Culture Adviser if access to their HR file is required. Where an individual requires information that may be held by a line manager or other individuals, a written request must be submitted to the Access to Records team (elft.accesstorecords@nhs.net). Identification will be required unless an East London NHS Foundation Trust email address is used.

  Ex staff, contractors or volunteers should submit their requests directly to the Access to Records team. Identification will be required.

  All requests must be explicit in what is required, give details of who may hold the information, the time period required and the subject matter of the data required.

  Requests will be processed by asking the individuals who hold personal data relating to the requester to disclose that data directly to the Access to Records team. If this is not acceptable it may not be possible to respond to the request. Requesters should note that all staff contracts contain a confidentiality code of conduct and that any deliberate withholding of information may result in action being taken against that individual.

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.
- **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 1Paragraph 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 -** If a service user has transferred care then the records are transferred to the new provider on receipt of a written request to the access to records team. Consent is not required.

- In most other 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.

  Where a request is received by another health or social care organisation or a third party such as a solicitors, requesting specific information about a patient this should be directed to the most appropriate clinician or health professional involved or most recently involved in the patients care to respond to.

The advice of the Information Governance 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 21 calendar days.

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 Governance 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 Governance 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 Governance 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 Rights 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 an Information Governance 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 an Information Governance Manager. The Information Governance 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 Legal Affairs Department (elft.legalservices@nhs.net) 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 license, 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 Governance Manager supervising the request 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 Governance 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 for the records of living people and 21 calendar days under the Access to Health Records Act 1990 for the records of 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 Governance 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 Governance 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 Governance 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 stating 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.

The right of rectification only applies to factual information and not opinions made by professionals. 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.

Individuals also have the right to request erasure of information held about them, also known as the right to be forgotten. The right to erasure does not normally apply to health records, however requests should be reviewed and processed in line with The Data Protection Act 2018.

If an individual asks for rectification or the deletion or erasure of information the Trust holds about them, the request should be sent to the relevant manager, clinician or health care professional who should contact the Information Governance Manager to discuss the request which will be reviewed on a case by case basis so the Trust meets its obligations under section 46 and 47 of the Data Protection Act 2018. Discussion with the individual and the subsequent decision rests with the clinician and not with the Information Governance Manager.

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.

9.14 Requests for CCTV Footage

If a subject access request requires the review and/or disclosure of CCTV footage, the service (ward, department, etc.) from which CCTV footage is requested will be responsible for securing the footage in accordance with the Trust's CCTV Policy. The relevant service will also conduct any necessary redactions to protect the privacy of individuals not involved in the incident under investigation before disclosing the footage. The service may obtain guidance from an Information Governance Manager.

10. Monitoring

Access to Records Leads will provide statistics on volume and compliance status of subject access requests to the Senior Information Governance Manager - Systems, 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
Closed Circuit Television Policy

To be sent with disclosures to individuals

In accordance with Section 45 of The Data Protection Act 2018 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.

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.

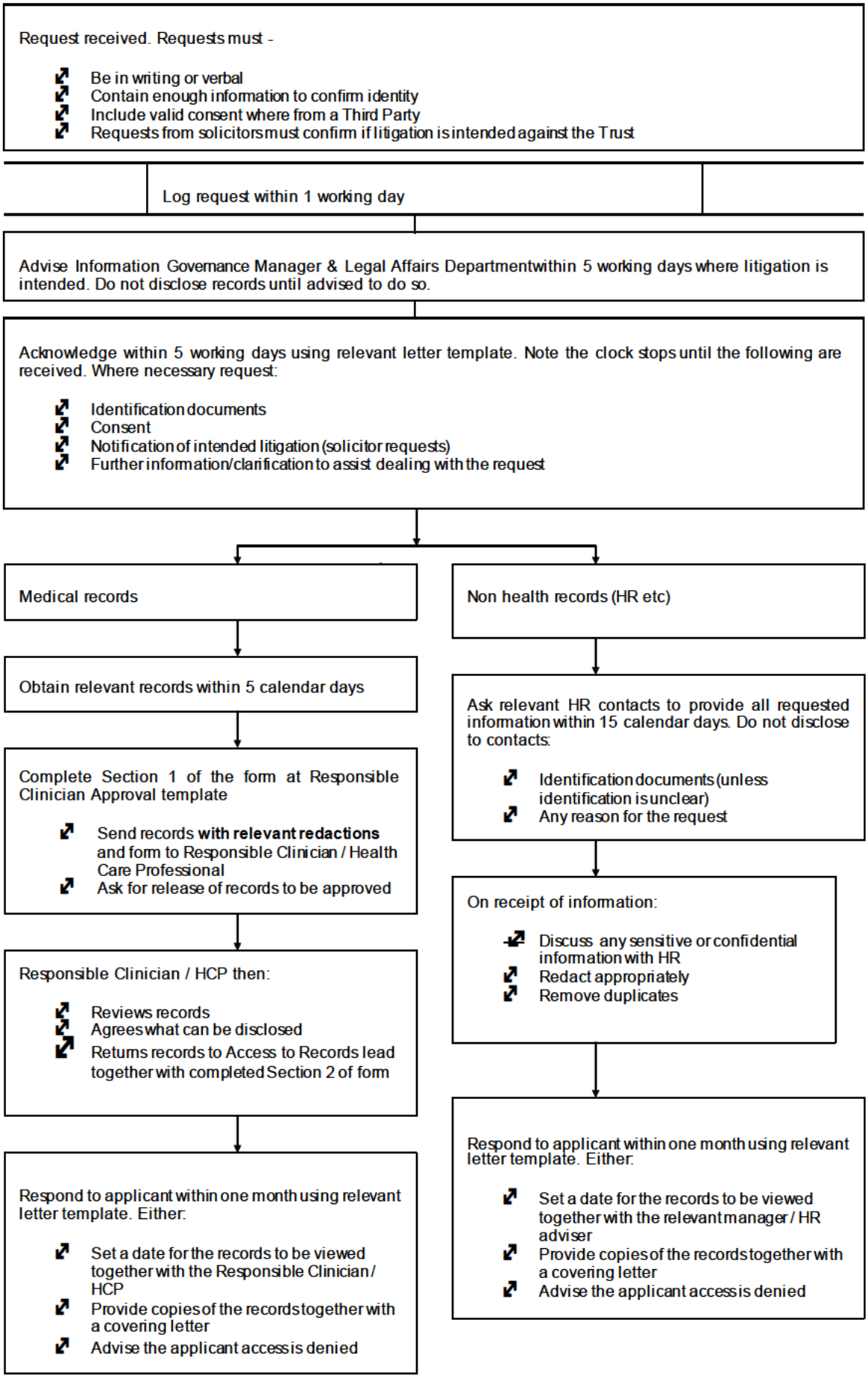
We do not use automated decision making to make any decisions about you.

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



East London
NHS Foundation Trust

Health Records Policy

Version number:	2.9
Consultation Groups	Digital Advisory Network Information Governance Steering Group
Approved by (Sponsor Group)	Information Governance Steering Group
Date approved	19 December 2025
Ratified by:	Quality Committee
Date ratified:	28 January 2026
Name of originator/author:	Head of Information Governance
Executive Director lead :	Senior Information Risk Owner
Implementation Date :	December 2025
Last Review Date	December 2025
Next Review date:	December 2028

Services	Applicable
Trust wide	X
Mental Health and LD	
Community Health Services	

Version Control

Version	Date	Author	Status	Comment
1.0	October 2011	Head of Information Governance	Final	Condenses previous versions of the policies and procedures below into one document: Clinical Records Management Procedures, Health Record Keeping Policy, Procedure for Health Record Archiving and Destruction
1.1	January 2012	Head of Information Governance	Final	Incorporates NHSLA Level 3 requirements
1.2	March 2012	Head of Information Governance	Final	Incorporates revised NHSLA Level 3 requirements published end January 2012
1.3	May 2012	Head of Information Governance	Final	Sets definitive timescales for entering information on to electronic record keeping systems
1.4	July 2012	Head of Information Governance Clinical Records Development Manager	Final	Revised to reflect access / tracer card practice in locations without a dedicated Records Manager
1.5	August 2012	Head of Information Governance	Final	Includes updated guidance on filing incident reports. Outlines clinical responsibility for ensuring new information about inpatients is seen and acted on
1.6	November 2012	Clinical Records Development Manager	Final	Strengthened guidelines to address queries related to errors identified in the entries made in clinical records. Clarified guidance on electronic health records.
1.7	January 2014	Head of Information Governance	Final	Revised guidance to transfer records from CAMHS to adult services
2.0	January 2016	Associate director of Assurance	Final	Revised as the primary health record is now electronic. Incorporates previous Clinical RiO policy

2.1	February 2016	Head of Information Governance	Final	Revised validations section following IGSG/IMTAC review
2.2	March 2017	Interim Head of Information Governance	Final	Addition of defining paragraph on responsibilities for the validation of collaborative entries to Validation Section 6
2.3	March 2017	Interim Head of Information Governance	Final	Added Goddard Enquiry hold on deletion of all records until further notice
2.4	October 2018	Information Rights Manager	Final	Revised to comply with GDPR
2.5	July 2019	Information Governance Manager	Final	Include appendix about Arts Therapies and Identification Criteria for Unknown Patients. DPO role made explicit
2.6	November 2021	Information Governance Manager	Final	Revised in line with Records Management Code of Practice, published October 2021
2.7	January 2022	Information Governance Manager	Final	Clarification regarding validation of electronic entries
2.8	March 2023	Data Protection Officer	Final	Section 5 outlines changed validation requirements. Document management section 14.1 strengthened
2.9	December 2025	Head of Information Governance	Final	Revised purpose, systems, addition of IAR, format and job titles following review, added file destruction process, revised Caldicott Guardian responsibilities and removed appendices examples.

Contents

Executive Summary

This policy provides a guide to the key elements of the records management process concerning health related records, outlining the legal framework and principles governing the Trust's records management process, outlines the roles and responsibilities for managers and staff in relation to record creation and management; as well as providing guidance on all aspects of managing health related records.

1. Introduction

High standards of record keeping underpin the delivery of high quality, evidence based healthcare. Records should be up to date, accurate and accessible when required. This policy provides a framework for achieving high quality safe record keeping based on the principle that records are electronic.

2. Purpose

A health records can be summarised as 'one which relates to the physical or mental health of an individual, made by or on behalf of a health professional in connection with the case of that individual". Thus with the exception of the anonymised information most if not all NHS information concerning patients whether held electronically or on paper will fall within the scope of the General Data Protection Regulation / Data Protection Act 2018.

This policy sets out the standards and processes required for maintaining high quality health record keeping standards for all service users.

The electronic record has replaced the paper record as the primary record for both community and mental health service.

3. Duties

All individuals

All individuals must ensure confidentiality, integrity, accuracy and appropriate availability of records. All individuals are personally responsible for the records they create or use and will not be allowed access to RiO or any other electronic clinical system until they have completed training at this Trust.

All NHS bodies and those carrying out functions on behalf of the NHS have a common law duty of confidentiality. Everyone accessing the health information of service users has a common law duty of confidentiality to both the service user and the Trust. Confidentiality extends even after the death of a service user.

Individuals should be aware that information recorded in a service user's record is legally binding. The record should therefore be non-judgmental and contain only information the individual would be willing to be accountable for in Court.

Any notes about a service user form part of the clinical record and should be uploaded to their clinical record e.g. during ward rounds, during CPA meetings, where Duty of Candour is invoked etc.

All teams should have an internal process for ensuring the relevant clinician / care worker is aware of all new documentation / correspondence relating to a service user.

All individuals should be familiar with their patient system crib sheets which guide the user through particular tasks.

Individuals should never share Smartcards. If information is accessed / added on behalf of another individual this should be made clear within the record. If an individual accesses the electronic record of a patient not under their direct care they will be prompted to state why they are accessing this information. This will be recorded and audited. Access without a legitimate reason may result in disciplinary action or dismissal and legal proceedings.

Line managers

All ward, team or service managers, supported by the Associate Director of Information Governance, are responsible for ensuring the principles set out in this policy are followed together with any local supporting procedures.

All line managers and supervisors must ensure that their staff, whether administrative or clinical, are adequately trained in the management of health records and apply the appropriate guidelines and crib sheet procedures.

Line managers will be responsible for authorising access to RiO and other systems requiring Smartcards through the Registration Authority (RA) who will issue smartcards on receipt of that authorisation.

4. Clinicians

Clinicians must ensure they adhere to the records management standards of their professional body in addition to the requirements of this policy.

5. Validation

Staff are no longer required to validate entries on RiO. This ensures consistency of standards with other clinical systems used by the Trust. In the event of any challenge or concern the Trust's Data Protection Officer will approve the production of a legitimate relationship report from the back end of RiO. The DPO should be approached for approval in the first instance and the approval subsequently included when the requester logs the request on Service Now.

6. Local Records Managers

Each directorate will have a local Records Manager under whose guidance designated staff will:

For paper records:

- Maintain safe and structured records management stores
- Ensure there is a process for the retrieval of case notes and update tracer cards.
- Organise the safe transportation of records from one location to another
- Deal with requests for access to health records within statutory time limits. In some services there is designated access to records leads. This is covered in detail in the Trust's Access to Records policy.
- Maintain an Information Asset Register for both digital and paper records systems used.

7. Duty Senior Nurse

Out of hours, the Duty Senior Nurse / Manager in charge is the only individual permitted to access a paper records store to retrieve case notes and update tracer cards. Out of hours, the Duty Senior Nurse / Manager in charge must enter inpatient events on to the relevant electronic clinical recording system within four hours of the occurrence of the event.

8. Data Controller

The Chief Executive is the Trust's Data Controller and has an overarching duty to make arrangements for the safety and integrity of the Trust's health records.

9. Data Protection Officer

The Associate Director of Information Governance is the Trust's registered Data Protection Officer and has responsibility for ensuring health records meet statutory requirements. 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.

10. Caldicott Guardian

The Chief Medical Officer is the Caldicott Guardian and has responsibility for matters relating to patient confidentiality. Clinical Directors and Medical Directors also provide local Caldicott Guardian advice. Please note that Medical Directors are designated as Deputy Caldicott Guardians. Clinical Directors are local Caldicott Guardian leads and the first point of contact, who can then escalate matters up as and when necessary.

11. Service Directors as Information Asset Owners (IAOs)

Service Directors are Information Asset Owners for the health records within their service and must ensure the quality, integrity and security of records in their directorates.

12. Information Asset Administrators (IAAs)

IAAs support the IAOs by managing information assets on a day-to-day basis.

13. General principles

13.1 Health Records Use

Health records must be reliable, accurate and timely to support:

- Continuity of care
- Multi-disciplinary working
- Defence in cases of litigation or complaints
- Evidence based clinical practice
- Administrative and managerial decision making

- Legal requirements including requests for access to records
- Clinical audit and effectiveness
- Statutory and contractual reporting requirements

13.2 Health Records Standards

Health records must:

- Be factual, consistent and be written according to Trust policy and accepted professional standards
- Contain as a minimum the service user's name, date of birth and NHS number. Where the NHS number is not known it should be verified via SCR / PDS. To ensure continuing accuracy of records the service user's full name, address and key contact details (including GP) should be verified at each contact and differing records synchronised.
- Completed as soon as possible after the event. Services should check local CQUINS / KPIs adhering to any shorter timescales where required. In particular, Trust timescales are:
    - Referrals within 24 hours of receipt
    - Outpatient / community entries within 24 hours of event
    - Inpatient entries within four hours of occurrence e.g. admission, discharge, transfer, AWOL, leave etc.
    - Physical health forms within 24 hours

13.3 Confidentiality

Information in a service user's record must be held in complete confidence and only viewed by those directly involved in the provision of care or who are otherwise authorised by the Trust to do so. Unauthorised disclosure and misuse of information constitute a breach of confidentiality and breach of this policy which may lead to disciplinary action, dismissal and legal action.

Information contained in a service user's record should only be accessed on a 'need to know' basis. Individuals are specifically not permitted to access the records of people they know via a work, social or family connection or in response to media interest.

The Trust will undertake regular and targeted audits to identify instances where confidentiality is breached and take action against any individual found to have inappropriately accessed a record.

Where copies of records are taken outside the Trust (e.g. to visit a service user) they should not be opened / looked at whilst on public transport, left in a visible location (e.g. the back seat of a car) & stored securely whilst not in use.

13.4 Format

Health records will be in a number of formats including emails, x-rays, photographs and audio visual recordings. The same principles apply to all formats. Where paper copies are received note that the primary health record in the Trust is electronic. Paper copies that are not duplicates

should therefore routinely be scanned and held electronically then confidentially destroyed, unless the format or legislation prevents this.

13.5 Records Retention

Records in any media (electronic or paper) must be retained according to the Trust's Record retention and disposal schedule:
https://transform.england.nhs.uk/documents/165/NHSE_Records_Management_CoP_2023_V5.pdf

This is based on the NHS Records Management Code of Practice.

Inactive records that have reached the minimum retention period should be reviewed annually to identify the need for extended retention or destruction. After review the list should be updated to show those identified for destruction and those identified for extended retention. Paper records identified for destruction should be destroyed by the relevant Trust approved company and a destruction certificate must be obtained from the company.

Audit/check list – shredding/destruction companies

1 – Are there secure receptacles or bins where members of staff can place confidential documents to be shredded/destroyed?

2 – How is security of these receptacles or bins ensured so that documents cannot be accessed?

3 – How is the material in the bins collected?

4 – Where are they shredded / destroyed?

5 – Is there a risk that paper may escape from the receptacles or bins between these being collected and the actual shredding/destruction operation?

6 – What type of shredding/destruction is used? Is it enough to ensure that information cannot be put back together?

7 – What documents does the company have to show compliance with security best practices?

8 – Are members of staff duly checked before they start working for the company?

9 – What is done with the shredded/destroyed material?

File destruction process

All files identified for destruction must be reviewed and approval granted prior to destruction taking place.

The following process should be followed:

- Fill in a blank destruction template (a template can be provided on request) with list of all files to be destroyed, leaving the **Destruction Certificate Obtained** column blank until obtained

- Send your Service Director a spreadsheet of all records for destruction, asking for DMT approval for destruction. Copy in the Service Director's EA

- When approved at DMT the Service Director's EA should send you the DMT minutes approving destruction

- Forward the minutes and spreadsheet to elft.records.management@nhs.net , asking for approval for destruction

- The Records & IG Coordinator then checks the spreadsheet and DMT approval, prepares a summary and forwards to the Data Protection Officer chris.kitchener@nhs.net for approval.

- The DPO after approving returns the form to the Records & IG Coordinator who advises the requester that destruction can take place.

- Once you have received notification you can send the list for destruction to the storage provider (if the records are being destroyed in-house you can securely destroy them at this stage)

- On receipt of the Destruction Certificate complete the **Destruction Certificate Obtained** column on the spreadsheet and send a copy to the Information Rights Coordinator (if the records are securely destroyed in house then complete this column with the date of destruction)

Confidential waste

All confidential waste must be securely destroyed. Waste material should be sent to the designated confidential destruction site or shredded. All waste paper baskets must be properly labelled to read 'No Confidential Waste'. In the absence of a shredder, confidential waste must be kept in a 'Confidential Bag' which should be kept in secure location and send to the confidential destruction site. Many services in the Trust will have locked bins from companies authorised to shred confidential information. The bins will be collected by these companies which will securely shred/destroy the bins contents.

Information sharing

Generally, the following principles apply:

- The Trust does not need to seek consent to share information for health purposes with health and social care agencies. Where RiO is used, the Additional Personal Information form should be completed with contact preferences and preferences for sharing information where there is a choice (family, school, voluntary agencies etc.). The form should be updated at regular intervals. Service users should also be given a copy of the "Your records and you" leaflet that explains how their information is processed, and advised that in some circumstances it may not be possible to care for them if their information is not shared. "Your records and you" posters with these details should also be visible at Trust sites.

- Service user information may not be passed on to others without the service user's consent except for healthcare purposes, or when there is a legal requirement, including where there is a risk to the safety of the individual or others.

- Explicit consent is required if identifiable service user information is used in any publication.
- Where identifiable information is disclosed a record of the disclosure and the reasons for doing so should be recorded in the notes. If a decision not to disclose is made, this should similarly be recorded.
- In circumstances where information is shared without the consent of the service user the responsible clinician should make this decision. The Head of Information Governance, Associate Director of Information Governance or Caldicott Guardian can also advise.
- When a child or vulnerable adult is believed to be at risk then relevant information should be shared without delay. This requirement will always override all other confidentiality considerations. Conversely, if it is believed disclosure may compromise an individual's safety, or that it is not in the public interest to disclose, then the information should not be shared. Reasons must always be documented in the record.

13.6 Mental Health Act Documentation

There are specific requirements regarding the receipt and scrutiny of documents under the Mental Health Act 1983:

- Receipt of section papers - only Mental Health Law staff and clinical staff at Band 5 or above (or equivalent) who have at least one year's experience at that level and have attended the relevant Trust training are authorised to formally receive section papers and scrutinise them
- Leave periods - the granting of leave and the conditions attached to it should be recorded in the notes and on the Trust's section 17 form. Copies of the form should be given to the service user, any appropriate relatives or friends and any professionals in the community who need to know
- The service user's legal status in respect of their detention, leave and consent to treatment should be immediately apparent from the medical notes

13.7 Incident Forms

- Where an incident relates to a service user the incident form must be added to the health record or as a minimum the InPhase reference logged in the health record.
- Where incidents relate to more than one service user they may be added / logged in each health record provided person identifiable information relating to the other service user(s) is redacted. Otherwise use the InPhase reference number filed in each service user's progress notes together with a summary of the incident.
- Any Duty of Candour correspondence or conversation should routinely be uploaded to the clinical system

13.8 Complaints Records

Complaints records must be filed separately from the service user's health record unless there is a need to record the complaint (for example where it is directly relevant to the service user's health and failure to recognise this when caring for the service user could have a detrimental effect on the

health and well-being of that individual).

13.9 Child Health Records

Transfer of records from CAMHS to adult mental health services

For service users admitted to an adolescent inpatient service within the Trust or elsewhere (e.g. the private sector), who are approaching 18 years of age and are known to community CAMHS, it will usually be the responsibility of community CAMHS to initiate the transfer process. All CAMHS records are now electronic. Detailed information is available in the Transition policy for CAMHS.

13.10 Research and Teaching

The Trust has teaching hospital status for students in a number of disciplines. All students are bound by the principles of confidentiality. The following standards apply:

- Service user records may be used for teaching purposes and clinical supervision within the clinical area
- If records are to be used for teaching purposes outside of the clinical area then service user details must be made completely anonymous.
- The principles of access and confidentiality remain the same and the right of the patient to refuse access to their records should be respected and documented in their notes
- The Local Research Ethics Committee must approve the use of service user records for research
- Any use of service users' records for research purposes must comply with the Department of Health's Research Governance Framework

13.11 Service Closure or Transfer

- If a service or site is closed, split or amalgamated with or from another service or Trust, the service manager should advise the Associate Director of Information Governance who will coordinate work with the electronic clinical records team, access to records leads / local Records managers and Estates to ensure appropriate transfer, access, storage and retention of the relevant records.
- A Data Transfer Agreement may be required to ensure data transfers securely to the new organisation. The Associate Director of Information Governance will advise,

- In some circumstances, an information sharing agreement or SLA may be required. In such cases the Associate Director of Information Governance should be consulted.

13.12 Criteria for Safer Temporary Identification of Unknown Patients – see Appendix 2.

14. Electronic Records

The Trust's primary record keeping systems are electronic. Duplicate paper records systems must not therefore be used.

14.1 Principles

The following principles apply:

- Only Trust approved scanners will be used for scanning documents

- All information about a service user must be uploaded to the clinical system. It must not be

retained on separate drives or in email systems except when in draft format. If for any reason it is not feasible to upload documentation to the clinical system it must be properly named on a secure drive, accessible only to those who have a legitimate relationship with the patient. A note should be added to the clinical record advising the location.

- All emails, Teams chat or similar data that is about a service user must be uploaded to the clinical system as this forms part of their record. In the event of a subject access request or other request, it is an offence to knowingly destroy data to avoid disclosure.

- All information about a service user received in paper format will be scanned, subsequently uploaded to the clinical system and the original securely destroyed

- All services will set up team based shared folders on the K drive, Microsoft One Drive or on Microsoft Teams where data is relevant to groups of service users (e.g. MDT meetings). Folders and files / documents will be locked down to those individuals with a specific need to access the information. Standardised naming conventions will be used. Folders will be used only for drafting, processing and auditing information prior to uploading to the clinical system and will not become a secondary clinical system.

- When the clinical system is unavailable paper records should be scanned and temporarily held in the team folder on the K or other secure drive, Microsoft One Drive or on Microsoft Teams. Electronic records should similarly be temporarily held on the K drive, Microsoft One Drive or on Microsoft Teams rather than individual mailboxes or personal drives. When the clinical system becomes available, priority should be given to uploading documents.

- The electronic clinical system record is the primary record. No other current records will be kept other than a small temporary folder used by some services. All original paper and electronic information will therefore be deleted once the scanned copy on the electronic clinical system has been verified as attaining the same standard as the originating copy. This is to prevent duplication of systems and information and the potential for information to be missed, incorrectly added to or otherwise inappropriately processed.

- Teams will set up a systematic process for alerting all members of the treating team to newly received and uploaded information including incoming electronic and paper documents

- Where teams or individuals outside the treating team add information to a clinical system they will routinely alert the treating team to raise awareness of any immediate or significant issues

- Clinicians will routinely check the clinical system for newly received information prior to an appointment / intervention with a service user

- Correspondence must not be filed in the clinical system unsigned. Typed correspondence must always contain an electronic signature. Where the clinician prefers to delegate authority to an administrator for adding the signature, this should be confirmed by email and the email also retained in the clinical system

- Electronic records are subject to the same retention and deletion periods as paper records (i.e. the retention period does not alter simply because the format is electronic rather than paper)

- Electronic records are subject to regular audit including record keeping standards and

legitimate relationship access to records. This may include targeted audits

- Records pre-dating clinical system implementation will be retained in paper format and will not currently be uploaded to the clinical system except in instances where the Responsible Clinician believes there is distinct value in doing so

- Where records are recalled from archiving for subject access request purposes these may be attached to the clinical system and the original destroyed in accordance with the guidelines set out for deletion of records

- Requests for access to records will be centrally managed by the Access to Records leads.
    - Where solicitors require access to the service user's electronic record this should be redacted for third party information. This should comply with the one month timescales referred to within the GDPR.

- Services should always access Reporting Services for contemporaneous clinical information when RiO is unavailable

- The electronic record is the primary record. No other current records will be kept other than the temporary folder outlined below. Original documents will be deleted once the scanned copy has been verified as attaining the same standard as the original document. This is to prevent duplication of systems and information and the potential for information to be missed, incorrectly added to or otherwise inappropriately processed

14.2 Temporary Paper Folder Actions

Document type	Retain in paper format once episode of care complete?	Action on completion of episode of care
'This is me' first person care plan	No	Stamp and upload to clinical system
Prescription / depot charts	Yes	

Observation forms	Yes	Also upload to clinical system
Outcome measures & other questionnaires	No	Upload to clinical system
Written copy of CPA form with signatures	Yes, temporarily until next review	Upload to clinical system
Sticky labels with patient details (for ordering investigations)	No	
Registration form printout	Yes	
Current care plan	No	Upload to clinical system
Current risk assessment	No	Upload to clinical system
Patient property receipts	No	Upload to clinical system
MHA documents (excluding police documentation which should be uploaded to RiO	Yes	
Alerts with an immediate impact on patient care	Yes	Also upload to clinical system
Do not resuscitate forms	Yes	Also upload to clinical system
Results / investigations / bloods	No	Upload to clinical system
Audio visual recordings	No	Transcribe and upload to clinical system
Artwork / non standard scan size documents	Check if patient wants	Take photo and upload to clinical system
Process notes	No	Destroy. Do not scan / upload unless Therapist advises should be kept
Seclusion documents	No	Scan and upload to clinical system
ECGs	Yes. Store in the resealable wallets provided specifically for this purpose	
Growth charts	No	Scan and upload to clinical system. Download back to hardcopy if patient presents again.

- For services using RiO the processes on the RiO user guide pages on the intranet must be

followed at all times

15. Paper Records

15.1 Principles

Although the primary record is electronic, the Trust still holds historic paper records. The following principles apply:

Paper records must be stored in an area where service users, members of the public and unauthorised staff are unable to gain access to them

- Requests for records held in an external repository (e.g. Iron Mountain) must be made via the Access to Records Leads / local Records Managers.
- Trust individuals are only allowed access to records stores during normal working hours with the permission of the relevant local Records Manager / Access to Records Leads and on production of valid identification. Out of Hours, the only access is via the Duty Senior Nurse / Manager in charge.
- Where records are stored in areas that do not have a 24/7 staff presence then they must be secured in an area that is securely locked when the premises are unstaffed.
- Missing or part missing health records must be reported via the Trust's incident reporting process and as a result will be investigated.

15.2 Tracking Procedure

- Tracer cards should be used to document the movement of paper records unless there is an electronic tracking system.
- Only medical records staff or the Duty Senior Nurse / Manager in charge are authorised to retrieve records and update tracer cards. In smaller centres where there are no dedicated medical records staff, the service manager will assign responsibility to relevant staff members to ensure compliance with the record tracking procedure.

15.3 Filing Area Standards

The following standards apply at all times:

- Place files on the shelf in the correct numerical or alphabetical order with the spine underneath and the case note number facing outwards
- Leave the tracer card in situ at all times. Complete movements and mark RETURNED when case notes are filed back. Do not add any other documentation
- The file storage area should be regularly audited utilising the above standards
- Separate records over three inches thick into separate volumes
- Do not eat, drink or smoke near records

15.4 Paper Records in Transit

If paper records need to be transported from one clinical area to another it is the personal responsibility of the individual transporting the records to ensure their safety and security whilst in transit and ensure they cannot be accessed by an unauthorised individual at any time during transit. The following standards apply:

- Records should be handled carefully - never thrown, transported with materials that could cause risk to the records (e.g. chemicals) or exposed to weather, excessive light or risk of theft
- Records must not be transferred internally using the internal mail service as this service does not meet Trust confidentiality standards. They should be transferred using the internal courier service (man with a van / man with a car service)
- An approved courier must be used when transferring health records externally (normally TNT, Loomis or Royal Mail Special Delivery) using 'track and trace' including the provision of a signature on delivery
- Couriers transporting records for archiving / off site storage purposes must meet information governance standards
- Large quantities of health records should be boxed in suitable crates or boxes that give adequate protection. Otherwise, tamper proof envelopes or padded envelopes should be used
- All packaging should be clearly marked with the recipient's name and address. The Trust's PO Box Return to Sender address must be included on the reverse of the envelope
- All packages should be marked 'Private and Confidential. To be opened by the addressee only'
- Records in transit must be stored securely e.g. in the locked boot of a car rather than the back seat
- Where practical, records should not be left unattended in a vehicle
- If it is absolutely necessary to retain records overnight in no circumstances should they be left in a vehicle. They must be kept under the same conditions of security as on Trust premises i.e. in a locked cupboard within a locked building
- Records should not be looked at in a public place

15.5 Paper Records Review

Inactive records that have reached the minimum retention period should be reviewed annually, based on the NHS England Records Management Code of Practice, to identify the need for extended retention or destruction.

- A sticky year label should be affixed in the 'year label' box on the folder front cover at the service user's first contact with the service
- The sticker should be updated if the service user has subsequent contacts. The last contact is the date used to determine retention or destruction

- Deceased patients' folders should be marked 'Deceased' with marker pen on the front cover of the folder

- An electronic clinical system search should be undertaken annually to identify inactive and deceased patients' records. The search should be verified with the paper records before any decision regarding destruction is taken. In the same way all information about a service user should be drawn together to assist the review

- Records that have been identified as potentially reaching the end of their retention period should be listed by the local Records Manager to include:

    - Name
    - Date of birth
    - NHS number
    - Address
    - Last contact date
    - Record status – inactive or deceased

- After review the list should be updated to show those identified for destruction and those identified for extended retention (e.g. research or legal value, historical retention at the Public Records Office, identified familial illness). This should be approved by a senior clinician and documented in the record and a 'Do Not Destroy' sticker attached to the record

- The services' local clinical governance committee will agree destruction / extended retention. Prior to destruction, this should be agreed by the Associate Director of Information Governance, who will then report to the Information Governance Steering Group (IGSG)

- On notification of final approval from Associate Director of Information Governance, record destruction should be undertaken in a secure manner. Approved contractors should be used to destroy records under secure conditions. A certificate of destruction must be obtained and permanently kept with the locality records manager