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.

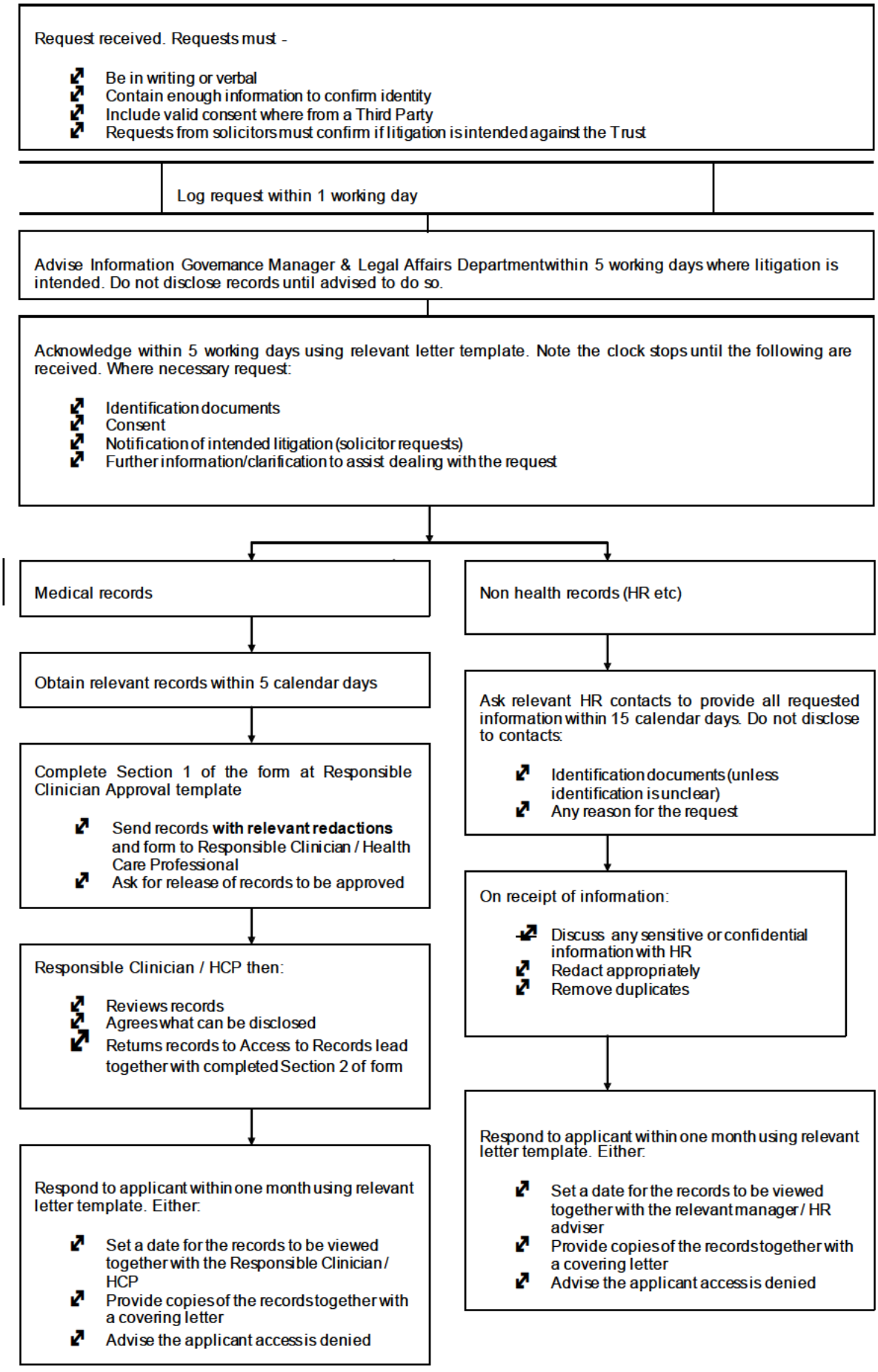
We do not use automated decision making to make any decisions about you.

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



Data Protection and Confidentiality Policy

Version number :	1.3
Consultation Groups	Quality Committee
Approved by (Sponsor Group)	Information Governance Steering Group
Date approved	11th February 2025
Ratified by:	Quality Committee
Date ratified:	26th March 2025
Name of originator/author:	Data Protection Officer
Executive Director lead :	Chief Quality Officer
Implementation Date :	April 2025
Last Review Date	March 2025
Next Review date:	March 2028

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

Version Control Summary

Version	Date	Author	Status	Comment
1.0	03.12.18	Information Rights Manager	Final	New policy providing guidance on data protection and confidentiality.
1.1	18.07.2019	DPO	Final	Updated to include committee structure, Information Asset Owner responsibilities, DPO requirement
1.2	03/2022	DPO	Final	Updated to include changes to SIRO, Executive oversight & operational responsibilities
1.3	01/2025	DPO	Final	Routine review. Fax as a method of communication removed. GDPR conditions for sharing information added. Job roles updated. Information governance content extracted from Information Governance & IMT Policy to become a standalone policy

Contents

Executive Summary

This policy provides a guide to the key elements of the legal framework governing information handling, outlines the responsibilities for managers and staff in relation to data protection and confidentiality and provides guidance on all aspects of information handling.

1.0 Introduction and purpose

1.1 Introduction

The Data Protection Act (2018) and the UK General Data Protection Regulation set the legal framework by which the Trust can process personal information. They apply to information that might identify any living person. The common law duty of confidentiality governs information given in confidence to a health professional (about a person alive or deceased) with the expectation it will be kept confidential. The Human Rights Act (1998) Article 8 provides a person with the right to respect for private and family life. The key rights provided by this legal Framework are also set out in the NHS Constitution (section 3A). It applies to all areas of the Trust and all staff who handle information.

Data protection and confidentiality is a component of information governance and as such this policy and associated procedures form part of the Trust's overall Information Governance Framework.

1.2 Purpose

The objectives of this policy are:

- To outline the ways in which patient and staff data is handled effectively and securely
- To promote best practice and innovative use of personal information, especially to inform care and research
- To ensure responsibilities and obligations are understood

2.0 Duties and responsibilities

2.1 Management responsibilities

The **Chief Executive** is the Trust's **Accountable Officer** and responsible for overall leadership and management of the Trust with the ultimate responsibility for ensuring compliance with the Data Protection Act (2018), the UK General Data Protection Regulation, Human Rights Act (1998) and the Common law Duty of Confidentiality. The Chief Executive delegates aspects of her responsibility to relevant executive directors according to their organisation portfolios.

The **Chief Quality Officer** is the **Senior Information Risk Officer (SIRO).**

The Associate Director of Information Governance is the **Data Protection Officer** and Responsible for managing data protection issues throughout the Trust. 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 Chief Quality Officer has executive responsibility for information governance including chairing the **Information Governance Steering Group,** where data protection issues are discussed and escalated to relevant groups and committees when necessary.

Day to day responsibility for data protection and confidentiality management is the responsibility of **Senior Information Governance Managers** and the **Information Governance Managers.**

The **Chief Medical Officer** is the **Caldicott Guardian** with specific responsibility for the confidentiality agenda and the collection, use and sharing of patient information.

The Caldicott Guardian is supported by the Deputy Medical Directors and Clinical Directors who fulfill the role of Deputy Caldicott Guardians.

Service Directors / Associate Directors are Information Asset Owners, supported by **Team Managers** who are Information Asset Administrators.

All **Managers** are responsible for the local implementation of this policy in their areas of responsibility.

2.2 Individual responsibilities

Everyone working for the NHS has a legal duty to keep information about service users and other individuals such as staff or volunteers confidential. Staff are required to adhere to confidentiality agreements, e.g., common-law duty of confidentiality, contract of employment, NHS Confidentiality Code of Practice.

The terms and conditions within Trust employment contracts include specific conditions relating to confidentiality which must be adhered to.

All members of staff are responsible for ensuring they keep up to date with Information Governance/Data Security training in accordance with the Trust Statutory and Mandatory training needs analysis.

The need for data security training also applies to agency staff, contractors and volunteers working at the Trust who may have access to personal information. Most agencies working with the NHS provide their staff with this training. Where this is not the case, local arrangements should be made to ensure the employee is adequately trained before working at the Trust.

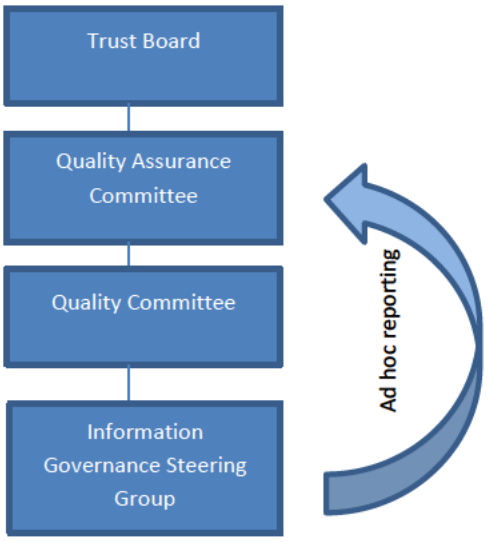
All users must sign a confidentiality agreement, either as part of their contract or as a separate
confidentiality agreement. Furthermore, individuals with privileged access to systems are required to sign an enhanced agreement to ensure they take their responsibilities seriously.

3.0 Reporting structures

The Information Governance Steering Group oversees the information governance agenda and
is responsible for holding the information governance function to account.

The Information Governance Steering Group is a subcommittee of Quality Committee. Quality Committee receives quarterly update reports on information governance matters plus any exception reporting. It ratifies policies approved at Information Governance Steering Group.

The Quality Assurance Committee is a Board subcommittee. Quality Committee reports to the Quality Assurance Committee. The quarterly reports tabled at Quality Committee are summarised at Quality Assurance Committee. Ad hoc information governance reports including the annual SIRO report are regularly tabled at Quality Assurance Committee.



4.0 Principles

To appropriately balance openness and confidentiality, the Trust places importance on the confidentiality and security of data to safeguard both personal information about patients and staff and commercially sensitive information. It also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

Accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision- making processes.

There are 4 key interlinked strands to data protection policy:

- **Openness:**
  - Non-confidential information about the Trust and its services is available to the public through a variety of media, in line with the Trust's code of openness
  - Policies are established and maintained to ensure compliance with the Freedom of Information Act, data protection and other associated legislation
  - Service users must in most circumstances have ready access to information relating to their own health care, their options for treatment and their rights as patients

- **Legal compliance:**
  - All identifiable personal information relating to patients is confidential unless there is a legal reason to override confidentiality
  - All identifiable personal information relating to staff is confidential except where national policy on accountability and openness requires otherwise

- **Information security**
  - Policies are established and maintained to ensure information assets are secure. This is set out in the Trust's IMT Security policy

- **Quality assurance**
  - Policies are established and maintained to ensure information quality assurance and records management. This is set out in the Data Quality policy

- Pseudonymisation will be used where de-identified data is required (pseudonymisation is a data management and de-identification procedure by which personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. A single pseudonym for each replaced field or collection of replaced fields

makes the data record less identifiable while remaining suitable for data analysis and data processing). Advice should be sought from the Informatics team where pseudonymisation is necessary.

5.0 Data Protection Act 2018 and UK GDPR

The Data Protection Act (2018) (DPA) and the UK General Data Protection Regulation (GDPR)
set out the legal requirements and duties placed on data controllers (i.e. the Trust), and data processors (anyone the Trust uses to process data on our behalf) and explains the 'information
rights' held by data subjects (individuals we hold information about).

As a Data Controller, the Trust is required to register annually with the Information Commissioner. The Trust's unique registration number is **Z5601596.**

The Data Protection Act (2018) defines six Data Protection Principles which all processors of personal information must abide by:

1. Processing shall be lawful, fair and transparent
2. The purpose of processing shall be specified, explicit and legitimate
3. Personal data processed shall be adequate, relevant and not excessive
4. Personal data shall be accurate and kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary
6. Personal data shall be processed in a secure manner

The Data Protection Act (2018) does not apply to deceased persons. The Access to Health Records Act 1990 governs the access to health records of deceased patients. The NHS has issued guidance which states that, where possible, the same level of confidentiality should be provided to the records and information relating to a deceased person as one who is alive. The issues arising from the processing and provision of access to deceased persons records can be complex and where these arise advice should be sought from the Information Governance Team: elft.information.governance@nhs.net

Under GDPR each controller of personal information must decide under what basis it is processing personal information. If there is no relevant basis, then the processing is likely to be
unlawful.

- Under Article 6, the Trust's basis for processing personal information is usually:
- Article 6(1)(e) the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- As the Trust processes special category information – which includes health data then it must have a second basis (under Article 9), which is usually:
- Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards

The UK GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing

- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

6.0 NHS Caldicott Report

The 1997 Caldicott Report (updated in 2013 and 2016) focusses on the protection and processing of patient identifiable information within the NHS. The reports provide the NHS with eight principles:

- Justify the purpose for collecting or holding patient-identifiable information
- Use confidential patient-identifiable information only when necessary
- Use the minimum necessary information
- Access to confidential information should be on a strict need to know basis
- Everyone with access to confidential information should be aware of their responsibilities
- Understand and comply with the law
- The duty to share information for individual care is as important as the duty to protect patient confidentiality
- Inform patients about how their confidential information is used

The Caldicott Guardian advises the Trust Board on matters of patient confidentiality and promotes the safe and secure handling of patient data. The Caldicott Guardian will consider and approve, as appropriate, applications for the disclosure or processing of patient data which fall outside routine procedures, where there are ethical considerations.

7.0 Data processing

Data processing is the obtaining, recording, using, storing, disclosure and disposal of data. The lawful and safe processing of data is important to successful business operations and to maintain confidence between the Trust and its patients, staff and others. The DPA requires that processing of any personal information must be both fair and lawful. Processing must meet fair processing criteria and satisfy one or more 'conditions for processing' set out in the DPA. 5.3.3. We must demonstrate that we:

- are open and honest about our identity
- tell people how we intend to use any personal data we collect about them
- usually handle their personal data only in ways they would reasonably expect
- do not use their information in ways that unjustifiably have a negative effect on them
- help people to understand their rights

To meet this requirement the Trust publishes a fair processing notice to inform individuals about the way we handle and use their personal data. This is published on the Trust's public website.

Routine data processing for the purposes of patient care will normally satisfy one of the processing conditions in the DPA. When sharing takes place for non-care reasons (often referred to as secondary purposes) it can be more challenging to satisfy a condition for processing and demonstrate it is lawful processing. This is particularly the case when sharing sensitive information or when sharing personal information without consent.

A Data Protection Impact Assessment (DPIA) should be completed on all projects, proposals or business changes that involve personal information. This could be patient information or staff information.

8.0 Access to IT systems

IT systems holding personal data must have adequate controls in place to prevent loss, unlawful processing or inappropriate access.

The Information Governance & IMT Security Policy provides detailed guidance on the security of
Trust IT systems including minimum standards of access controls.

Individuals should not attempt to access or use electronic record systems they have not been trained to use or are not authorised to access. Existing system users should not allow others to access systems using their login credentials. Action may be taken against individuals who share passwords and Smartcards.

9.0 Accessing records

The Trust holds individual service user records in a variety of formats. In addition, it holds personal records for present and former members of staff and others it does business with. While it is clearly necessary for many members of staff to routinely access and use these records to carry out their work, it is important staff know that any access to records which is not legitimate or authorised is not allowed and may be unlawful. Appropriate action will be taken against any individual contravening this standard.

Digital systems may allow a user to access any individual record held in that system. Users should only access records where they have authorisation to access them for specific purposes
or in the case of health records where they have a 'legitimate relationship' with the service user.

Staff have no right to access personal information held in records about their relatives, colleagues or friends.

Staff should not access their own data held in any Trust systems without specific authorisation. Instead they should make a subject access request.

Procedures for obtaining access to or copies of health records about individuals that are held by the Trust are explained in the Access to Health Records Policy.

The Trust carries out audits of access to personal data and any individual who is found to be in breach of this guidance by inappropriately accessing their own or other peoples' records / data may face action.

10.0 Communicating personal information

To provide effective care there is a need to transfer information between organisations and individuals. To comply with the DPA principles it is important that any transfer or communication of personal data is carried out securely and safely and the risk of accidental disclosure or loss in transit is minimised.

Any electronic data containing identifiable information transferred outside the Trust for processing must be securely encrypted during transit. Any transfer outside the European Economic Area must only be carried out if appropriate security controls are in place.

A guide on the transfer or communication of personal data by post, hand, e-mail and other methods of electronic communication is available on the intranet. Fax should not be used. Written communications containing personal information must be in a sealed envelope and addressed by name to a designated person. Judgement should be used on the appropriateness of using tracked / recorded delivery. Post should be marked "Personal and Confidential – to be opened by the recipient only".

11.0 Disclosure and sharing of personal information for care purposes.

To provide safe and effective care, personal information about service users will be shared not only with the clinical team providing care, but also the direct care team which may include
pharmacy staff, social care staff, specialist care teams and administrative staff supporting the care process.

In accordance with the DPA 2018, GDPR and Caldicott principles information shared for care purposes should be relevant, necessary and proportionate. In applying this principle, care should be exercised to avoid compromising care. Confidentiality should not become a barrier to safe and effective care.

Caldicott Principle 7 (Duty to share) emphasizes the need to share information in certain circumstances where the need to share information clearly outweighs the normal duty of confidentiality owed, for example, when there is a threat to the safety of others and the sharing of personal information about individuals (e.g. vulnerable adults or children) with the police or other agencies may prevent a threat materialising.

GDPR Article 9(2)(h) permits the sharing of information without consent for the purposes of preventative or occupational medicine, or the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment

Disclosing information to relatives and carers

Staff will deal with numerous inquiries from relatives and friends of patients seeking information about progress and treatment. Many inquiries will be made over the telephone by people who are not registered as the patient's next of kin or carer and in these circumstances, it is sometimes difficult to decide if any information should be passed on. While in most circumstances a patient will not object to updates about their condition being given in response to an inquiry, circumstances do arise when this will not be appropriate. It is therefore good practice to establish and record if the patient wishes to place any restrictions on the information provided about them to others. This will make it easier to respond appropriately to any telephone inquiries received. Where restrictions are placed on information to be provided about patients it is important all staff likely to handle inquiries are made aware of the details to avoid a breach of confidentiality.

On receipt of an inquiry from a person not known to staff, where practical, the consent of the patient to disclose information should be sought. Where this is not possible a disclosure decision has to be made based on the information provided by the caller justifying their 'need to know'. Sensitive and detailed information should normally only be disclosed or discussed with nominated or recognised next of kin, close relatives or carers.

If suspicious about the motives of a person making an inquiry about a patient do not pass on any details but take a contact number and discuss with a senior colleague and seek advice before making contact again.

12.0 Sharing personal information for non-direct care purposes

Non-care purposes (also known as secondary purposes) will include research, service development and improvement, billing and invoicing, service management and contracting. Where possible these activities should be carried out using anonymized or de-identified data. This removes the need to consider consent issues.

In certain circumstances the law requires that confidential information should be disclosed

without consent. Examples of this include a direction within a court order to disclose confidential information or the requirement to notify Public Health officials when a patient is suspected of suffering from a notifiable disease.

Where a legal obligation to disclose does not exist there are some limited circumstances where the sharing of personal information without consent may be justified in the 'Public Interest'. Disclosures made without consent to support the detection, investigation and punishment of serious crime and to prevent abuse or serious harm to others are examples of such circumstances. Such disclosures are considered on a case by case basis and can be complex. The public good that would be met by sharing the information has to be weighed against the obligation of confidentiality owed to an individual and the public good in maintaining trust in a confidential service.

Disclosing information to the police

Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018 provides a lawful basis for the Trust to disclose personal data about a person in the absence of their consent where this will support certain aspects of law enforcement and in particular:

- the detection, punishment and prevention of crime
- the identification, apprehension and prosecution of offenders

Unless there is a high harm threshold for the request (alleged homicide, threat to national security, serious sexual abuse) the police should provide the consent of the data subject prior to the Trust disclosing any information. Furthermore, all requests should be in writing. Each police force will have a specially designed template. Many inquiries made by the police will be handled first by the Information Governance Team or locality access to records leads. Occasionally inquiries will be made direct to wards and departments. The Information Governance team can provide advice if required.

Occasionally urgent requests will be made asking for specific information to be provided in a short period of time. Often this is due to strict timelines imposed on the police to make decisions to charge suspects or to support urgent lines of investigation. In these circumstances decisions may have to be made quickly but staff should not be pressured into disclosing information when they feel it is not in the patient's best interest. Note that in most circumstances the police should provide consent.

Whilst the law permits disclosure in the circumstances outlined above it does not compel the Trust to comply with such information requests. Each case should be considered on the individual merits of the request. Where consent to disclose information to the police is not provided or refused the Trust has to consider the duty of confidentiality owed to the data subject and the public interest in maintaining a confidential service and balance this with the wider public interest in making the requested disclosure to support law and order purposes. Striking the appropriate balance in some situations can be challenging and in these scenarios, where possible, staff should seek specialist advice from the Information Governance Team.

In addition to the police, other agencies such as the Home office, HMRC and NHS Counter Fraud Services may request information about patients using exemptions.

Sharing information for safeguarding purposes

Caldicott Principle 7 makes clear that in certain situations the duty to share information is as important as considerations of confidentiality. This is particularly the case in matters of safeguarding where in the past public authorities have failed individuals by not sharing information they have held which if passed on may have prevented someone harming them.

Where an individual is thought to be at risk, relevant information should be shared between

agencies involved with the individual if the provision of that information might reduce or eliminate the identified risk. If it is possible to obtain consent from the subject to share their data this should be done, but the absence of or a refusal to provide consent should not deter staff from sharing information where it is felt to be appropriate and justified to support a safeguarding purpose.

Access to information for audit, service improvement and research purposes

Clinical audit – recognised as a necessary tool to check the care provided by the Trust meets acceptable standards and is safe and effective. Access to patient personal information (e.g. detailed medical records) without consent for the purpose of clinical audit is normally permissible. The audit should be internal to the Trust and not part of a multi-site/organisation audit and the audit would normally be registered with the Trust clinical audit service. Where these criteria are not met and access to patient information is requested advice should be sought before sharing information or allowing access to patient records.

Service improvement – dependent on the circumstances access to patient personal information without consent for the purpose of conducting a Service Improvement project may also be permissible. The term 'service improvement' is widely used to cover a range of improvement activities and caution should be exercised to ensure the boundaries between service improvement and research activities are not blurred.

Research – the Trust undertakes medical research and clinical trials. Most research activity requires formal ethical approval and patient consent is normally required before access to any patient personal information is provided or made. The need to obtain patient consent can be waived in some circumstances following formal application to the NHS Research Authority (NHSRA). Where access to medical records is required, the researcher must provide the reason for access, steps taken in order to maintain confidentiality and names and status of those needing access to notes. Those users must sign a declaration of confidentiality. Data subjects must be de-identified and signed consent must be obtained.

The flowchart at Appendix A sets out guidance on sharing information.

13.0 Consent

Individuals must in most circumstances be fully informed about the information that is held about them and its intended use. When necessary, their consent will be sought for such use. This is in accordance with data protection law

Obtaining consent

Consent is not normally required for direct care purposes. GDPR Article 9(2)(h) sets this out. Where consent is required this will be recorded on the relevant clinical system

Consent for non-direct care purposes will be sought at the earliest opportunity and subsequently at regular intervals. This must be at the first contact with the person concerned unless the individual is unable, at that time, to fully comprehend the implications or make an informed judgement.

Consent must be sought to share information with relatives, carers, friends etc

Where a person does not have the capacity to make an informed decision but another person has authority to act as their guardian and take decisions on their behalf, then this situation must be explained to that person.

In order to ensure that consent to the sharing of personal information for non-direct care purposes is informed, and to set out rights for individuals, the Trust has a Your Records and You leaflet that explains:

The rights of individuals under the Data Protection Act 2018 and GDPR, particularly in relation to sensitive information.

- Procedures in place to enable clients/patients to access their records.
- Procedures that may have to be initiated when a member of staff suspects that a patient has been or is at risk of abuse. These procedures must include details of whom information will be shared with at each stage, what information will be shared and how the information will be used.
- Circumstances under which information may be shared without consent and the procedures which will be followed.
- Complaints procedures to follow in the event that the individual concerned believes information about them has been inappropriately disclosed.
- How the information is recorded, stored and the length of time it will be retained

Recording consent

Consent for non-direct care purposes or for sharing information with family, friends etc will be recorded on the relevant clinical system by which an individual or their guardian can record whether they give consent to the disclosure of personal information and what limits, if any, they wish placed on that disclosure.

Checking for consent

An individual's record must always be checked before personal information is disclosed for non-direct care purposes to another organisation.

Particular care must be taken before sensitive information is released. Special categories of information must only be released if their disclosure is vital to the case and explicit consent has been given to its release for that purpose, unless it is for direct care as explained above.

14.0 Disposal of personal information

It is a principle of the DPA that data should 'not be kept for longer than necessary'.
To assist staff in meeting this requirement the Trust adopts the retention schedule contained in the NHS Records Management Code of Practice.

All printouts, reports and printed copies of records containing personal data should be kept secure at all times. This particularly applies to handover reports and documents used by staff working in ward areas.

Any documents containing personal data should be disposed of securely and not discarded in domestic waste and recycling bins. The Trust operates a confidential waste disposal service and provides regular collections of confidential waste from all Trust areas.

The disposal of items of electronic equipment which may hold personal data (PCs, laptops and any other devices with information storage capabilities) should be carried out through the Digital department to ensure all data is effectively removed before disposal.

The disposal of medical devices and equipment should follow the guidance on Decommissioning and Disposal provided in the Medical Devices Policy.

15.0 Breach of policy and procedure

Any breach of data protection and confidentiality can have severe implications for the Trust, service users and staff and can impact on the reputation of the NHS as a whole.

Breaches of confidentiality or unauthorised disclosure of any information subject to the Data Protection Act 2018 may constitute a serious disciplinary offence or gross misconduct under the Trust Disciplinary Policy. Staff found in breach of this policy may be subject to disciplinary action up to and including summary dismissal.

The Information Commissioner's Office (ICO) regulates data protection and is charged with upholding individuals' information rights. The ICO has a wide range of powers to enforce compliance which includes the imposition of financial penalties.

Staff must report incidents relating to data protection, data security and confidentiality and should follow the incident reporting procedures contained in the Trust Incident Reporting Policy.

Occasionally it may be necessary to access information on an individual's network account. The rationale and process are set out in the IMT Security policy.

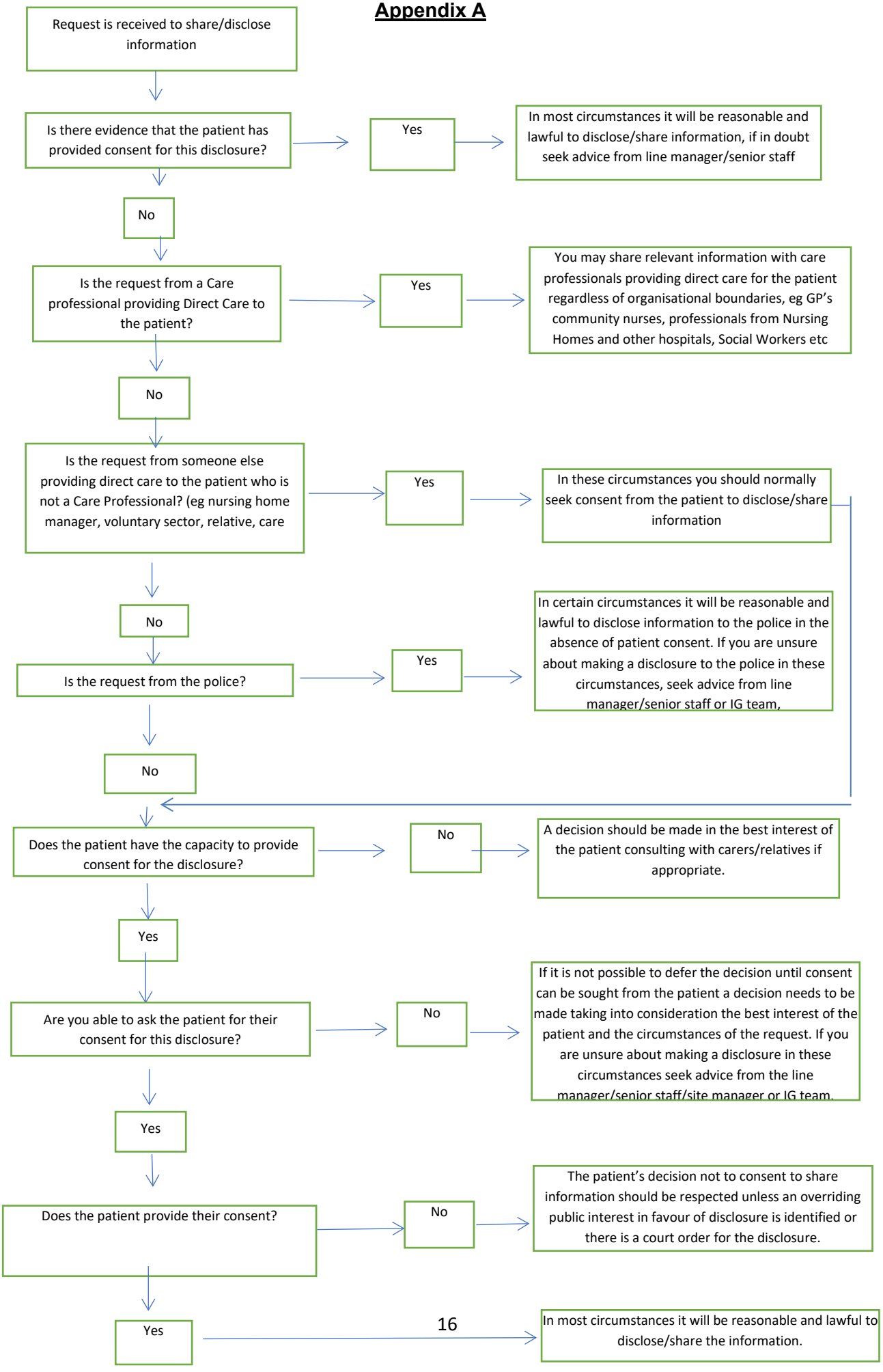
16.0 Definitions

Term	Definition
Personal data	Any information relating to an identifiable person who can be directly or indirectly identified
Data controller:	The organisation (in this case, the Trust) that determines the purposes for which, and the manner in which any personal data are, or are to be, recorded.
Data flow	A continuing or repeated flow of information which takes place between individuals or organisations and includes personal data.
Data processor	Any person or agency that processes data on behalf of the data controller.
Direct care	Provision of clinical services where interaction between the patient and a health care provider takes place. Examples include assessment, performing procedures and implementation of a care plan.
Duty of confidence	Arises when one individual discloses information to another in circumstances where it is reasonable to expect that the information will be held in confidence. It arises from common law.
Explicit consent	Consent normally given orally or in writing, where clear and positive indication is given that the individual understands what they are agreeing to. For data protection purposes, this must clearly set out how the information is going to be used and how consent can be withdrawn.
Information governance	A combination of legal requirements, policy and best practice designed to ensure all aspects of information processing and handling are of the highest standards.
Legitimate relationship	A relationship that exists between a patient and an individual or group of individuals involved in their treatment which provides the justification for those users to access a patient record. Can also apply to staff records.
Processing	The collection, recording or holding of information or data, or carrying out any operation or set of operations on the information or data, including but not restricted to its alteration, retrieval, disclosure and destruction or disposal.
Non care or secondary purpose	Purposes other than direct care such as healthcare planning, commissioning, public health, clinical audit and governance, benchmarking, performance improvement, medical research and policy development.

17.0 Related Trust Policies

- Health Records Policy
- Non Health Records Policy
- Disciplinary Policy
- Clinical Data Quality Policy
- Audio Visual Recording Policy
- Clinical Coding Policy
- Freedom of Information Policy
- Incident Policy
- Access to Health Records Policy
- Registration Authority Policy
- Network, Internet and Email Usage Policy
- Information Governance & IMT Security Policy

Appendix A


Request is received to share/disclose information
Is there evidence that the patient has provided consent for this disclosure?
Yes
In most circumstances it will be reasonable and lawful to disclose/share information, if in doubt seek advice from line manager/senior staff
No
Is the request from a Care professional providing Direct Care to the patient?
Yes
You may share relevant information with care professionals providing direct care for the patient regardless of organisational boundaries, eg GP's community nurses, professionals from Nursing Homes and other hospitals, Social Workers etc
No
Is the request from someone else providing direct care to the patient who is not a Care Professional? (eg nursing home manager, voluntary sector, relative, care
Yes
In these circumstances you should normally seek consent from the patient to disclose/share information
No
Is the request from the police?
Yes
In certain circumstances it will be reasonable and lawful to disclose information to the police in the absence of patient consent. If you are unsure about making a disclosure to the police in these circumstances, seek advice from line manager/senior staff or IG team,
No
Does the patient have the capacity to provide consent for the disclosure?
No
A decision should be made in the best interest of the patient consulting with carers/relatives if appropriate.
Yes
Are you able to ask the patient for their consent for this disclosure?
No
If it is not possible to defer the decision until consent can be sought from the patient a decision needs to be made taking into consideration the best interest of the patient and the circumstances of the request. If you are unsure about making a disclosure in these circumstances seek advice from the line manager/senior staff/site manager or IG team.
Yes
Does the patient provide their consent?
No
The patient's decision not to consent to share information should be respected unless an overriding public interest in favour of disclosure is identified or there is a court order for the disclosure.
Yes
In most circumstances it will be reasonable and lawful to disclose/share the information.