SAR Process

Index:

- Information Governance Manager (IGM).
- Information Governance Co-ordinator (IGC).
- Responsible clinician (RC).
- Senior Manager (SM).
- Information Rights Officer (IRO)
- Associate Director of Information Governance (AD of IG).

Day	Action	Action by	Checklist
1	SAR received (email or post). SAR assigned to Case Handler The ATR inbox is only to be accessed by the IGC & IGM	IGM / IGC	✓ Is the request actually a SAR request or is it a request for specific information etc. that should be forwarded to the relevant clinician to respond to or a transfer of care to be actioned by the IGC. ✓ Is the request for Beds and Luton Adult or CAMHS mental health, Tower Hamlets adult mental health services or Newham adult mental health services? If not, then check who the relevant SAR Lead is and forward to them. ✓ Ensure the request is saved in the relevant sub folder and added to the relevant tab on the SAR spreadsheet. ✓ If the email in anyway indicates a possible complaint, this must be forwarded to the AD of IG for information. ✓ If the email is from the ICO, it must be forwarded IMMEDIATELY to the AD of IG. ✓ If a request indicates there is a claim or potential claim against the Trust, this is sent to the legal team for their information, copying in the AD of IG.
2	SAR logged, file opened. Case files should be named under the service user's name – last name then first name	IRO	✓ Who is the request from? i.e, patient, solicitor, police, friend or family member? ✓ Who is the patient? ✓ Is the patient alive or deceased? ✓ What records are they asking for? i.e, clinical records, emails, letters, reports, telephone recordings, CCTV? ✓ Do we need ID? ✓ De we need consent or authority? ✓ Do we need clarity on what records are needed? i.e, which service, date range etc? ✓ Do we need evidence of access rights if patient is deceased.

2	Send acknowledgment.	IRO	Which acknowledgment needs to be sent? Ensure it is the template for the correct type of requester and asks for any outstanding information needed to process the request or the "accepted" acknowledgement if nothing else is required. If patient is alive, ensure to send SAR template. (1 month to respond by.) If patient is deceased, ensure to send ATHR template. (21 calendar days to respond by.) If the requester is a Solicitor or Police asking for ALL records, ensure to send the acknowledgement asking for further information. Ensure the first bullet point is included asking them to specify which records are needed, not just all.
If ID, consent / authority or further information is required then the clock pauses until it has been received when the clock starts again.			
3	Receive any outstanding ID, consent / authority or further information.	N/A	N/A.
3	Check the ID, Consent / Authority is appropriate.	IRO	✓ The ID should ideally consist of photo ID such as a driving licence or passport. It should also contain proof of address such as a utility bill or bank statement. Proof of address should be dated within the last 6 months (good practice). ✓ Consent or authority should also be dated within the last 6 months (good practice). ✓ Consent or authority must clearly detail what the patient is giving consent to, i.e. which records, and who to send the records to.
3	Check dates for all required actions and enter them into the Access to Records outlook calendar.	IRO	N/A.
3	Start collation of records.	IRO	✓ Check the scope of the request before deciding which systems etc to go to, to collate the records. The following systems may need to be checked **Systems:** ✓ Rio ✓ EMIS ✓ SystmOne ✓ Care Path ✓ Restore – Bedfordshire and Luton only

			✓ Iron Mountain –London ✓ Datix ✓ IAPTus ✓ JAC **Non systems:** ✓ Staff emails ✓ Shared drives
3	Ascertain who the RC / SM is who will need to review and approve the records for release.	IRO	✓ Check the records to see who the latest consultant was that treated the patient. If it is not obvious who this is, email the relevant Head of Admin to ask them to advise who the appropriate RC will be. If it can still not be determined who the RC is, discuss with the IGC or IGM who to send the records to for review and approval. It MUST be a consultant or senior clinician with authority to approve or a senior manager if the records are not clinical. NOTE: For all Newham cases, email Diane Ball to ask who the appropriate RC is.
3	Email the RC / SM to advise they will be receiving records to review shortly and advise them approximately how many records there are. There is a template email for this.	IRO	N/A.
10	Create sub folder, within case file, called 'Original Records' Save all records collated within this folder.	IRO	
10	Create sub folder, within case file, called 'Redacted Records'. Combine into one PDF document all records collated so far. This should be done using Adobe Pro. Save into the Redacted Records folder. Repeat this as and when more records become available, i.e, from IT or archive records.	IRO	N/A
10	Begin review of the combined document and apply suggested redactions using Adobe Pro redactions software.	IRO	✓ Ensure when reviewing the records that anything that is not within the scope of the request is either removed from the combined PDF record or redacted. ✓ Look for 3rd party names detailed within the records and decide if it is likely if the patient / requester would know if the 3rd party references would be there.

	Repeat this as and when more records become available, i.e, from IT or archive records. If records have been received in batches ensure that once they have been reviewed that they are combined into one PDF document.		I.e, record states that patient attended an appointment with their sister. It would be reasonable to assume that the patient knows that their sister attended the appointment with them and does not need to be redacted. If the record states that the patient's friend contacted the clinician to raise concerns about the patient, it is reasonable to assume that this information was given by the friend in confidence and the patient does not necessarily know that their friend this did and therefore any part of that reference including the friends name and the conversation had, should be redacted. Any clinician or staff member named within the records is unlikely to require redaction as it would be reasonable to assume that the patient / requester knew their name. Junior staff member's names could be redacted if it is unlikely that the patient / requester knows who they are, such as a receptionist or junior admin staff member. If there is reference within the records that would suggest releasing a staff members name could potentially cause them harm or distress then it should be redacted. ✓ Any reference within the records that could have the potential to cause harm or distress to the patient / requester should be redacted, however it is usually more appropriate for the responsible clinician or senior manager to decide if this is required.
By day 15	Send the combined records to the RC / SM for review and approval for release. Request the clinician review and confirm approval by day 20.	IRO	✓ Check who the RC / SM is from the action on day 3. ✓ Ensure to attach the RC audit form as an attachment to the email. ✓ For Beds, Luton and Newham use the form for second line review. ✓ Ensure to send details or the actual request so the RC understands the scope of the request. This could be the form completed by the requester or an email from them confirming which records are required. Note: for IAPTUS records, they should be sent to: Bedford - elt-tr.bedfordiapt@nhs.net Newham - newhamtalking.therapies2@nhs.net
18	Send reminder to RC / SM that they need to confirm approval by the deadline given in previous step.	IRO	N/A.

20	If no response from RC / SM, send a chase email.	IRO	N/A.
22	If no response from RC / SM, escalate to IGC.	IRO	N/A.
22	Chase RC / SM.	IGC	N/A.
24	Chase RC / SM.	IGC	N/A.
26	If no response from RC / SM, escalate to IGM.	IGC	N/A.
26	Escalate to Associate Clinical Director (ACD).	IGM	N/A.
28	Chase ACD.	IGM	N/A.
30	If no response from RC / SM, escalate to AD of IG.	IGM	N/A.
20	As soon as the RC confirms their approval apply the redactions previously highlighted using Adobe Pro.	IRO	✓ Has the RC / SM requested any further redactions be applied? If so, ensure to apply those redactions. ✓ If you are unsure if the requested redactions should be applied, discuss with IGC or IGM.
20	Create sub folder, within case file, called 'Disclosed Records' Save the final combined PDF document with fully applied redactions into the Disclosed Records folder.	IRO	N/A.
20	Send the records to the requester.	IRO	✓ Records should be sent to the requester in the same format as the request was received, i.e, by post or email, unless they have specified in their request that they would like to receive it in a different format. ✓ Check where the requester has asked the records to be sent to, i.e, specific email or postal address. ✓ If sending by email, ensure to send using the [secure] method. Then send a non [secure] email to the requester advising that the records have been sent by encrypted email and that it will give them a link to click on to retrieve the records.

			✓ If sending by post, ensure they are contained in a sealed tamper proof envelope and sent by recorded delivery. Ensure that the envelope has the Trusts return PO address on the back. If there is an email address for the requester, email them to advise that the records have been posted. ✓ If the records are too large to be emailed, the combined document may have to be split into smaller PDF documents and sent in more than 1 email. Splitting the combined PDF document can be done within in Adobe Pro. ✓ Save the disclosure email containing attachments in the Disclosed Records folder
20	Update log to confirm date sent and update the notes section to confirm how and when the records where sent.	IRO	N/A.

NOTES:

1. Ensure that the SAR log is updated at every point in processing the request.

2. Check the dates entered into the Access to Records outlook calendar to know when each action should be completed by. The days set are the ideal latest day for the action to be completed. If actions can be completed earlier they should be. If it is not possible to complete the actions by the specific day, ensure the notes section on the SAR log is updated to explain why there is a delay in the relevant action being completed, i.e, records not received from archive etc.

3. Depending on the scope of the request it may be identified that the request is going to be complex. At this point a formal request for an extension should be sent to the IGM. The request should explain the reasons for the extension request. If the extension is approved the requester should be written to, to advise that there will be an extension due to the complexity of the records. A new revised date should be provided.

4. If not all records have been received, i.e, not received from archives or IT etc, combine and review the records that are available. If it appears that the request is likely to breach due to records not being received on time, any records that are available should be combined, reviewed and sent to the RC / SM for review and approve to release. Advise the RC / SM that further records will be sent for review and approval as soon as they are available. Additionally in this instance, the requester should be advised that we are only releasing part of the information requested and give an estimated date when the remaining records will be sent.

5. If it appears that the request is likely to breach due to no records being available or because the RC / SM hasn't responded on time, a formal request for an extension must be sent to the IGM. The IGM will confirm or deny the extension request. The IRO should then write to the requester to apologise and advise that there will be a delay in providing the records. A new estimated date should be provided. Put a reminder in the Access to Records outlook calendar to write to the requester again if it is not going to be possible to provide the records by the new estimated date.

6. If there are over 100 documents in Rio that need to be downloaded a complex SAR request should be sent to IT for them to download the records from the back end of Rio.

7. The IGC will have weekly catch ups with the IROs to ensure that any cases coming up to the due date are noted and if early escalation to the IGM is required, this is done without undue delay.

8. All cases should be worked simultaneously and new cases not delayed by work being completed on existing cases.

9. Please note that all days are subject to working days in the context of the teams actions and if an action falls on a weekend or bank holiday, it can be carried out on the next working day. HOWEVER, the date due for response falls on a weekend or bank holiday, it MUST be actioned the working day prior to the weekend or bank holidays.

10. All emails sent by IROs when dealing with matters should be saved in the folder and then deleted from the ‘sent’ items in the ATR mailbox.

NHS
East London
NHS Foundation Trust

Individual Rights Training

Information Governance Manager – Information Rights

NHS
East London
NHS Foundation Trust

Training Contents

- Introduction, Aims and Objectives
- Types of Requests
- Legislation
- Recognising a Request
- ID, Consent or Authority
- Children's Records
- Processing a Subject Access Request (SAR),
- Processing an Access to Health Records Request (ATHR)
- Review and Redaction Considerations
- Redaction Process
- Disclosure
- Letter Templates
- Additional Information

NHS
East London
NHS Foundation Trust

Introduction, aims and objectives

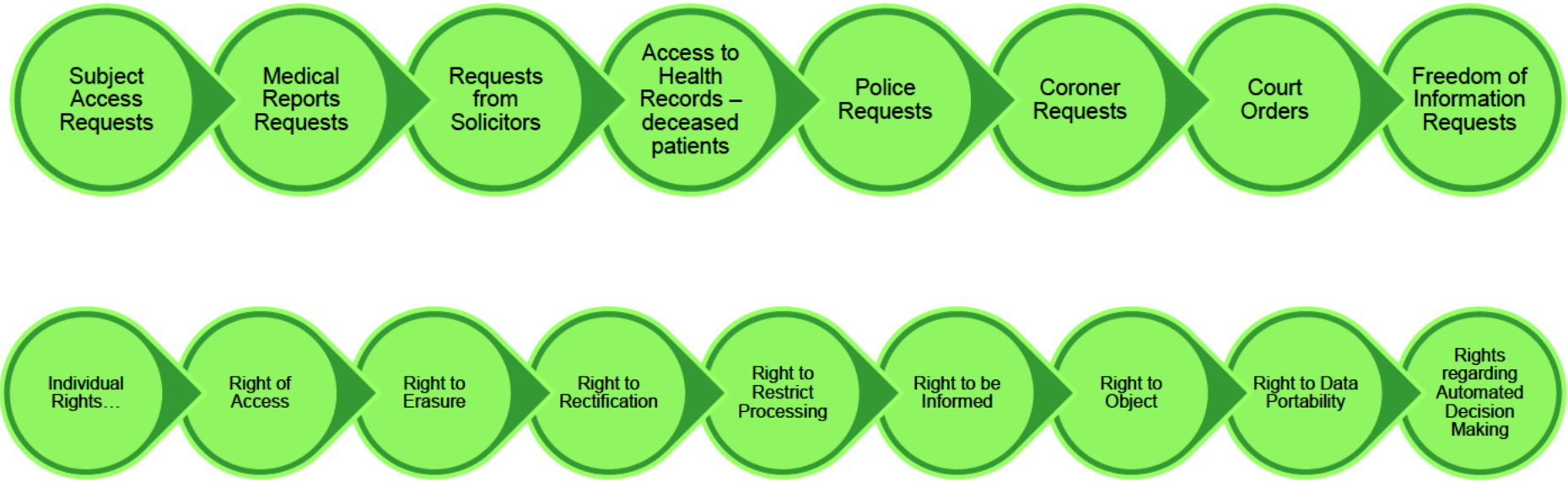
- This training has been developed for all SAR Leads within East London NHS Foundation Trust to support and build on existing knowledge and act as a refresher.

- The training includes information on the legislation we are required to adhere to, different types of requests and processes.

- By the end of this training you should feel more confident about how to process requests for information and have a resource to fall back on should you require it.

NHS
East London
NHS Foundation Trust

Types of Requests



NHS
East London
NHS Foundation Trust

Data Protection Act – Subject Access Requests (SAR)

- The Data Protection Act only applies to Living Individuals!
- All individuals (known as data subjects) have the right to access information held about them.
- They can make a SAR request themselves or ask a personal representative to make the request on their behalf, whether family, friend or legal representative.
- Requests should be in writing, wherever possible and be accompanied by the appropriate ID and / or consent / authority.
- We have 1 calendar month to respond to a SAR.
- The clock starts as soon as the request is received into the organisation (not necessarily the team that will process the request). The clock can be paused if ID or further information is required to process the request and will restart once that information has been received.
- This may be extended for a further 2 months if the request is complex. Processing a SAR for medical records SHOULD NOT automatically be considered complex. All extensions beyond one month need to be approved by the Information Governance – Information Rights Manager.
- We cannot charge a fee unless the request is a duplicate and the records have been provided previously.
- All records should be reviewed and any 3rd party information redacted. Additionally if there is information within the records that could cause harm to the data subject or the requester, this should also be considered for redaction.
- All records should be checked by an appropriate clinician / manager before being disclosed.

NHS
East London
NHS Foundation Trust

Police Requests

- From time to time the Police may need to request copies of records for either a perpetrator or a victim depending on what evidence they require for an investigation.

- All police requests must come accompanied by a Data Protection Act (DPA) form, which should detail who the data subject is, exactly what records they require and under which legislation they require the records. Note – only information relevant to the investigation should be disclosed.

- Ideally they should also provide consent from the data subject, however it is not always appropriate for the police to obtain consent. This may be because making the data subject aware that the police are requesting information about them could jeopardise the police investigation.

- If consent is not provided, the police should confirm in writing why obtaining consent is not appropriate.

- Once this has been completed the request should be processed as a SAR.

Access to Health Records (AtHR)

NHS East London NHS Foundation Trust

- Access to Health Records only applies to deceased individuals.
- Although the Data Protection Act doesn't apply to deceased individuals, a duty of confidentiality should remain in place as per common law.
- Requests for a deceased persons records can only be granted to a very limited type of requester:
  - If the requester is the deceased's personal representative, i.e. they are the executor or administrator of the deceased person's estate. Evidence of this must be obtained.
  - If the requester can establish a claim arising from the data subjects death. The claim would have to be evidenced prior to releasing data.
- Prior to releasing records, any recorded wish by the deceased to not allow their records to be shared, must be checked and adhered to.
- Records should always be reviewed and any 3rd party information redacted as well as any information that may cause harm to the deceased's reputation or the requester.
- If an AtHR is received by a public body such as the Courts, various regulators and commissions such as the Audit Commission or CQC, it is generally considered appropriate to disclose the requested records, however confirmation should be clarified as to why the records are required and if anonymised records would be sufficient prior to disclosure.
- Disclosures in the absence of a statutory basis should be in the public interest, be proportionate, and judged on a case-by-case basis.
- A request should be processed within 21 days where the record has been added to in the last 40 days, and within 40 days otherwise. These are calendar days. It is seen as good practice within the NHS to always aim to respond within 21 days and therefore **ELFT requires all AtHR requests to be responded to within 21 days.**

Coroners Requests

- The public interest served by Coroners' inquiries normally outweighs considerations of confidentiality and competing public interests.
- Coroners have powers to request information under the Coroners and Justice Act 2009.
- The Trust's legal team are the **only** team authorised to liaise directly with the Coroner's Office.
- Normally records are disclosed in full.
- Where there is concern regarding a potential disclosure or requirement for redaction the Associate Director of Legal Affairs will liaise in the first instance with the DPO.

Medical Reports Requests (MRR)

NHS
East London
NHS Foundation Trust

- Medical Records Requests provides access to medical reports made by a medical practitioner who is or has been responsible for the clinical care of the patient.
- These reports may be for insurance or employment purposes.
- Consent of the patient must be evidenced prior to disclosure.
- The patient must be offered the opportunity to review the medical report prior to release of the report.
- The report should not be released to the requester until the patient has consented to the disclosure.
- Patients have the right to request amendments to the report. Requests should be considered and the report amended or a note added if the clinician declines to amend. Amendment requests should be made in writing.
- If a patient is not happy with the report they can refuse to allow disclosure.
- Reports should be reviewed to ensure there is nothing recorded that could cause harm to the patient.
- Requests for Medical Reports should be managed and processed by the most appropriate clinician and not the Access to Records team or SAR Leads.

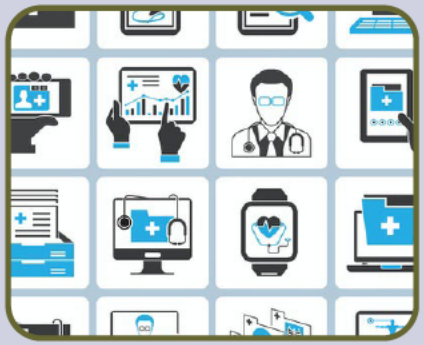
Court Orders

- We must request evidence of court proceedings.
- Do not simply rely on an email saying there is a Court Order.
- Redaction will depend on what is being asked, however any references to other patients, whose information may have been accidentally recorded in the wrong file, must be redacted.
- All requests with Court Orders must be assessed and processed on a case by case basis.

Legislation

East London NHS Foundation Trust

Access to Medical Reports Act 1988



Access to Health Records Act 1990

GDPR / Data Protection Act 2018

Freedom of Information 2000

Recognising a request - examples

NHS East London NHS Foundation Trust

Subject Access Request

- A request for personal information of a living individual.
- *"Please can you send me a copy of my physiotherapy records."*
- *"We act on behalf of your patient and require copies of all their inpatient records."*

Access to Health Records

- A request for personal information of a deceased individual.
- *"Please provide a copy of my late mothers discharge letter."*

Request for Medical Reports

- A request for a report about a patient.
- *"Please provide us with a report regarding this persons ability to testify in court."*
- *"Please provide information regarding why this person was referred to your service."*

Freedom of Information

- A request for corporate information about a public authority organisation.
- *"Please send me copies of your annual reports for the last 3 years."*
- *"Please send me a list of all your off framework agency providers."*

Identification

NHS East London NHS Foundation Trust

A subject access request must be accompanied by photocopies of two different official documents that between them provide sufficient information to prove name, date of birth and current address e.g. driving licence, medical card, birth certificate or passport etc. together with a utility bill, council tax notice, bank statement (with the financial details blanked out).

- If the request has been received by the data subject themselves, then ID will need to be obtained for them only.
- If the request has been received by a family member or friend on behalf of the data subject, ID will need to be obtained for the data subject and the person making the request.
- If the request has been received by a legal representative, ID does not need to be obtained specifically but you should ensure you are satisfied that the legal representative has completed all due diligence with the data subject.
- If the request has been received by an individual (family member or friend) for records of a deceased person, ID must be obtained for the requester.
- There will be times when ID is not required. For example, a clinician who regularly cares for a patient and who receives a SAR request directly from the patient. The clinician clearly knows who the patient is and therefore it would be unreasonable to request ID.
- Similarly it may not always be possible for a data subject to provide ID if perhaps they are homeless or currently in prison. In these instances it is advisable to ask the data subjects most recent clinician if they are satisfied that the data subject is who they say there are.

Consent

NHS
East London
NHS Foundation Trust

Consent should be fully informed and explicit. The Trust should be satisfied that the data subject (subject to their mental capacity) has provided consent fully understanding what they are consenting to. For example, what information is being requested and who it is being shared with. E.g. a data subject may think their representative is only asking for records around the time of an accident where as in fact the representative is asking for full records.

- Consent should always be reviewed so you are satisfied, to the best of you knowledge and ability, that the consent has been signed by the data subject.
- If you are at all unsure that the signed consent is genuine or you believe that the data subject would not have consented, it is advised to contact the data subject directly to ask them to confirm if the consent is genuine. In most cases consent will be genuine but that is NOT always the case!!
- If you are at all unsure that the data subject has fully understood what they have consented to, again it is worth checking directly with the data subject.
- If you believe the data subject does not, or did not at the point of time in question, have the mental capacity to consent, this should be discussed with the data subjects clinician or a manager depending on who the data subject is. Also see next slide on Authority.
- Police – just because the police request copies of records, doesn't mean they have the automatic right to be provided with it. You should always ask the police to provide consent from the data subject or advise why consent cannot be obtained – see next slide on Authority.

NHS
East London
NHS Foundation Trust

Authority to Act

Authority for a representative to request copies of records on behalf of a data subject could be for a number of reasons. If the data subject is fully aware of the request and has the capacity to consent, then consent should be obtained. However if the data subject does not have capacity to consent – remembering that this could be a moment in time lack of capacity or a longer term lack of capacity – then the requester must provide appropriate legal evidence of their right to request the information.

- This could include a Lasting Power of Attorney (LPoA). If LPoA is provided, it should be checked to ensure it is the correct type. For copies of medical records the LPoA should provide the requester the right to act on behalf of the patient in terms of their Health and Welfare. An LPoA for Property and Finance Affairs can only be used if the information being requested is to support the requester in managing property or finance on behalf of the data subject.

- Litigation friend - A litigation friend can be appointed to make decisions about a court case for either: an adult who lacks the mental capacity to manage their own court case either with or without a solicitor or for a child. Confirmation of Litigation Friend is provided by the Court.

- You may be asked to provide copies of records to the police where they are unable to provide consent of the data subject as they may be unable to locate the data subject or, requesting consent could prejudice a criminal investigation. Therefore the police request should be accompanied by a DPA form advising exactly what is being required and the legislation under which it is being requested. It should also state the reason why consent cannot be obtained and be signed by a senior officer.

- Should the request be made by a deceased persons personal representative, evidence that they are the deceased persons personal representative must be provided. If the requester is not a personal representative they may advise they have a claim arising from the data subjects death and again, evidence of this must be provided.

Request types verses due diligence checks

NHS East London NHS Foundation Trust

	Identification	Data Subject Consent	Authority to Act
Data Subject	✓	X	X
Personal Representative – Living Data Subject with Capacity	✓ (Both DS and Personal Rep)	✓	X
Personal Representative – Living Data Subject without Capacity	✓ (Both DS and Personal Rep)	X	✓
Personal Representative - Deceased Data Subject	✓ (For Personal Rep)	X	✓
Solicitors – Living Patient	X	✓	✓
Solicitors Agents – Living Patient	✓	✓	✓
Solicitors – Deceased Patient	X	X	✓
Police – Data Subject Aware	X	✓	✓
Police – Data Subject Unaware	X	X	✓
Court Order	X	X	X
Coroner Request	X	X	X
Medical Report	X	✓	X

This is not set in stone and consideration should be taken to each individual case before deciding what is needed

NHS
East London
NHS Foundation Trust

Children's Records

When a request is made for a child's records, a number of considerations should be made:

- Is the child old enough to request their own records.
- Is the child old enough to consent to a representative requesting their records.
- Generally if a child is 12 years old, they are considered old enough to consent, however this will also depend on their competency / mental capacity to consent. It is likely the child's clinician is best placed to make this judgement.
- Competence is assessed depending on the level of understanding of the child.
- Whilst we should take a reasonable approach a child should not be considered competent if it is evident he or she is acting against their own best interests

If a personal representative requests records on behalf of a child you should check:

- Does the representative have authority to act for the child / do they have parental responsibility?
- Are they the usual parent / guardian of the child?
- Are there any court orders relating to the parental / guardian responsibility.
- Is there anything in the child's records that would indicate the requester should not have authority?
- Are there any safeguarding concerns around the requester having access to the child's records?
- Is there any information held within the child's records that should not be released to the requester as the information could cause harm to the child?

NHS
East London
NHS Foundation Trust

Processing a Subject Access Request

Receive request

-

1 month clock starts

Request ID / consent / authority –

Clock pauses

ID / consent / authority received –

Clock restarts

Gather records requested

Review and redact

Obtain approval from appropriate person (clinician / manager)

Disclose records

We care We respect We are inclusive

NHS
East London
NHS Foundation Trust

Processing an Access to Health Records Request

Received request

-

21 / 40 calendar days deadline starts

Request appropriate evidence of right to access deceased records as well as proof of ID

–

Clock pauses

Receive ID and evidence of right to access

-

Clock restarts

Review evidence of right to access and decide if records can be disclosed

If records can be disclosed, gather records within the scope of the request

Review and redact

Obtain approval from appropriate person (clinician / manager)

Disclose records

We care We respect We are inclusive

East London NHS Foundation Trust

Review and Redaction Considerations

Redactions Continued

NHS East London NHS Foundation Trust

- Any data relating to a different data subject must be redacted from the records. This should also be followed up to ensure the records are placed onto the correct records.
- Information given about or provided by a family member of friend of the data subject that was given confidence. If the information is clearly known by the data subject already, i.e. the data subject had discussed a conversation they had with their mother, then this does not need to be redacted. However should the mother be requesting the records on behalf of the data subject, this should be re-reviewed.

  When redacting 3rd party information, redacting names alone may not be sufficient and consideration should be made to the full information recorded around the 3rd party.

  Redacting 3rd party data will very much depend on what the data subject / requester is already aware of.
- Safeguarding information that could cause potential harm to the data subject or requester should be reviewed and redacted.
- Information that could cause serious harm to the data subject (or another individual) physical or mental health, should they receive it, should be considered for redaction with reasons documented. This does NOT include information that could cause embarrassment to the organisation.
- Information about children should be considered inline with redactions around 3rd party data and safeguarding concerns.
- Information provided by other services / organisations, if held by the Trust, form part of our record for the data subject and therefore should NOT automatically be redacted. The decision to include those parts of the record should be made based on the scope of the request itself.
- Staff and clinician names are NOT generally considered to be 3rd party information. The names will usually be detailed in their professional capacity and therefore do not require redaction. However, it should be checked that all staff / clinician names are detailed in their professional capacity and not in a personal capacity, e.g. they are also a family member of the data subject and have been named in that respect.

Redactions Process

NHS
East London
NHS Foundation Trust

- Before disclosing any records to a requester they should be fully reviewed and appropriate redactions made.
- Has it been recorded anywhere that the data subject **does not** wish for their records to be disclosed either in full / part or to a named individual / organisation?
- It is recommended that records are disclosed as PDF documents via secure email. Redaction software can be purchased to complete appropriate redactions on the PDF documents. It is also easier to combine all records into 1 PDF document than have lots of different records saved.
- Most requesters will ask for records to be disclosed to them electronically, however if they have requested paper records, this should be granted. Once the PDF records have been redacted, print them and arrange delivery / collection for the requester.
- It is NOT recommended to redact paper copies using permanent markers and photocopying as this does not always fully redact the information beneath it.
- A clean (un-redacted) copy of all disclosed records should be saved in an appropriate folder. A redacted copy of all disclosed records should also be saved in a separate folder. This allows a full review should a complaint or query about the disclosure be raised.

Disclosure

NHS
East London
NHS Foundation Trust

- Ensure all records have been fully reviewed and appropriate redactions made.
- Check all pages are in the correct order and not upside down or eligible.
- Are the records in the format required by the requester?
- Have the records been fully reviewed and redactions confirmed by the responsible clinician or manager?
- Check where and how the records should be sent. If the requester has not specified how they wish to receive the records, they should be disclosed using the same format the request was received.
- If email, send via secure method – [secure]
- If post, use secure tracked delivery.
- Confirm in the disclosure letter what systems have been searched, confirmation of any redactions, including page numbers, and reasons for redactions.
- All disclosure letters should include the requesters right to complain and how to do so.

Letter Templates

ELFT has standard letter / email templates to:

- Acknowledge a request
- Request ID / consent / authority / further information
- Seeking clarification
- Request clinician / manager approval
- Disclosure of records

Additional Information

NHS East London NHS Foundation Trust

Manifestly unfounded - A request may be manifestly unfounded if there is:

- No clear intention to access / use the information.
- Malicious intent:
  - To cause disruption
  - The request makes unsubstantiated accusations
  - The individual is targeting someone they have a grudge against
  - There are systematic or frequent requests designed to cause disruption

Excessive - A request may be excessive if it:

- Repeats the substance of previous requests and a reasonable interval has not elapsed
- It overlaps with other requests
- It is NOT excessive just because the individual has asked for a lot of information. We can ask the requester if they are able to refine their request to specify the services they accessed or time frames for the records, however if the requester is unable to refine their request then we are required to comply

Scope of the request

- Remember to only disclose records within the scope of the request. If the request asks for records from 15th January to 17th February, then only these records need to be gathered and processed.
- Equally if the requester has asked for everything and confirms this is what is required, then every effort should be made to obtain all records held for the data subject by all and any department within the Trust. This is best to be co-ordinated by one team rather than lots of teams processing different aspects of the request.

Charges

- You **cannot** charge for a Subject Access Request, however if the request is repeated e.g, the requester asks for paper copies after disclosure, a reasonable fee can be charged.
- You can still charge for an Access to Health Records Request as well as for a Medical Report Request. **Note: ELFT does not charge for Access to Health Records Requests**.

NHS
East London
NHS Foundation Trust

Transfers of Care

- We often receive requests for records from other NHS organisations who require patient records in order to continue treatment for the patient.
- This maybe if the patient has moved to a different area and now comes under a different hospital.
- These requests should be processed as quickly as possible to prevent delays.
- No redactions should be made, however the records should be checked to ensure there is no information relating to an incorrect data subject.
- ID, Consent and Authority are not required for Transfers of Care.
- No charges can be requested.

NHS
East London
NHS Foundation Trust

Questions

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