

IG-003 Access to Records Policy

*(also known as Subject Access Requests or
Access to Records Requests)*

Document Type	Policy
Document Number	POLEECH/003
Document Owner / Author:	Head of Governance
Document Service / Designation	Information Governance / Governance & Resilience
Approval / Ratification	Approval – Information Governance Group/Senior Information Risk Owner (SIRO) Ratification – Director of Corporate Affairs
Medicines	n/a
Standards, legislation or key related documents (including related Policies & SOPs)	• UK General Data Protection Regulation (UK GDPR) • Data Protection Act 2018 • Access to Health Records Act 1990 • ICO Guidance on the Right of Access • NHS Records Management Code of Practice • Trust Information Governance Policy • Subject Rights Request / Access to Records SOP
CQC Domain	Effective, Responsive, Well Led
Keywords	Access to records, ATR, SAR, Subject Access Requests, Information Governance, IG, Data Protection, GDPR

This is a controlled document. Whilst it may be printed, the electronic version on the Trust's Intranet is the controlled copy. Any printed copies are not controlled.

Version Control Summary

Version Number	Name and Title of Author or Committee	Description of Change to Document or Status (including page or section)	Date Approved
0.1	Head of Governance	Review of NCHC and CCS existing policies to create single new organisational policy.	March 2026
0.2	Head of Governance	Review by IG leads in NCHC and CCS	March 2026
0.3	Head of Governance	Review by Information Governance Steering Group	March 2026
0.4	Head of Governance	Executive Director review and comment	March 2026
1.0	Executive Team	Policy Approved for Day 1	1 st April 2026
1.1	Head of Governance	Errors identified by audit have been updated	8 th July 2026

Access to Records Policy

Contents

Section		Page
	Version Control Summary	2
1	Introduction / Purpose	4
2	Aims & Objectives	4
3	Scope	4
4	Policy Statement or Procedure / Standards	5
5	Individual, Departmental and Committee Duties - Accountability and Responsibilities	6
6	Training / Competency	7
7	Monitoring and Audit for Compliance	7
8	References	8
9	Equality Impact Assessment (EIA) and Quality Impact Assessments (QIA)	8
Appendices		
Appendix 1	Glossary / Definitions	11
Appendix 2		
Appendix 3		
etc		

1. Introduction / Purpose

- 1.1 This This policy sets out the Trust's approach to fulfilling its legal obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and, where applicable, the Access to Health Records Act 1990 (AHRA 1990) when individuals request access to personal information held about them.

Individuals have the right to request access to their personal data and to exercise a set of additional rights over that data. Within this policy:

- Subject Access Requests (SARs) refers to requests made by or on behalf of living individuals under UK GDPR/DPA 2018.
- Access to Records Requests (ATRs) is used as an umbrella term that includes SARs and requests for access to a deceased person's health records under AHRA 1990.

This policy ensures the Trust responds to requests lawfully, transparently, promptly, and securely, in a manner that maintains trust, protects confidentiality, and supports high quality record keeping.

This policy should be read alongside the Subject Access Request / Access to Records Standard Operating Procedure (SOP), which contains detailed operational instructions and workflows

2. Aims & Objectives

- 2.1 The aims of this policy are to:
- Ensure the Trust complies with legal requirements governing individual rights of access and control.
 - Provide clear guidance for staff on recognising, receiving, and responding to SARs/ATRs.
 - Support timely, accurate disclosure of information within statutory timeframes (normally 30 calendar days, with a lawful extension where justified).
 - Protect confidentiality, including the appropriate handling and redaction of third party information.
 - Promote transparency and consistent practice across the organisation.
 - Reduce the risk of data breaches, complaints, and regulatory action by ensuring that all requests follow a governed process.

3. Scope

- 3.1 This policy aims to:
- Ensure the Trust complies with legal requirements governing individual rights of access and control.
 - Provide clear guidance for staff on recognising, receiving, and responding to SARs/ATRs.
 - Support timely, accurate disclosure of information within statutory timeframes (normally one calendar month, with a lawful extension where justified).
 - Protect confidentiality, including the appropriate handling and redaction of third party information.
 - Promote transparency and consistent practice across the organisation.

- Reduce the risk of data breaches, complaints, and regulatory action by ensuring that all requests follow a governed process.

4. **Policy Statement / Procedure and Standards (*delete as applicable*) (sections relating to the body of the procedural document)**

4.1 Policy Statement -

The Trust is committed to:

- Ensuring individuals can exercise their rights over personal data easily and transparently.
- Maintaining the accuracy and integrity of the information we hold.
- Responding to SARs/ATRs within 30 calendar days unless a lawful extension is justified.
- Ensuring disclosures are secure, appropriate, and in line with statutory exemptions.
- Upholding confidentiality, including after a patient's death.
- Ensuring redaction and removal of third-party data where required.
- Providing copies in an intelligible format, including explanations of medical terminology where necessary.

4.2 Summary of Procedure (Full details in Appendix A–E)

All staff must follow the high-level steps below.

Operational routes may differ depending on local service arrangements, but the required standard is the same for all teams across the organisation.

1. Recognise a request

Any verbal or written request for personal information must be treated as an Access to Records / Subject Rights Request (ATR/SAR), regardless of the terminology used.

2. Initial handling of the request

Requests should be handled according to the applicable local process model, which will fall into one of the following approved routes:

- **Route A** – Direct handling by the Information Governance (IG) Team
Where local arrangements require the IG Team to process, extract and prepare the relevant information before it is shared with services for review.
- **Route B** – Service-led retrieval and review
Where local arrangements require service teams to locate, retrieve and review records themselves before providing them to the IG Team for checking and release.

Both routes follow identical standards for validation, review, redaction, and disclosure.

3. Validation

The IG Team will:

Confirm the identity and authority of the requester
Confirm the scope of the request
Confirm the applicable legislation
Log the request and assign a reference number

4. Locating and reviewing records

Depending on the operational route:

Records will either be retrieved by the IG Team or retrieved by the service area, but in all cases the same standards apply:
All relevant information must be captured

No information may be excluded solely because it is archived, aged or difficult to retrieve

Review must identify any third-party content or sensitive material requiring redaction

5. Redaction and third-party review

Only information appropriate for disclosure will be included

Third-party or harmful information must be withheld or redacted

Sensitive cases must follow clinical or IG guidance

6. Double-check process

A mandatory quality-assurance review to be completed before disclosure.

This may be undertaken by:

- The IG Team
- Service Managers
- Senior or clinical leads

depending on the operational route.

7. Secure disclosure

Information is disclosed in the requester's preferred format unless unreasonable

Approved secure transfer methods must always be used

8. Documentation and record-keeping

A complete audit trail must be maintained

Records must be retained according to the organisational retention schedule

4.3 Exemptions and Withholding Information (Summary)

Full details are provided in Appendix C.

The decision to withhold information follows the same criteria, regardless of operational route. Information may be withheld if disclosure would:

- Reveal third-party information without consent
- Cause serious physical or mental harm to any person
- Breach legal privilege or statutory restrictions
- Include confidential information provided by authorised external agencies

4.4 Appeals and Complaints (Summary)

Full details are provided in Appendix D.

All requesters have the right to:

- Request an internal review if dissatisfied with the outcome
- Escalate concerns to the Information Commissioner's Office (ICO) if still dissatisfied

The appeals process applies consistently across all operational routes.

5. Individual, Departmental and Committee Duties - Accountability and Responsibilities

5.1 Chief Executive - Overall accountability for ensuring the Trust meets its legal obligations.

5.2 Senior Information Risk Owner (SIRO) - Leads oversight of the management of SARs, including ICO communications and compliance concerns.

5.3 Caldicott Guardian - Ensures that disclosures involving patient information uphold confidentiality and the Caldicott Principles.

- 5.4 Data Protection Officer (DPO) - Provides expert advice on data protection law and oversees rights management and compliance.
- 5.5 Information Governance Team - Responsible for:
- Receiving, logging and validating requests
 - Coordinating retrieval, review, redaction, and disclosure
 - Advising staff and managing compliance with statutory timeframes
 - Reporting breaches or delays through governance structures
 - Maintaining central records of ATR/SAR cases
 - Supporting appeals and ICO investigations
- 5.6 Service Managers & Directors
- Ensure timely responses by locating and reviewing records
 - Conduct mandatory double checks
 - Ensure clinical staff review complex cases
 - Verify accuracy and lawful redaction prior to disclosure
 - Maintain compliance within their service areas
- 5.7 All Staff
- Must recognise and forward all ATR/SAR-related requests immediately
 - Maintain confidentiality and ensure good record management
 - Support IG in locating relevant information promptly
- 5.8 Meetings
- Information Governance Group: oversight of policy and performance
 - Quality Committee: assurance to the Board on compliance and quality

6. Training / Competency

- 6.1 Mandatory Training - All staff should complete annual Information Governance training, including recognition of SARs/ATRs.
- 6.2 Specialist Training
- 6.3 Additional training is required for:
- IG Team
 - IAOs and IAAs
 - Staff involved in retrieval and redaction
 - Staff processing complex or sensitive ATRs
- 6.4 Competency and Monitoring
- Training completion monitored via LEAD systems.
 - Assurance of competency through SOP adherence and audit findings.

7. Monitoring and Audit for Compliance

- 7.1 Monitoring Methods
- Audit of ATR/SAR case files
 - Spot checks on redaction quality
 - Review of statutory timeframe compliance
 - Incident reporting (data breaches or delays)
 - Reports to IG Group and Quality Committee

7.2 Non-Compliance
Breaches or failures to comply are escalated in line with IG governance and may require action plans.

7.3 Learning
Themes and lessons are shared with service areas and committees, informing improvements to processes, training, and SOPs.

8. References

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Access to Health Records Act 1990
- ICO Guidance on the Right of Access
- NHS Records Management Code of Practice
- Trust Information Governance Policy
- Subject Rights Request / Access to Records SOP

9. Equality Impact Assessment (EIA) and Quality Impact Assessments (QIA)

The author has carried out an Equality Impact Assessment (EIA) and a Quality Impact Assessment (QIA).

EQUALITY IMPACT ASSESSMENT – WHAT IS THE IMPACT TO DIFFERENT GROUPS?		
Choose either a Positive or Negative impact. POSITIVE - it could benefit or would have little or no impact. NEGATIVE - it could disadvantage or have an adverse impact. Please provide supporting comments, both on positive and negative impacts. You may need to complete a full Equality Impact Assessment to understand the impact further.		COMMENTS
Age: Consider and detail across age ranges on old and younger people. This can include safeguarding, consent, and child welfare.	Positive	
Disability: Consider and detail on attitudinal, physical, and social barriers.	Positive	
Race: Consider and detail on difference ethnic groups, nationalities, Gypsies, Roma, Travelers, language barriers.	Positive	
Sex: Consider and detail on men and women	Positive	
Gender reassignment: (including transgender) Consider and detail on transgender and transsexual people. This can include issues such as privacy of data and harassment	Positive	
Sexual orientation: Consider and detail on heterosexual people as well as lesbian, gay and bi-sexual people.	Positive	
Religion or belief: Consider and detail on people with different religions, faiths, or beliefs or none.	Positive	
Pregnancy and maternity: Consider and detail on working arrangements, part-time working, and infant caring responsibilities.	Positive	
Marriage and civil partnership: Consider people married or in a civil partnership.	Positive	
Environment: Consider impact on transport, energy, and waste	Positive	

Other identified groups: Consider and detail and include the source of any evidence on different socio-economic groups, area inequality, income, resident status (migrants) and other groups experiencing disadvantage and barriers to access.	Positive	
Were any NEGATIVE impacts identified?	No	
If YES , you will need to complete a full Equality Impact Assessment . Please contact the Company Secretary and Freedom to Speak Up Guardian for assistance to complete a full Equality Impact Assessment via sarah.feal@nhs.net		

QUALITY IMPACT ASSESSMENT – WHAT IS THE IMPACT TO DIFFERENT GROUPS IN SOCIETY?		
Choose Positive, Negative or No impact. POSITIVE it could benefit or would have very little or no impact. NEGATIVE it could disadvantage. Please provide supporting comments, both on positive and negative impacts. You may be asked to complete a FULL QUALITY IMPACT ASSESSMENT to understand the impact further.	COMMENTS	
Compliance with NHS Constitution right to: - Quality of care and environment - Nationally approved treatments/ drugs - Respect, consent and confidentiality - Informed choice and involvement - Complain and redress - Care delivered in a timely way	Positive	
Impact on partner organisations and any aspect of shared risk	Positive	
Impact on organisations duty to safeguard children and vulnerable adults	Positive	
Impact on other services within the organisation	Positive	
List any other risk indicators relevant to the Duty of Quality	No Impact	
PATIENT SAFETY		
Impact on patient safety	Positive	
Impact on preventable harm	Positive	
Impact on reliability of safety systems and processes	Positive	
Impact on systems and process for ensuring that the risk of healthcare acquired infections to patients is reduced	Positive	
PATIENT EXPERIENCE		
Impact on self- reported experience of patients and service users in national / local surveys	Positive	
Impact on self- reported experience of patients and services users through the complaints process	Positive	
Impact on the self- reported experience of patients and service users through PALS contacts	Positive	
Impact on patient choice	No Impact	
Impact on patient access	No Impact	
Impact on the commitment to provide individualised care	No Impact	
CLINICAL EFFECTIVENESS		

Impact on the implementation of evidence based practice	No Impact	
Impact on clinical outcomes	No Impact	
Impact on clinical leadership	No Impact	
Impact on the full adoption of best practice	No Impact	
Impact on variations in care	No Impact	
Impact on ensuring care is delivered in the most clinically and cost effective setting	No Impact	
Impact on clinical engagement	No Impact	
Impact on clinical workforce – capability, capacity and skills	No Impact	
Impact on non clinical workforce – capability, capacity and skills	No Impact	
Were any NEGATIVE impacts identified?	NO	
If YES, you will need to complete a full Quality Impact Assessment and send to Chief Nurse. Form available on the Document Control Library.		

Statements

Consultation and development process	<i>Fill in here</i>
Dissemination	<i>Fill in here</i>
Financial Implications	Financial Implications: In line with the Economic Crime and Corporate Transparency Act 2023, the Trust has a framework in place to prevent and detect fraud, bribery, and corruption. This includes clear governance structures, financial controls, due diligence procedures, staff training, and accessible reporting mechanisms. The Local Counter Fraud Specialist (LCFS) plays a key role in supporting compliance through awareness, and the investigation of suspected wrongdoing. The Trust is committed to fostering a culture of integrity and transparency, ensuring all staff understand their responsibilities and know how to raise concerns. The LCFS contact details are available on the Trust's Intranet.
Diversity & Inclusion Statement	East of England Community Health and Care NHS Trust will ensure that this policy is applied in a fair and reasonable manner that does not discriminate on such grounds as age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex & sexual orientation.
Sustainability	Sustainable Development – Environmental  Do you really need to print this document? Please consider the environment before you print this document and where possible copies should be printed double-sided. Please also consider setting the page range in the print properties, when relevant to do so, to avoid printing the document in its entirety.

This is a controlled document. Whilst it may be printed, the electronic version on the Trust's Intranet is the controlled copy. Any printed copies are not controlled. As a controlled document, this document should not be saved onto local or network drives, but should always be accessed from the Trust Intranet page.

Appendix A – Glossary/Definitions

Access to Health Records Act 1990 (AHRA 1990)

Legislation that governs the rights of certain individuals to access the health records of deceased persons.

Access to Records Request (ATR)

An umbrella term used by the Trust to refer to any request for access to personal information, including:

- Subject Access Requests (SARs) for living individuals
- Requests for access to deceased persons' records under AHRA 1990

Audit Trail

A documented record showing how an ATR/SAR was handled, including decisions, redactions, checks, disclosures and communications.

Authorised Representative

A person legally permitted to request information on behalf of an individual (e.g., parent, attorney, legal guardian, solicitor with consent).

Caldicott Guardian

A senior clinician responsible for protecting the confidentiality of patient information and ensuring disclosures follow the Caldicott Principles.

Data Breach

Any incident where personal data is lost, disclosed, accessed or altered unlawfully or in error.

Data Protection Act 2018 (DPA 2018)

UK legislation supplementing the UK GDPR, outlining how personal data must be processed, protected, and accessed.

Data Protection Officer (DPO)

The statutory role providing expert advice on data protection law and overseeing compliance with individual rights, including SARs.

Double-Check Process

A mandatory quality assurance step where disclosures are reviewed by IG, service managers or clinical leads to ensure accuracy, lawful redaction and completeness before release.

Harm Test

An assessment used to determine whether releasing information would cause serious physical or mental harm to any person.

Identity Verification (ID Check)

A validation step ensuring the requester has the legal right to access the information and that their identity (and authority, if acting for another) is confirmed.

Information Commissioner's Office (ICO)

The UK regulatory authority overseeing data protection legislation and individual rights. Individuals may complain to the ICO if dissatisfied with the Trust's handling of an ATR/SAR.

Information Governance (IG) Team

The team responsible for receiving, logging, validating, coordinating and disclosing ATR/SAR requests, including advising on redaction, exemptions and secure transfer.

Lawful Extension

A permitted extension (up to two months) to the 30 calendar days statutory timeframe when ATR/SAR cases are complex or numerous.

Operational Routes (Route A / Route B)

Two approved Trust pathways for processing ATRs/SARs:

- Route A: IG Team retrieves, prepares and reviews records.
- Route B: Service teams retrieve and review records before passing them to IG.

Personal Data

Any information relating to a living individual who can be identified directly or indirectly.

Record Retrieval

The process of locating all information relevant to a request, including electronic and paper records, archived materials and scanned documents.

Redaction

The removal or obscuring of information that must not be disclosed (e.g., third-party data, harmful content, legally restricted information).

Request Validation

The stage where IG confirms the identity of the requester, determines the correct legal basis, clarifies scope and assigns a reference number.

Secure Disclosure

The safe and lawful transfer of information to a requester using approved methods such as encrypted email, secure portals or recorded delivery.

Senior Information Risk Owner (SIRO)

The executive lead responsible for overseeing information risk, compliance with rights of access, and liaison with the ICO.

Sensitive Information

Information requiring special protection due to its nature (e.g., clinical notes, safeguarding details, mental health content).

Statutory Timeframe

The legal period in which ATR/SAR requests must be completed — normally 30 calendar days, unless a lawful extension is applied.

Subject Access Request (SAR)

A request made by or on behalf of a living person to access their personal data under the UK GDPR and DPA 2018.

Subject Rights Request (SRR)

A broader term sometimes used to refer to any request made under individual data protection rights, including right of access.

Third-Party Information

Information that identifies or relates to someone other than the requester. This must not be disclosed without consent or lawful justification.

Validation

The formal process of confirming the legitimacy of the request, checking identity, ensuring authority, and establishing the legal framework that applies.