NHS Derby and Derbyshire Integrated Care Board

NHS Lincolnshire Integrated Care Board

NHS Nottingham and Nottinghamshire Integrated Care Board

Information Rights Policy

(including Subject Access Requests)

October 2026 – October 2029

Policy purpose
This policy sets out the shared approach for NHS Derby and Derbyshire Integrated Care Board, NHS Lincolnshire Integrated Care Board and NHS Nottingham and Nottinghamshire Integrated Care Board to recognise, manage and respond to information rights requests, including Subject Access Requests (SARs) and other rights available under data protection legislation. It supports compliance with UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025, the Access to Health Records Act 1990 and current Information Commissioner's Office guidance.

CONTROL RECORD	
Title	Information Rights Policy (including Subject Access Requests)
Reference number	DLN-IG-002
Version	1.1
Status	Final
Author	DDICB and NNICB Information Governance Teams
Sponsor	Director Corporate Governance and Assurance Director of Outcomes/Senior Information Risk Owner (SIRO)
Team	DLN Information Governance Team
Amendments	Addition of paragraph 6.78 (page 14) under the Access to Health Records Act 1990 (for deceased patient records)
Superseded documents	All predecessor NHS Derby and Derbyshire ICB, NHS Lincolnshire ICB and NHS Nottingham and Nottinghamshire ICB policies, procedures, guidance and local documentation relating to Subject Access Requests, information rights requests and associated information rights processes.
Audience	All staff working for, or on behalf of, NHS Derby and Derbyshire ICB, NHS Lincolnshire ICB and NHS Nottingham and Nottinghamshire ICB.
Consulted with	Data Protection and Security Steering Group
Equality Impact Assessment	September 2026
Approving body	Audit Committee
Date approved	8 October 2026
Date of issue	October 2026
Review date	October 2029 (or earlier if legislation, national guidance or organisational arrangements change)
Policy retention period	Life of organisations plus six years
This is a controlled document and whilst this policy may be printed, the electronic version available on the ICB's document management system is the only true copy. As a controlled document, this document should not be saved onto local or network drives.	

Contents

1. Introduction 4
2. Purpose 4
3. Scope 5
4. Definitions 5
5. Roles and responsibilities 5
6. Policy requirements 6
7. Equality and Diversity Statement 15
8. Communication, monitoring and review 15
9. Confidentiality 16
10. Staff training 16
11. Interaction with other policies 17
12. References 17
13. Equality Impact Assessment 18
Appendix A: Definitions and glossary of terms 21

1. Introduction

1.1 This policy applies to NHS Derby and Derbyshire Integrated Care Board, NHS Lincolnshire Integrated Care Board and NHS Nottingham and Nottinghamshire Integrated Care Board (collectively referred to as 'the ICBs').

1.2 The ICBs are public authorities and data controllers responsible for processing personal data in the delivery of their statutory functions, commissioning responsibilities, corporate activities and workforce management. The ICBs are committed to ensuring that personal data is processed lawfully, fairly, transparently and securely.

1.3 The UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 and associated data protection legislation provide individuals with a range of rights in relation to their personal data. These include the rights to be informed, access, rectification, erasure, restriction, portability, objection, and safeguards relating to automated decision-making and profiling.

1.4 This policy establishes a consistent approach across the Derbyshire, Lincolnshire and Nottinghamshire (DLN) ICBs for recognising, recording, validating, managing and responding to information rights requests, including Subject Access Requests (SARs) and other rights exercised under data protection legislation.

1.5 This policy should be read alongside the ICBs' wider information governance, data protection, records management, confidentiality and information security policies, together with any supporting procedures and guidance documents.

2. Purpose

2.1 This policy sets out the approach of the ICBs to managing information rights requests and complying with the requirements of the UK GDPR, Data Protection Act 2018 as amended by Data (Use and Access) Act 2025, Access to Health Records Act 1990 and relevant Information Commissioner's Office (ICO) guidance.

2.2 The policy aims to ensure that information rights requests are recognised, handled consistently, lawfully, securely and within statutory timescales across the ICBs.

2.3 It defines the responsibilities of staff and the Information Governance Team, supports proportionate searches and lawful disclosure, and establishes arrangements for quality assurance, monitoring, reporting and continuous improvement.

3. Scope

3.1 This policy applies to all individuals working for or on behalf of the ICBs who may receive, identify, manage or hold information relevant to an information rights request.

3.2 This policy applies to all personal data for which the ICBs are data controllers or joint controllers, regardless of format, including information held electronically, on paper or in other media.

3.3 This policy applies to information rights requests received verbally or in writing, including requests submitted by email, letter, telephone, online services or through an authorised representative.

3.4 Requests made under the Freedom of Information Act 2000 and Environmental Information Regulations 2004 are managed under separate arrangements. Where requests contain both personal data and other recorded information, advice should be sought from the Information Governance Team.

4. Definitions

4.1 Definitions of key terms referenced in this policy are described in Appendix A.

5. Roles and responsibilities

5.1 Key responsibilities for specific roles and staff groups are described below:

Role	Responsibilities
Chief Executive	Has overall accountability for ensuring the ICB complies with its statutory obligations relating to information rights and maintains effective governance arrangements.
Senior Information Risk Owner (SIRO) / Deputy SIRO	Provides executive and senior oversight and assurance regarding the effectiveness, capacity, risks and performance of information rights arrangements.
Data Protection Officer (DPO)	Provides independent advice and monitoring in relation to data protection legislation and information rights compliance, including complex requests, exemptions, complaints, incidents and emerging risks.
Caldicott Guardian	Provides advice on the use, disclosure and protection of confidential patient and service user information and supports decision-making in complex cases involving health or care records.
Information Governance Team	Acts as the central coordination point for information rights requests. The team validates requests, provides advice and guidance, coordinates activity, monitors statutory timescales, supports the application of exemptions and redactions,

Role	Responsibilities
	undertakes quality assurance, maintains records and issues responses on behalf of the ICB. Also responsible for maintaining this policy, supporting policy approval and review processes, ensuring publication and providing assurance regarding policy compliance
Information Asset Owners (IAOs)	Ensure information assets within their area of responsibility are appropriately managed, searchable and retained. Support searches, identify relevant information and provide assurance regarding the completeness of records returned.
Senior Managers (SLT) and Heads of Service	Ensure staff understand their responsibilities under this policy, support compliance within their service area, allocate resources to support requests and ensure complete and timely responses are provided.
Key service areas	Are responsible for identifying, retrieving, reviewing and providing all relevant information held within their service. This includes undertaking appropriate searches, reviewing records for relevance, confirming search methodologies and documenting any limitations. Services such as **Human Resources, Continuing Healthcare (CHC), Safeguarding, Complaints and Patient Experience, Primary Care,** and other operational teams are responsible for returning complete and accurate information within agreed timescales. The Information Governance Team provides coordination, advice and quality assurance but does not assume responsibility for identifying records held within service areas.
All staff	Must recognise information rights requests, forward them promptly to the Information Governance Team, preserve relevant records, cooperate with searches and reviews, and maintain confidentiality throughout the process.
Processors and third-party suppliers	Must assist the ICB in meeting its information rights obligations in accordance with contractual requirements, data processing agreements and documented instructions.
Joint controllers	Must maintain transparent arrangements setting out respective responsibilities for compliance with information rights legislation whilst ensuring individuals can effectively exercise their rights.

6. Policy requirements

6.1 The UK General Data Protection Regulation (UK GDPR) provides individuals with a number of rights in relation to their personal data. The ICBs are committed to supporting and facilitating these rights in accordance with applicable legislation, recognising that some rights are subject to specific

conditions, limitations and exemptions. The table below summarises the key information rights and the ICBs' policy position in relation to each.

Information right	Policy position
Right to be informed	The ICBs will provide clear, transparent and accessible information about how personal data is collected, used, shared, retained and protected through privacy notices and related information.
Right of access	Individuals have the right to obtain confirmation that their personal data is being processed and to receive a copy of that data and associated supplementary information, subject to applicable exemptions.
Right to rectification	Individuals may request correction of inaccurate personal data or completion of incomplete personal data. Requests will be assessed in accordance with applicable legal and professional requirements.
Right to erasure	Individuals may request erasure of personal data in certain circumstances. Requests will be assessed against applicable legal obligations, statutory duties and relevant exemptions.
Right to restrict processing	Individuals may request restriction of processing in specified circumstances. Requests will be considered and applied where the legal requirements are met.
Right to data portability	Where applicable, individuals may request personal data in a structured, commonly used and machine-readable format. This right applies only in circumstances prescribed by law.
Right to object	Individuals may object to the processing of their personal data in certain circumstances. Objections will be considered in accordance with the lawful basis for processing and applicable legal requirements.
Rights relating to automated decision-making and profiling	The ICBs will ensure that any automated decision-making or profiling involving personal data is lawful, transparent and subject to appropriate safeguards, including human review where required.

Recognising Information Rights Requests (including SARs)

6.2 Individuals have a range of rights under UK GDPR and the Data Protection Act 2018. Requests to exercise these rights do not need to refer to specific legislation or use terminology. Staff should consider the substance of a request and seek advice from the Information Governance Team where required.

6.3 Information rights requests may relate to an individual's right to access, rectify, erase, restrict processing of, object to the processing of, or obtain a copy of

their personal data, as well as rights relating to automated decision-making and profiling.

6.4 An information rights request does not need to refer to UK GDPR, the Data Protection Act 2018, or any specific information right, nor does it need to be submitted on a particular form. A request is valid where an individual is seeking to exercise one of their legal rights in relation to their personal data.

6.5 Information rights requests may be made verbally or in writing, including by email, letter, telephone, face-to-face contact, online services, social media or through an authorised representative acting on behalf of an individual.

6.6 All information rights requests must be forwarded to the Information Governance Team immediately upon receipt through the approved reporting route.

6.7 Where a request is received verbally, staff must record the date received, the requester's details, contact information and an accurate summary of the request, and provide this information to the Information Governance Team.

6.8 Staff must not require an individual to submit a request using a specific form or through a particular communication channel as a condition of recognising or accepting the request.

6.9 Staff must preserve any information relevant to a request and must not delete, amend or dispose of records that may be within scope of the request.

6.10 Staff must not respond substantively to information rights requests through social media or informal messaging platforms. Requests received through these channels must be preserved and referred securely to the Information Governance Team.

6.11 Where there is any uncertainty regarding the nature of a request or the information right being exercised, advice must be sought from the Information Governance Team without delay.

Logging, validation and time limits

6.12 The Information Governance Team will log all information rights requests, allocate a reference number, record the date of receipt, identify the applicable information right and determine the statutory response deadline.

6.13 Requests will be handled promptly, transparently and without undue delay in accordance with applicable legislative requirements and statutory timescales. Subject Access Requests and other information rights requests subject to UK GDPR timescales will be responded to within one calendar month of receipt, unless a lawful extension, suspension or other provision applies. Individuals will be kept informed where identity verification, clarification or other action is required to support the handling of their request.

6.14 Where reasonable doubt exists regarding an individual's identity or authority to act on behalf of another person, the Information Governance Team may request proportionate evidence before processing the request.

6.15 Where clarification is reasonably required to identify the information requested or the right being exercised, the Information Governance Team may seek further information from the requester. Clarification must not be requested unnecessarily or used to delay a response.

6.16 Where permitted by legislation, the response period may be extended where a request is complex or where an individual has made multiple requests. Any extension will be applied in accordance with legal requirements, and the requester will be informed of the reasons and revised timescales.

6.17 The Information Governance Team will maintain appropriate records of requests, correspondence, decisions, extensions, pauses and outcomes to demonstrate compliance with legislative requirements.

Identity, authority and requests made on behalf of others (including children)

6.18 Before disclosing personal data, the ICBs must be satisfied as to the identity of the requester and, where applicable, the authority of any individual acting on another person's behalf.

6.19 Any request for identification or evidence of authority must be reasonable, proportionate and limited to what is necessary to protect personal data from inappropriate disclosure.

6.20 Where a request is made by a solicitor, advocate, family member, carer or other representative, appropriate evidence of authority must be provided before information is disclosed. This may include written consent from the individual, parental responsibility, a Lasting Power of Attorney, Enduring Power of Attorney, Court of Protection Deputyship Order, court order or other lawful authority, as appropriate to the circumstances.

6.21 The ICBs will assess the scope, validity and relevance of any authority provided and will only disclose information where the representative is authorised to receive it. The type of authority required will depend on the nature of the request, the information requested and the individual's capacity.

6.22 Requests made on behalf of children must be assessed on a case-by-case basis. The ICBs will consider the child's age, maturity, competence, best interests, confidentiality expectations and any evidence of parental responsibility or other authority before deciding whether disclosure is appropriate.

6.23 Where a request relates to an individual who may lack capacity, the ICBs will apply the principles of the Mental Capacity Act 2005 and consider whether the representative has appropriate legal authority to act on the individual's behalf.

Searches and preservation

6.24 The ICBs will undertake reasonable and proportionate searches to identify information relevant to an information rights request. Search activity will be determined by the nature of the request and the locations where relevant information is reasonably likely to be held.

6.25 The ICBs are not required to search every system, mailbox, record set or repository in every case. Searches will be targeted and proportionate, taking account of the scope of the request, the information sought, the likelihood of relevant information being held and the resources required to undertake additional searches.

6.26 Information Asset Owners, senior managers, service leads and other staff must cooperate with search requests and provide complete and accurate information within the timescales specified by the Information Governance Team.

6.27 Service areas are responsible for undertaking appropriate searches of the records and systems they manage and for providing assurance that all reasonable and proportionate searches have been completed.

6.28 Search activity must be appropriately documented, including the systems searched, individuals consulted, search parameters used, information identified and any limitations or decisions regarding the scope of searches undertaken.

6.29 Where a request, complaint, internal review, legal proceedings, regulatory investigation or other exceptional circumstance indicates that additional or enhanced searches may be required, the ICBs may undertake further search activity where considered appropriate and proportionate.

6.30 Following receipt of an information rights request, relevant information must not be deleted, concealed, destroyed or altered except in accordance with applicable law, retention requirements and approved business processes. Where necessary, routine disposal activities must be suspended until the request has been concluded.

6.31 Where information previously held by the ICB has been lawfully destroyed in accordance with approved retention arrangements, the requester will be informed where appropriate.

6.32 Where the ICB does not hold information falling within the scope of a request, the requester will be informed accordingly. Where reasonable and appropriate, the ICB may provide advice or signposting to another organisation that is likely to hold the information.

Review, redaction and supplementary information

6.33 Personal data identified in response to a Subject Access Request (SAR) must be reviewed before disclosure to ensure the response is accurate, intelligible, relevant and lawful.

6.34 Information relating to third parties must be assessed to determine whether disclosure is appropriate, taking account of consent, any duty of confidentiality, the rights and freedoms of others, reasonableness of disclosure and the need for redaction or extraction.

6.35 Relevant exemptions and restrictions may be applied where permitted by law, including those relating to legal privilege, crime prevention and detection, confidential references, negotiations, management information, regulatory functions, health and social work information, and the rights of others.

6.36 Decisions to withhold information, apply an exemption, refuse a request or charge a fee must be documented.

6.37 Where a request is refused in whole or in part, the requester must be informed of the reason, their rights to complain to the ICBs and the ICO.

6.38 Information identified for disclosure must be reviewed for relevance, scope, accuracy, intelligibility, confidentiality, exemptions and third-party information. All redactions must be quality checked and applied in a manner that prevents recovery of withheld information.

6.39 SAR responses must include any required supplementary information, including the purposes of processing, categories of personal data, recipients, retention arrangements, individual rights, the right to complain to the ICO, the source of the data where applicable, and information about any relevant automated decision-making.

Third-party information and confidentiality

6.40 Information relating to another individual must be reviewed before disclosure. The ICBs will consider whether disclosure is lawful, fair and reasonable and may redact or withhold information where necessary to protect the rights and confidentiality of others.

6.41 The Common Law Duty of Confidentiality continues to apply where relevant, including after death. Confidential health and care information must be managed in accordance with the law, the Caldicott Principles and professional guidance.

Exemptions, restrictions and serious harm

6.42 Exemptions and restrictions must be considered on a case-by-case basis and must not be applied routinely or as blanket exclusions.

6.43 Where an exemption or restriction is applied, the ICBs must document the legal basis, the information affected, the rationale for the decision and whether partial disclosure is possible.

6.44 Relevant exemptions and restrictions may apply where permitted by law, including those relating to the rights of others, legal professional privilege, crime

and taxation, regulatory functions, confidential references, management information, negotiations, research, health, education and social work information.

6.45 Where disclosure of health, education or social work information may cause serious harm to the physical or mental health of any individual, advice must be obtained from an appropriate health or other relevant professional in accordance with the applicable legal provisions.

6.46 Complex or high-risk cases must be referred to the Data Protection Officer and, where appropriate, the Caldicott Guardian or legal adviser.

Manifestly unfounded or excessive requests and fees

6.47 The ICBs will normally respond to information rights requests free of charge. However, where permitted by legislation, the ICBs may refuse to act on a request, or charge a reasonable fee, if the request is manifestly unfounded or excessive.

6.48 The threshold for relying on these provisions is high. Each request must be assessed on its own merits and supported by clear evidence. Previous requests, persistent correspondence or challenging behaviour do not in themselves demonstrate that a request is manifestly unfounded or excessive.

6.49 Any decision to refuse a request, apply an exemption, or charge a fee must be documented, including the rationale, supporting evidence, fee calculation (where applicable) and approval obtained. Advice from the Data Protection Officer should be sought for complex, high-risk or disputed cases.

6.50 The requester must be informed of the decision, the reasons for it, and their rights to complain to the ICBs, and complain to the ICO within the applicable statutory timescale.

Refusal and partial refusal

6.51 The ICBs may refuse a request, or part of a request, only where permitted by applicable legislation and following appropriate review and authorisation.

6.52 Where a request is refused wholly or partly, the response must explain the decision to the extent legally possible and identify the information withheld, the legal basis for the refusal and, where appropriate, the reasons why the information cannot be disclosed.

6.53 The requester must be informed of their right to complain to the Information Commissioner's Office (ICO).

6.54 Any refusal or partial refusal must be documented.

Responding and secure disclosure

6.55 The ICBs will ensure that responses are clear, intelligible, accessible and written in plain language.

6.56 Information requested electronically will normally be provided in a commonly used electronic format unless an alternative format is requested and it is reasonable to provide it.

6.57 Personal data must be disclosed using secure and proportionate methods appropriate to the volume, sensitivity and nature of the information.

6.58 The ICBs will consider and, where reasonable, provide adjustments, alternative formats or communication support to enable individuals to exercise their information rights.

6.59 In accordance with the Equality Act 2010, the ICBs will consider and, where reasonable, provide adjustments, alternative formats, communication support or other assistance to enable individuals to exercise their information rights.

Data-protection complaints

6.60 In accordance with the Data Protection Act 2018 (as amended by the Data (Use and Access) Act 2025), the ICBs will maintain an accessible process for complaints relating to the processing of personal data or the handling of an information rights request.

6.61 The ICBs will acknowledge receipt of a data protection complaint as soon as possible and within 30 days of receipt.

6.62 The ICBs will, without undue delay, take appropriate steps to investigate and respond to the complaint, including making enquiries where necessary and keeping the complainant informed of progress.

6.63 The complainant will be informed of the outcome of the complaint without undue delay. The complainant will also be advised of their right to complain to the Information Commissioner's Office.

6.64 Findings, decisions, learning and improvement actions arising from complaints will be recorded and used to support service improvement and compliance monitoring.

6.65 Where practicable, complaints should be reviewed by a person who was not responsible for the original decision. Significant, complex or systemic concerns will be escalated to the Data Protection Officer, SIRO or appropriate governance forum.

Controllers, joint controllers and processors

6.66 Each ICB remains accountable for compliance with information rights obligations in relation to personal data for which it is the controller.

6.67 Joint controller arrangements must clearly define responsibilities for handling information rights requests, without affecting an individual's right to exercise their rights against any joint controller.

6.68 Processors and suppliers must support controllers in fulfilling their information rights obligations in accordance with contractual and legal requirements. Responsibility for compliance remains with the controller.

Rectification, erasure, restriction, objection and portability

6.69 Requests to exercise rights relating to rectification, erasure, restriction, objection or data portability will be assessed by the Information Governance Team in accordance with applicable legislation, taking account of the purpose of processing, lawful basis and any relevant exemptions or restrictions.

6.70 Where the accuracy of personal data is disputed, the ICBs will consider whether processing should be restricted while the matter is investigated, where the statutory conditions are met.

6.71 Professional opinions will not be amended solely because they are disputed. Where appropriate, additional information, annotations or statements of disagreement may be added to the record.

6.72 Where required by law, the ICBs will notify relevant recipients of any rectification, erasure or restriction of processing unless this is impossible or involves disproportionate effort.

Access to records of deceased individuals

6.73 Data protection legislation applies only to living individuals. Requests for access to the health records of a deceased person will be considered under the Access to Health Records Act 1990 where applicable.

6.74 Access may be granted to the deceased person's personal representative or to a person who may have a claim arising from the death, subject to verification of their identity, authority and eligibility.

6.75 Disclosure must be limited to information the applicant is entitled to receive and must take account of any applicable exemptions, third-party information, and the continuing Common Law Duty of Confidentiality.

6.76 The ICBs will consider any known wishes of the deceased, whether disclosure is lawful, fair and proportionate, and whether access may cause serious harm to the physical or mental health of any individual.

6.77 Requests will be managed in accordance with applicable legislation.

6.78 The response period is 21 calendar days where the application relates only to records made within the 40 days immediately preceding the date of the application. In all other cases, the response period is 40 calendar days.

7. Equality and Diversity Statement

7.1 The ICBs pay due regard to the requirements of the Public Sector Equality Duty (PSED) of the Equality Act 2010 in policy development and implementation, as commissioners and providers of services, as well as employers.

7.2 The ICBs are committed to ensuring that the way services are provided to the public and the experiences of staff does not discriminate against any individuals or groups based on their age, disability, gender identity (trans, non-binary) marriage or civil partnership status, pregnancy or maternity, race, religion or belief, gender or sexual orientation.

7.3 The ICBs are committed to ensuring that activities also consider the disadvantages that some people in the diverse population experience when accessing health services. Such disadvantaged groups include people experiencing economic and social deprivation, carers, refugees and asylum seekers, people who are homeless, workers in stigmatised occupations, people who are geographically isolated, Gypsies, Roma and Travellers.

7.4 To help ensure that these commitments are embedded in day-to-day working practices, an Equality Impact Assessment has been completed, and is included within this policy.

8. Communication, monitoring and review

8.1 This policy will be published on the ICBs' public websites and made available to staff through appropriate communication, training and awareness activities.

8.2 Managers will ensure that staff are aware of this policy and understand their responsibilities in relation to recognising and promptly referring information rights requests to the Information Governance Team.

8.3 Compliance with this policy will be monitored through the ICBs' Information Governance assurance arrangements. This will include oversight of information rights performance, statutory compliance, requests received, response times, complaints, incidents, risks, identified themes, lessons learned and improvement actions. Relevant information will be reported through the Information Governance Compliance Report to the Data Protection and Security Steering Group to provide assurance regarding compliance with legislative and organisational requirements.

8.4 Risks arising from information rights activities, non-compliance, complaints, incidents or emerging themes will be recorded and managed through the ICBs' IG Risk Log in accordance with the Risk Management Policy.

8.5 This policy will be reviewed every three years, or sooner where required by changes to legislation, regulatory guidance, NHS requirements, organisational arrangements or identified learning.

8.6 Any queries regarding this policy, or how it applies in practice, should be directed to the Information Governance Team.

9. Confidentiality

9.1 Information rights requests may involve confidential, sensitive or special category information. The ICBs will manage all information rights activities in accordance with applicable legislation, the Common Law Duty of Confidentiality, the Caldicott Principles and the ICBs' Information Governance framework.

9.2 Access to information rights records, correspondence, searches, disclosure material and decision records will be restricted to individuals with a legitimate business need to access the information.

9.3 Information rights information will be stored, processed, disclosed and retained securely in accordance with the ICBs' information governance policies, approved retention arrangements and the NHS Records Management Code of Practice.

9.4 Any actual or suspected loss, unauthorised disclosure, misdirection, failure to preserve information or breach of confidentiality arising from information rights activities must be reported and managed in accordance with the ICBs' incident management arrangements.

10. Staff training

10.1 The ICBs will ensure that staff receive appropriate information governance training and awareness to support compliance with this policy and applicable information rights legislation.

10.2 All staff must complete mandatory Data Security Awareness training in accordance with organisational requirements.

10.3 Additional information rights training, guidance or awareness activity may be provided where identified through the ICBs' IG Communication Plan and Training Needs Analysis (TNA).

10.4 The Information Governance Team will maintain awareness of relevant legislation, regulatory guidance and NHS requirements and will communicate significant changes where appropriate.

10.5 Compliance with mandatory training requirements and information governance awareness activities will be monitored through the ICBs' Data Protection and Security Steering Group.

11. Interaction with other policies

11.1 This policy should be read in conjunction with the ICBs' wider governance, information governance, records management, information security, risk management and complaint management policies, procedures and guidance.

12. References

12.1 This policy has been developed with reference to relevant legislation, regulatory requirements and guidance, including:

a) UK General Data Protection Regulation (UK GDPR)

b) Data Protection Act 2018

c) Data (Use and Access) Act 2025

d) Access to Health Records Act 1990

e) Freedom of Information Act 2000

f) Environmental Information Regulations 2004

g) Equality Act 2010

h) Mental Capacity Act 2005

i) Public Records Act 1958

j) Common Law Duty of Confidentiality

k) Information Commissioner's Office (ICO) guidance relating to information rights, subject access requests and data protection complaints

l) NHS England Records Management Code of Practice

m) NHS England Information Governance guidance

n) National Data Guardian's Caldicott Principles

12.2 The Information Governance Team will apply the most current version of applicable legislation, regulatory requirements and national guidance when managing information rights requests and complaints.

12.3 This reference list is not exhaustive and may be supplemented by additional legislation, case law, regulatory guidance or NHS requirements where relevant.

13. Equality Impact Assessment

Date of assessment:	**September 2026**			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Age[1]	No specific adverse impact identified at draft stage.	Requests can be made through multiple routes and responses can be adapted to individual needs.	None identified at draft stage.	Supports access to personal information for all age groups, with additional safeguards for children and young people where required.
Disability (Including: mental, physical, learning, intellectual and neurodivergent)[2]	Potential barriers may exist where requesters require accessible formats, communication support or reasonable adjustments.	Alternative formats, communication support and reasonable adjustments will be considered wherever possible.	Needs should be assessed on a case-by-case basis.	Promotes accessible communication and supports equitable access to information rights.
Gender (including trans, non-binary and gender reassignment)[3]	No specific adverse impact identified at draft stage.	The policy requires lawful, fair, confidential and consistent handling of all requests.	None identified at draft stage.	Supports transparent access to personal information and the exercise of information rights.

[1] A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).

[2] A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.

[3] The process of transitioning from one gender to another.

Date of assessment:	September 2026			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
Marriage and civil partnership[4]	No specific adverse impact identified at draft stage.	Requests are handled consistently regardless of marital or civil partnership status.	None identified at draft stage.	Supports fair access through a consistent process.
Pregnancy and maternity[5]	No specific adverse impact identified at draft stage.	Requests can be made through multiple routes and support provided where needed.	None identified at draft stage.	Supports equitable access to personal information and information rights.
Race[6]	Potential barriers may exist where English is not the requester's first language or where communication needs are not recognised.	Alternative formats and communication support will be considered wherever possible.	Needs should be assessed on a case-by-case basis.	Supports transparency and fair access to information rights.
Religion or belief[7]	No specific adverse impact identified at draft stage.	Requests are managed consistently and without	None identified at draft stage.	Supports fair and consistent access to information rights.

[4] Marriage is a union between a man and a woman or between a same-sex couple.

Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.

[5] Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth, and is linked to maternity leave in the employment context. In the non-work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.

[6] Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.

[7] Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.

Date of assessment:	September 2026			
For the policy, and its implementation, please answer the questions against each of the protected characteristic and inclusion health groups:	Has the risk of any potential adverse impact on people in this protected characteristic group been identified, such as barriers to access or inequality of opportunity?	If yes, are there any mechanisms already in place to mitigate the adverse impacts identified?	Are there any remaining adverse impacts that need to be addressed? If so, please state any mitigating actions planned.	Are there any positive impacts identified for people within this protected characteristic group? If yes, please briefly describe.
		regard to religion or belief.		
Sex[8]	No specific adverse impact identified at draft stage.	Requests are managed consistently in accordance with legislation and organisational procedures.	None identified at draft stage.	Supports equitable access to information rights and complaint processes.
Sexual orientation[9]	No specific adverse impact identified at draft stage.	Requests are handled confidentially and consistently.	None identified at draft stage.	Supports equitable access to personal information regardless of sexual orientation.
Carers[10]	Potential barriers may arise where carers act on behalf of individuals and authority or consent is unclear.	Representative requests are assessed proportionately and appropriate evidence of consent or authority obtained where required.	Staff guidance should support consistent handling of representative requests.	Supports the appropriate involvement of carers and representatives where authorised.

[8] A man or a woman.

[9] Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none. https://www.equalityhumanrights.com/en/equality-act/protected-characteristics

[10] Individuals within the ICB which may have carer responsibilities.

Appendix A: Definitions and glossary of terms

Definitions of key terms referenced in this policy are described in the table below:

Term	Definition
Access to Health Records Act 1990	Legislation providing rights of access to the health records of deceased individuals in specified circumstances.
Automated Decision Making	A decision made solely by automated means without meaningful human involvement that has legal or similarly significant effects on an individual.
Common Law Duty of Confidentiality	A legal duty requiring confidential information to be kept confidential unless there is a lawful basis or other justification for disclosure.
Controller	The person or organisation that determines the purposes and means of processing personal data.
Criminal Offence Data	Personal data relating to criminal convictions and offences or related security measures.
Data Protection Complaint	An expression of dissatisfaction about the processing of personal data or the handling of an information rights request.
Data Protection Officer (DPO)	The role responsible for advising on and monitoring compliance with data protection legislation.
Data Subject	An identified or identifiable living individual to whom personal data relates.
Information Rights Request	A request by or on behalf of an individual to exercise a right under data protection legislation, including the rights of access, rectification, erasure, restriction, portability, objection and rights related to automated decision making.
Joint Controllers	Two or more controllers that jointly determine the purposes and means of processing personal data.
Personal Data	Information relating to an identified or identifiable living individual.
Processor	A person or organisation that processes personal data on behalf of a controller.
Reasonable and Proportionate Search	A search involving reasonable efforts to locate requested personal data, taking account of the nature and scope of the request, the systems and locations likely to hold relevant information, the difficulty and cost of retrieval, and the fundamental nature of the right of access.
Special Category Data	Personal data receiving additional protection under UK GDPR, including data concerning health, genetic and biometric data used for identification, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and a person's sex life or sexual orientation.
Subject Access Request (SAR)	A request by or on behalf of an individual to access their personal data and applicable supplementary information.
UK GDPR	The UK General Data Protection Regulation.