NHS
Central East
Integrated Care Board

Access to Records Policy

(Subject access request, Access to Health Records, Medical reports and other types of personal information requests)

NHS
Central East
Integrated Care Board

Document Status:

This is a controlled document. Any printed or downloaded copies are not controlled. The version of this document published on the Central East Integrated Care Board website is the controlled copy www.centraleast.icb.nhs.uk

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.

Document Control

Document Owner	Associate Director of Data Security and Information Risk (& Data Protection Officer)
Document Author(s)	Data Security & IG Officer
Directorate	Strategy, Planning and Evaluation
Approved By	CE ICB Board
Date of Approval	1.4.2026
Date of Next Review	31.3.2028
Effective Date	1.4.2026

Version Control

Version	Date	Reviewer(s)	Revision Description
1.0	1.4.2026	ICB Board	Approved

Contents

1. Introduction

1.1 This policy sets out the principles and requirements for Access to Records within Central East Integrated Care Board. It aims to ensure a consistent and effective approach that supports the organisation's objectives, complies with statutory and regulatory requirements and promotes best practice.

1.2 The ICB has a duty to comply with the UK General Data Protection Regulation (UKGDPR) and the Data Protection Act 2018 (DPA 2018). They give individuals (data subjects) the right to request access to the information the ICB holds about them. This right is commonly known as a Subject Access Request (SAR).

1.3 The Access to Health Records Act 1990 (AHR Act 1990) grants rights to specified individuals to request information held by the ICB about a deceased individual.

1.4 Requests for information relating to personal data can fall under various different types depending on the requestor, type of information requested, and the status of the individuals identified within the information requested.

2. Purpose and Scope

2.1 The purpose of this policy is to:

- Define the steps that must be taken when receiving personal information requests.
- Set out clear guidelines for ICB staff in helping manage personal information requests and differentiate between different types of request.
- Ensure the ICB meets its obligations and legal compliance in relation to personal information requests, e.g. DSPT.

2.2 All personal data processed by the Integrated Care Board will be logged on the organisational information asset register, this is a requirement in UK GDPR, this covers all information classed as personal information under legislation and is not unique to medical or patient information.

All information processed, if meeting the criteria of personal, is covered by the right of access in legislation.

2.3 **Information covered by this policy**

Personal data is information that relates to an individual who can be identified either directly or indirectly and includes any expression of opinion about the individual and any

indication of the intentions of the information holder or any other person in respect of the individual.

It is the information/data that is assessed as identifiable and this does not exclusively apply to “medical/patient data/information” any person of whom data is held has rights to access including staff, visitors etc.

The organisation will be responsible for information, and therefore be required to provide under data subject access rights, that it creates or where created by another organisation that the ICB holds, as per any data sharing or processing agreement to which the ICB is a processor or joint controller.

All staff must ensure they do not download and store information from other organisational or national systems onto ICB systems including SharePoint/Teams (or NHS SharePoint/Teams) without permission from the system controller and an approved Data Protection Impact Assessment and Data Sharing/Processing agreement in place.

All staff must ensure that all data processed (created, stored, adapted, linked, shared, deleted, archived) is entered onto the ICB Information Asset Register and/or Information Sharing register. Staff must not download information/data on to personal devices; this includes NHS mail where only browser view must be used on personal device as per NHS England policy.

2.4 This policy applies to all NHS Central East ICB staff, Board members, and others whether permanent, temporary or contracted-in (either as an individual or through a third-party supplier).

3. Definitions

This section provides staff members with an explanation of terms used within this policy.

3.1 **Information Governance**

3.1.1 An umbrella term for a collection of distinct but overlapping disciplines. Information Governance is about the way in which the ICB handles its information, particularly personal data.

3.2 **Confidential Information**

3.2.1 Confidential information can be anything that relates to patients, staff or any other sensitive information (such as contracts and tenders, classified documents) held in any form (such as paper, electronic, microfilm, audio or video) howsoever stored (such as patient records, paper diaries, computer or on mobile devices such as laptops, tablets, smartphones) or even passed by word of mouth.

3.3 **Data Controller**

3.3.1 A Data Controller is the organisation that determines the use of personal data. They exercise the control over the purpose and means of processing.

3.3.2 The ICB is the Data Controller for the information it holds and is therefore responsible for compliance with data protection law and for ensuring organisations it shares information with or third parties who process information on its behalf have the appropriate technical and organisational measures in place to protect the information.

3.4 **Joint Data Controllers**

3.4.1 A joint Data Controller (also commonly described as Data Controller in common) will work together to determine the use and purpose of personal data and decide who will be take responsibility for each element of data protection law.

3.5 **Data Processor**

3.5.1 A Data Processor must act on the instruction from the Data Controller (including Joint Data Controllers). A Data Processor must be registered to process personal data with the Information Commissioner's Office (ICO) and be able to demonstrate that.

3.6 **Personal Data**

3.6.1 This means data which relate to a living individual who can be identified from those data and includes any expression of opinion about the individual. Typical examples of this type of data could include;

- Person's name, address, full postcode, date of birth.
- Email address and telephone numbers.
- Pictures, photographs, videos, audiotapes or other images of patients.
- NHS number or local unique identifiers, these are considered identifiable if the organisation holds the means to re-identify the person from this unique identifier.
- Any other data, or linked data, that may be used to identify a patient directly or indirectly. For example, rare diseases, drug treatments or statistical analyses which have very small numbers within a small population may allow individuals to be identified.

A **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3.7 **Special Category Data**

3.7.1 Data held about an individual which contains both personal and sensitive information. Under the UKGDPR the following types of information are deemed as special category:

- Race,
- Ethnic origin,
- Religious or other beliefs,
- Political opinions,
- Trade union membership,
- Genetics,
- Biometrics (where used for ID purposes),
- Physical or mental health,
- Sexual life, and
- Criminal proceedings or convictions.

3.8 Processing

3.8.1 Processing means obtaining, recording, holding the information or data or carrying out an operation on the information or data. An operation could include organising, adapting or altering the data. It also includes retrieving, consulting, linking to other data sources or using the information or data.

3.8.2 Disclosing the information or data by transmission or dissemination indicates processing as does alignment, combination, blocking, erasure, and destruction.

3.8.3 Viewing data on a computer screen is considered to be processing under the Data Protection Act (DPA) 2018 and the UKGDPR.

3.9 Pseudonymised and Anonymised Information

3.9.1 It is important that staff understand the difference between anonymised and pseudonymised information (see below for definitions) as the level of security and risk is different for each.

3.9.2 <u>Anonymised</u>

Definition - *"...information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable." - Recital 26, United Kingdom General Data Protection Regulations (UKGDPR)*

In simple terms, information is unrecognisable and cannot be re-identified by referring to or linking it with other information which is available or likely to be available.

Information can only be classed as anonymised if all of the following have been removed and cannot be reverted back to its original form:

- Name
- Address
- Full postal code
- NHS number
- Date of birth
- Local identifiers (such as an employee number or hospital number)
- Anything else that could identify a patient for example a photograph, x-ray or dental records

3.9.3 Pseudonymised

Definition - *"…the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." - Article 4, UKGDPR*

Pseudonymisation occurs when ALL identifiable e.g. name, address, NHS Number, Employee Number and any other unique identifier contributed to an individual has been replaced with alternative identifiers that bears no overt relationship to the true values which would identify an individual. Re-identification of data can only be achieved with knowledge of the de-identification key.

For example, in the situation where clinical trial data has had all identifiers removed, this can only be considered anonymised data if it is impossible to re-identify the trial subjects, even when cross referenced against supporting documentation.

Organisations frequently refer to personal data sets as having been 'anonymised' when, in fact, this is not the case. Staff must therefore ensure they consult

3.10 Data Protection Impact Assessments

Staff introducing changes must ensure that a Data Protection Impact Assessment is completed and approved before any changes are introduced especially where the processing of personal data is likely to result in a high risk to the rights and freedoms of individuals. A DPIA is an assessment of the impact of the envisaged processing operations on the protection of personal data'

3.11 Information Commissioner's Office (ICO)

The ICO is our regulator and issues guidance, help and support. They can also investigate us regarding complaints and incidents and can issue penalties. Further

information relating to the ICO can be below or via Information Commissioner's Office (ICO).

3.12 **Department of Health and Social Care (DHSC)**

The Department of Health and Social Care helps people to live more independent, healthier lives for longer. It leads, shapes and funds health and social care in England, making sure people have the support, care and treatment they need, with the compassion, respect and dignity they deserve.

3.13 **Care Quality Commission (CQC)**

The CQC are the independent regulator of health and social care in England. They monitor and inspect health and social care services to ensure they provide people with safe, effective, compassionate, high-quality care and encourage care services to improve.

3.14 **Table of Acronyms**

Term	Definition
FOIA	Freedom of Information Act 2000
FOI	Freedom of Information
UK GDPR	United Kingdom General Data Protection Regulation
DPA 2018	Data Protection Act 2018
EIR	Environmental Information Regulation 2004
AtHR	Access to Health Records
ICB	Integrated Care Board
CEICB	Central East Integrated Care Board
DP	Data Protection
IG	Information Governance
DPO	Data Protection Officer
SAR	Subject Access Request

4. Policy Statement

4.1 NHS Central East ICB is committed to ensuring a data subjects Right of Access is upheld by compliance with Article 15 of the UKGDPR and Schedule 2, 3 and 4 of the DPA 2018.

4.2 Individuals (data subjects) have the right to:

- Have access to a copy of the information an organisation holds about them, subject to certain safeguards.
- Be provided with a copy of the information held.
- Have the information explained if it is illegible or unintelligible.
- Be informed by any data controller whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller.

4.3 All staff are expected to adhere to the requirements set out in this policy.

5. Roles and Responsibilities

The following have specific responsibilities in relation to this policy:

5.1 **Data Protection Officer (and/or Deputy)**

5.1.1 The DPO is responsible for ensuring the ICB complies with the requirements of UKGDPR, DPA 2018 and AHR Act 1990. The DPO also acts as a contact point for data subjects and the supervisory authority (ICO).

5.2 **Caldicott Guardian (and/or Deputy)**

5.2.1 Acting as the “conscience” of the organisation, the Caldicott Guardian actively supports work to enable information sharing where is it appropriate to share and advises on options for lawful and ethical processing of information.

5.2.2 The Caldicott Guardian also has a strategic role, which involves representing and championing privacy and information sharing requirements at senior management level.

5.2.3 In addition, they are responsible for approving release of information requested as part of the subject access and access to health records process.

5.3 **Data Security & Information Governance Team**

5.3.1 The IG Team is responsible for overseeing the entire process, ensuring information requests are handled appropriately and efficiently, and are responded to within the statutory time period.

5.4 **All Staff Responsibilities**

- Be able to recognise a request when it is received.
- Store and manage information and ensure when leaving the organisation information is retained by the ICB and you no longer have access to it.
- All requests must be forwarded to the Information Governance Team at the time of receipt.
- If a request for searches from the Information Governance team is received, you must act upon it without delay and respond at least by the date given or if no date given within 5 working days.
- You are responsible for undertaking searches within all records you hold or have access to as per the detail in the criteria of the request, you must search for example.
- SharePoint, Teams (Office 365), Mail accounts, messaging (including apps in use and other apps), recordings made audio and video, paper/written records held such as notebooks and printed material.
- Although personal devices are not approved for business use in the ICB, however if you have used these, then these are covered under UK GDPR for searching for information requests and failure to do so may be a criminal offence.
- No information should be deleted after an information request has been made as this constitutes a criminal offence. It is recommended by the ICO to pause any destruction of data on receipt of a request, such as information reaching the end of its retention period. This is why no automated deletion of information should occur.

6. Processes and Procedures

Requests for Information relating to personal data can fall under various different types depending on the requestor, type of information requested, and the status of the individuals identified within the information requested.

An example of assessing how a request for information should be dealt with and which area of legislation it should fall within is shown in the flow chart in Appendix 3.

6.1 Subject Access Requests under UK GDPR and Data Protection Act 2018

6.1.1 The responsibility for oversight of a SAR rests with NHS Central East's Integrated Care Board's (ICB) Information Governance Lead with assistance from support staff and other ICB teams who have delegated authority to handle their own access to records requests.

6.1.2 There is no obligation upon a data subject to explain why they wish to access their own personal data.

6.1.3 All requests should be assessed as to the appropriate pathway to be used

6.1.4 Third Party Requests

Others can make legitimate requests on behalf of and for the individual (data subject), careful assessment should be made as to if the request is truly for the benefit and on behalf of the data subject and not a way for the requestor to obtain data about the data subject.

Where a third party has made a request stating it falls under the UK GDPR, Data Protection Act careful assessment should be undertaken to ensure the correct validity of the SAR is ensured.

6.1.5 An individual cannot be forced to make (or be forced to consent for others to make) a SAR and therefore many such requests would not fall within the legislative boundaries of a SAR.

6.1.6 It may also be the case that the individual may not realise the extent of information which will be released or is being requested by the individual nor can the ICB be assured of any signed agreements sent via the third party are valid.

6.1.7 If it does appear that the request is a valid SAR then the individual should be contacted for direct approval and confirmation of the request if appropriate.

6.1.8 If there is suspicion that a SAR has been forced on an individual, then this should be relayed to the requester clearly stating that; “The ICB does not consider this to be a valid subject access request as per the UK GDPR or Data Protection Act 2018 as this appears to be an enforced SAR and therefore breaches the Acts.”

6.1.9 Such requests apply to an employee’s recruitment by the requester; the person’s continued employment by person; or a contract for the provision of services to person and/or for the ICB to provide such records.

6.1.10 It may be that such a request can be made under and provision within a different piece of legislation such as the Medical Reports Act 1990.

6.1.11 It may also be the case that the requester has wrongly stated the request falls under UK GDPR when the request is relating to a deceased person, such requests may fall under Access to Health Records Act Requests or other types of requests.

6.1.12 Response time

Without undue delay at least within 1 calendar month from receipt, unless an extension has been applied. Only in specific circumstances when the request is excessive (i.e.,

requester has made more than one request) or its particularly complex the ICB can extend the one calendar month time allowed (for up to a further two calendar months).

However, the requester must be informed of the reasons for the extension within one calendar month from date the request was received.

6.2 Request under Access to Health Records (AtHR) Act 1990 (Deceased person)

6.2.1 Under this legislation a request can be made for access to health records relating to a deceased person specifically and only where there is a claim arising out of the patient's death.

6.2.2 Any person with a claim can make a request for such records however the Act provides limited scope of the information released.

6.2.3 The ICB will need to verify the validity of any claim and how that relates to the information within the records held. To do this the ICB can and should request the following information from the requester:

- NHS or ICB Patient number
- What claim is being made on the estate that requires such records?
- What specific information from the records is required for the claim?
- What specific date period is relevant to the information requested relating to the claim on the estate?
- Proof of executorship of requester and/or approval of executorship.
    - Where executorship is not held a letter of administration.
    - Where neither exist a detailed description of the claim and proof from either of the above.
    - Lasting Power of Attorney ceases to apply upon death of the donor
    - Next of Kin is not a legal standing in UK law and does not apply to this Act

6.2.4 Under Section 5(4) of the Act the ICB must only release information directly relating to and relevant to the claim and therefore the whole record is never likely to be subject to release.

6.2.5 The Common Law Duty of Confidentiality extends beyond death. Consideration must therefore be given to whether the data subject had requested confidentiality whilst alive. This is covered in Section 5 of the Act and if the patient had specifically stated an expectation information would not be released either to a specific individual or generally

by consent with exception of not being released the ICB has an exemption under the Act to refuse release of certain parts of the record.

6.2.6 The Act covers manual health records made since 1 November 1991. Access must also be given to information recorded before these dates if this is necessary to make any later part of the records intelligible.

6.2.7 Information relating to third parties within records should be assessed and redacted as per redaction section.

6.2.8 Not all requests for information relating to a deceased person will fall under the Act and therefore careful assessment of all requests for information should be undertaken to ensure correct pathway is followed.

6.2.9 Response time

1. Where the application relates to a record, or part of a record, none of which was made before the beginning of the period of 40 days immediately preceding the date of the application, the period of 21 days beginning with that date;

2. In any other case, the period of 40 days beginning with that date.

6.3 Request under Medical Report Act 1988

6.3.1 This relates to records requested for employment or insurance purposes and to a medical report based on records held by the ICB.

6.3.2 Requests for medical reports under this Act relies on consent of the person indicated in the report prior to the request being made. The ICB shall be notified by the requester and seek assurance prior to release that the individual has not requested access to the report prior to disclosure to the requester. If the ICB has supplied the report to the individual it must obtain permission to release the report to the requester.

6.3.3 The individual has a right to request amendments to the report and if the medical professional creating the report accepts the amendments the report will be amended, if the medical professional does not agree to the amendments, then the option to the individual will be made for a statement of the individual's view shall be attached to the report.

6.3.4 The above must be made in writing.

6.3.5 Medical reports must be retained for six months from date of which it was supplied/released.

6.3.6 A fee may be chargeable for requests to medical reports; however this is not currently in place within the ICB.

6.3.7 There are exemptions that can be considered in response to a request under this Act and should be reviewed upon receipt of a request, Section 7 of the Act.

6.3.8 All requests of this type MUST be handled through the Information Governance Department.

6.3.9 Response time

The medical report will be released to the requester not before 21 days has elapsed from the date of request where no notification has been received that the individual wishes to access the report before release.

If the individual has requested access to the report, the report will not be released until consent has been received from the individual in writing.

6.4 Request from Police

6.4.1 Law enforcement authorities can make requests for information under UK GDPR and the Data Protection Act 2018.

6.4.2 These requests must be made in writing using the National Police Chiefs' Council Request to external organisation for the disclosure of personal data to the Police.

6.4.3 As per NHS England policy this form MUST be counter signed by a rank of inspector level or above.

6.4.4 All requests of this type MUST be handled through the Information Governance Department.

6.4.5 Response time

No statutory period applies each request will be dealt with according to specific urgency.

6.5 Request from Court

6.5.1 Requests from the courts to provide information take the form of court order, witness summons and subpoena.

6.5.2 If a request is made in any other form stating it is a court order, then no information will be requested.

6.5.3 All official court order, witness summons and subpoena will be clearly marked, and the court can be contacted to confirm validity.

6.5.4 Court requests should be addressed to the correct organisation to be valid.

6.5.5 All requests of this type MUST be handled through the Information Governance Department.

6.5.6 Response time

As directed by the court.

6.6 Request from Coroner

6.6.1 A senior coroner can request information under Section 5 of the Coroners and Justice Act 2009.

6.6.2 As a coroner's inquest is a court of law then such requests may also fall under Court orders.

6.6.3 All requests of this type MUST be handled through the Information Governance Department.

6.6.4 Response time

As directed by the coroner/court.

6.7 Request from Regulatory Body

6.7.1 Regulatory bodies may have specific powers to request information from the ICB.

6.7.2 Each request will be assessed on a case-by-case basis.

6.7.3 All requests of this type MUST be handled through the Information Governance Department. Unless delegated to your department.

6.7.4 Response time

Dependant on request and legal obligations.

6.8 Request from Public Inquiry

6.8.1 There are two types of inquiry, Statutory and Non Statutory.

6.8.2 Statutory Inquiries have powers under the Inquiry Act 2005, and the terms of the inquiry will detail the obligations of organisations in releasing information.

6.8.3 Non-Statutory Inquiry, investigations and reviews relating to patient safety do not have the same powers however, health and care organisations must work with any investigation that is considering the safety of the care and support that the organisation has provided. This includes providing records and other information to allow the investigation to carry out its task.

6.8.4 All requests of this type MUST be handled through the Information Governance Department.

6.8.5 Caldicott Guardian and other senior ICB staff will be required to be part of the process for these types of requests.

6.8.6 Response time

Dependant on request and legal obligations.

6.9 Request from non-NHS organisation

6.9.1 Some organisations, including other government departments, may approach the ICB requesting details about individuals.

6.9.2 The ICB needs to take caution and assess if there is a legal basis for it to share information with such organisations not covered in this policy and the confidentiality of the individuals. It may be helpful to share but where no obligation or legal basis exists for the ICB to share the information it could result in a breach of data protection leaving the organisation open to civil and regulatory action.

6.9.3 All requests of this type MUST be handled through the Information Governance Department in association with the Caldicott Guardian.

6.10 Request from Other NHS Organisation

6.10.1 Where request for records relate to ongoing direct care of a patient or where immediate threat to life of a patient or others and safeguarding concerns exist, then there is an obligation for the ICB to assist with providing any information without delay.

6.10.2 Sharing under the above circumstances should be justifiable and the organisation will support staff when information is released for this purpose as per Caldicott Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality.

6.10.3 Staff do not need to inform Information Governance of such releases but must be documented, if they wish they may seek advice from: Information Governance, Data Protection Officer and/or the Caldicott Guardian.

6.10.4 If requests for information do not relate to direct care, then the ability to share information will be dependent on the project and reason for sharing. The ICB has a duty to maintain Common Law Duty of Confidentiality and act legally under UK GDPR and the Data Protection Act 2018. See DPIA policy.

6.10.5 All requests of this type MUST be handled through the Information Governance Department.

6.11 Requests from/for Minors

6.11.1 A child may make a Subject Access Request in relation to their own personal data as from the age of 13 they are normally considered competent enough to do so.

6.11.2 Those with parental responsibility for a child under 13 years may make an access request on their behalf but the information holder must consider whether it is in the best interests of the child to disclose information held.

6.11.3 Appropriate staff should be involved in assessing Fraser/Gillick competence of requestors under the age of 16.

6.12 Access Requests for those who lack capacity to consent

6.12.1 In certain circumstances a person acting as an advocate can seek access to personal information in so far as it is necessary or relevant to their role. This includes:

- Persons appointed by the Court of Protection.
- Persons holding a registered Lasting Power of Attorney (LPOA) for specified purposes*; NOTE: LPA Cease if the donor has capacity at the time of request or upon death of the donor.
- Persons appointed as Independent Mental Health Advocates under the Mental Capacity Act 2005.

**In the context of NHS Continuing Healthcare, where a health and welfare LPOA is not in place and the data subject is still alive but lacks capacity, it may well be in their best interests (under the Mental Capacity Act) for relevant information to be shared with a property and financial affairs deputy or attorney (or other third party who is acting as their advocate) This should not be all information held and the information released must only be necessary for the specific purpose of the request.*

6.12.2 There may be occasions when a family member or representative who does not fall under the remit of the above requests access to information the ICB holds and there may be circumstances where the request is appropriate.

6.12.3 Requests of this nature will be managed on a case-by-case basis applying the principles of the Mental Capacity Act (2005). Chapter 16 of the Mental Capacity Act (2005) Code of Practice provides further advice and guidance on this subject.

6.12.4 When applicable staff processing access to personal information requests should confirm validity of an attorney via the government process https://www.gov.uk/government/publications/search-public-guardian-registers.

6.13 Identification of requester

6.13.1 Applicants are required to provide proof of Identity, unless they are already known, in which case it is reasonable to process the request without. If there is any doubt about the identity of the person making the request you can ask for more information, however.

6.13.2 It is important that the ICB request information that is necessary to confirm who they are, as a rule the ICB should not be asking for any documentation not already in its possession to verify an individual, such as passport or driving licence.

6.13.3 Individuals must be notified as soon as possible that more information to confirm their identity is required before responding to their request; the period for responding to the request begins when the additional information is received.

6.13.4 The Information Commissioner's Office clearly expects a proportionate process in regard to requesting identification;

> *The key point is that you must be reasonable and proportionate about what you ask for. You should not request more information if the requester's identity is obvious to you. This is particularly the case when you have an ongoing relationship with the individual.*

6.14 Disclosing information safely

6.14.1 The ICB must take reasonable steps to ensure information released does not infringe on the rights of other individuals.

6.14.2 Where ICB/NHS staff detail is within the information to be release consideration should be taken. Where staff information is already known to the requester this should not be withheld or redacted, it may not be known to the person collating the response to the

request if the requester is in receipt of such information already and should adopt the basis of they would not hold unless it is obvious in the information under review.

6.14.3 Information released to the ICB by the requester should be released back to the requester without redaction, if the origin is clear to the person collating the request.

6.14.4 Where other third-party information is in the information considered for release, where possible, you should consider whether it is possible to comply with the request without disclosing information that identifies another individual.

6.14.5 If this is not possible, you do not have to comply with the request except where the other individual consents to the disclosure or it is reasonable to comply with the request without that individual's consent.

6.14.6 Where third party information can be redacted, this should be undertaken to meet the request.

6.14.7 Where the request contains the following types of information they may wholly or partially fall under exemptions:

Crime and taxation: general, Archiving in the public interest, Crime and taxation: risk assessment, Health, education and social work data, Legal professional privilege, Child abuse data, Functions designed to protect the public, Management information, Regulatory functions relating to legal services, the health service and children's services, Negotiations with the requester, Other regulatory functions, Confidential references, Judicial appointments, independence and proceedings, Exam scripts and exam marks, Research and statistics

6.14.8 If using an exemption advice must be obtained from the Data Protection Officer or deputy.

6.14.9 The requesters wishes should be considered in association with the method of release e.g. Post, Email, however the ICB should ensure that the method of communication is safe and secure.

6.14.10 The format of documents released should be in PDF format, for other types of information such as audio or video then the requester should be consulted as to their requirements.

6.14.11 Requester disabilities should be taken into account, where disclosed by the requester at the time of the request.

6.15 Redaction

6.15.1 Staff involved in dealing with releasing information should have undertaken training, if staff require training, then they should contact information governance team. Staff should read the ICO “How to disclose information safely” guide, available on the Information Governance Training and Information SharePoint Site or Directly on the ICO website.

6.15.2 Redaction must be carried out using a permanent approved redaction tool such as Adobe Acrobat Pro. If you require this software, it should be requested via IT and will be funded by your department budget code.

6.15.3 The person undertaking redaction should log the files and assessment of any redaction and reasoning for redactions so that should the requester challenge the ICB can reference the decisions made.

6.15.4 Two copies of the release should be stored, one with redactions and one without redactions.

6.15.5 Where documents are redacted, (and if you are using Adobe Acrobat redaction tool), each redaction reason should be identified within the redacted section by utilising Adobe Acrobat Redaction tool and selecting “use overlay text” within the properties toolbox and selecting the redaction code setting.

6.16 Exemptions

6.16.1 UK GDPR and Data Protection Act 2018 allow for certain information to be withheld or redacted from release.

6.16.2 Appendix 5 should be provided to requesters where redactions have been undertaken. Staff should consult with the Data Protection Officer and/or deputy regarding redactions.

6.16.3 This is to ensure consistency across the organisation is maintained for all releases of information.

6.17 Retention periods relating to information requests

6.17.1 All processing activity within the ICB must have associated retention periods linked to the information held for that processing activity. This enables the ICB to control the information it holds and ensures it meet the requirements set out in the UK GDPR and Data Protection Act 2018. Without set retention periods it is hard to justify not releasing information when requested.

6.17.2 Requests for access to information and the internal documentation related to requests, should be stored for six years after the date of final release.

6.17.3 The minimum period set out in NHS Records Management Code of Practice is three years where there has been no appeal and six years where there has been an appeal. As technical measures are not in place to separate these records robustly, it has been decided to retain all records for the six-year minimum period.

7. Statutory and National Guidance

Provide details of any statutory, national, or other relevant guidance that has been used to develop this document. Include NHS England guidance, legislation, and best practice standards.

7.1 This policy has been developed with reference to the following statutory and national guidance:

- United Kingdom General Data Protection Regulations (UKGDPR)
- Data Protection Act 2018 (DPA 2018)
- Access to Health Records Act (AtHR)1990
- Medical Report Act 1988
- Freedom of Information Act (FOIA)
- Environmental Information Regulations (EIR)

8. Stakeholder Engagement Record

8.1 The following stakeholders were engaged in the development of this policy:

Role/Group	**Date of Engagement**	**Summary of Feedback**
Joint IG Steering Group	16th March 2026	Changes made, ready for Board Approval.
CEICB Board	1st April 2026	TBC

Accessibility Statement

This policy is available in alternative formats upon request, including large print, Braille and translated versions, to ensure accessibility for all staff and stakeholders.

Implementation Plan

Development and Consultation: The following individuals were consulted and involved in the development of this document:

- Information Governance Team
- Joint IG Steering Group

Dissemination: Staff can access this document via the staff website and will be notified of new/revised version via the internal staff newsletter.

Training: The following training will be provided to make sure compliance with this document is understood:

- All new staff are required to attend a compulsory Induction Programme which incorporates Information Governance.
- In addition to this, all staff are required to complete and pass the NHS Data Security Awareness training on an annual basis.

Monitoring: Monitoring and compliance of this document will be carried out via:

- An assessment of compliance regarding information sharing is undertaken within the Data Security and Protection Toolkit, each year and audited by internal auditors.
- In addition, the ICBs Data Security & IG Team will undertake additional monitoring of compliance with this policy as a response to identification of any gaps or as a result of risks identified by incidents, external reviews or other sources of information and advice.

Review: The Document Owner will ensure this document is reviewed in accordance with the review date.

Equality, Diversity, and Privacy: See Appendices

Associated Documents: The following documents must be read in conjunction with this document:

- Information Sharing Policy
- Data Protection Policy
- Information Governance Framework Policy
- Records Management & Lifecycle Policy
- ICB Privacy Notice

NHS
Central East
Integrated Care Board

Appendix 1: Equality Impact Assessment

Please answer the questions against each of the protected characteristic and inclusion health groups. If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken. It is against the law to discriminate against someone because of these protected characteristics. For support and advice on undertaking EQIAs please contact: agcsu.equalities@nhs.net

Name of Policy:	Request for Information policy
Date of assessment:	February 2026
Screening undertaken by:	Data Security & IG Officer

Protected characteristic and inclusion health groups. **Find out more about the Equality Act 2010, which provides the legal framework to tackle disadvantage and discrimination:** **https://www.equalityhumanrights.com/en/equality-act/protected-characteristics**	**Could the policy create a disadvantage for some groups in application or access?** **(Give brief summary)**	**If Yes - are there any mechanisms already in place to mitigate the potential adverse impacts identified?** **If not, please detail additional actions that could help.** **If this is not possible, please explain why**
Age A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).	No	
Disability 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.	No	
Gender reassignment The process of transitioning from one gender to another.	No	

Marriage and civil partnership 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'.	No	
Pregnancy and maternity 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.	No	
Race 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.	No	
Religion or belief 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.	No	
Sex A man or a woman.	No	
Sexual orientation	No	

Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none.		
Carers Individuals within the ICB which may have carer responsibilities.	No	
Please summarise the improvements which this policy offers compared to the previous version or position.		
N/A		
Has potential disadvantage for some groups been identified which require mitigation?		
No – (If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken.)		

NHS
Central East
Integrated Care Board

Appendix 2: Data Protection Impact Assessment

Screening questions to determine if a full DPIA is required. Guidance on handling personal and sensitive data.

Data protection is the fair and proper use of information about people. Before completing this form, please refer to the Data Protection Impact Assessment (DPIA) Guidance in the Information Governance (IG) section on the staff Intranet or contact the Data Protection Officer for support via ***(insert email address once confirmed)***

A DPIA is a process to help you identify and minimise the data protection risks. You must do a DPIA for processing that is likely to result in a high risk to individuals. You can use our screening checklist below to help you decide when to do one. If you have answered 'Yes' to any of the 10 screening questions, you must then carry out a full DPIA using the Stage 2 form, which is also available on the Intranet in the IG section.

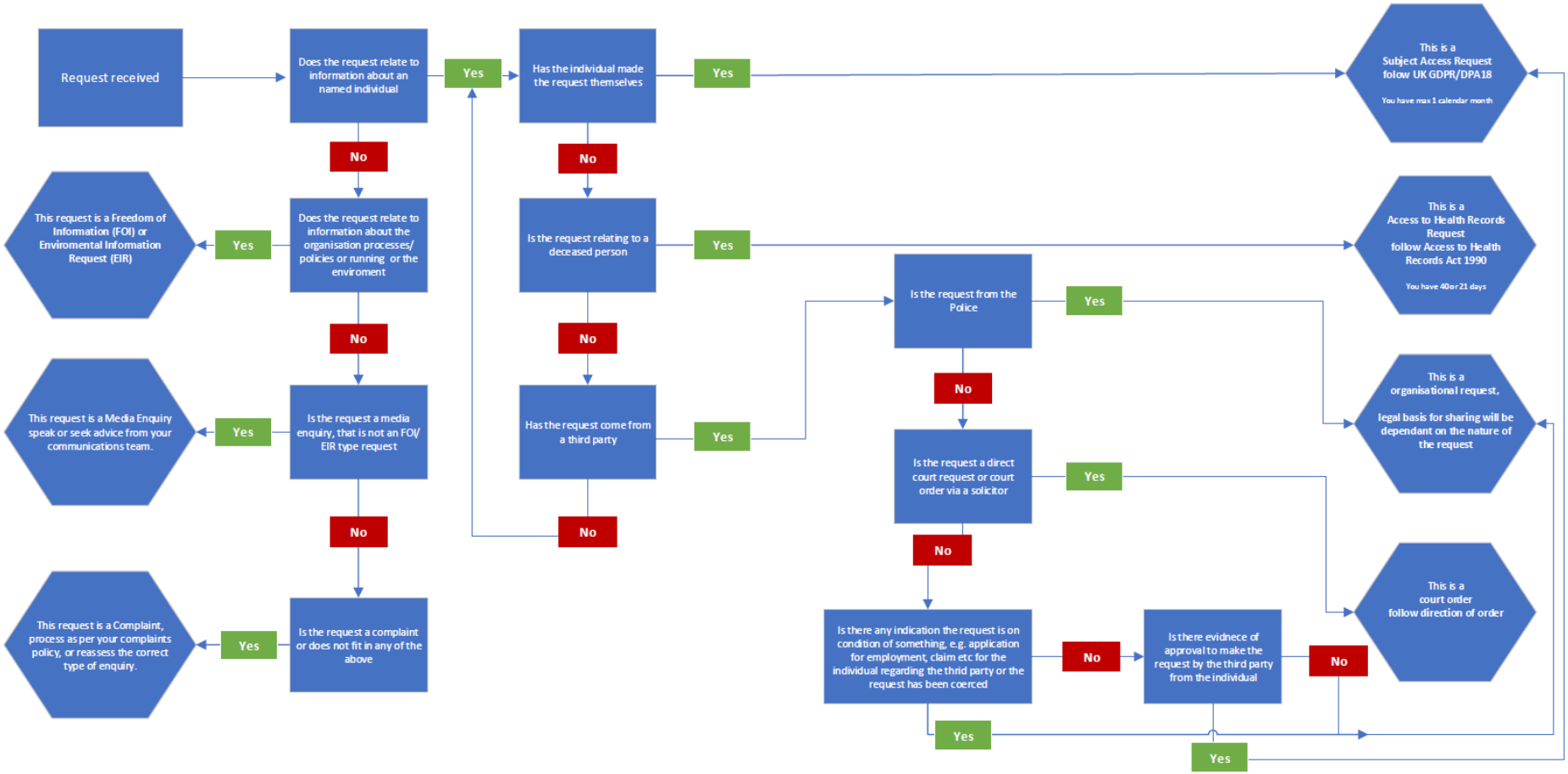
Name of Policy:	Request for Information policy
Date of assessment:	February 2026
Screening undertaken by:	Data Security & IG Officer

Stage 1 – DPIA form **please answer 'Yes' or 'No'**

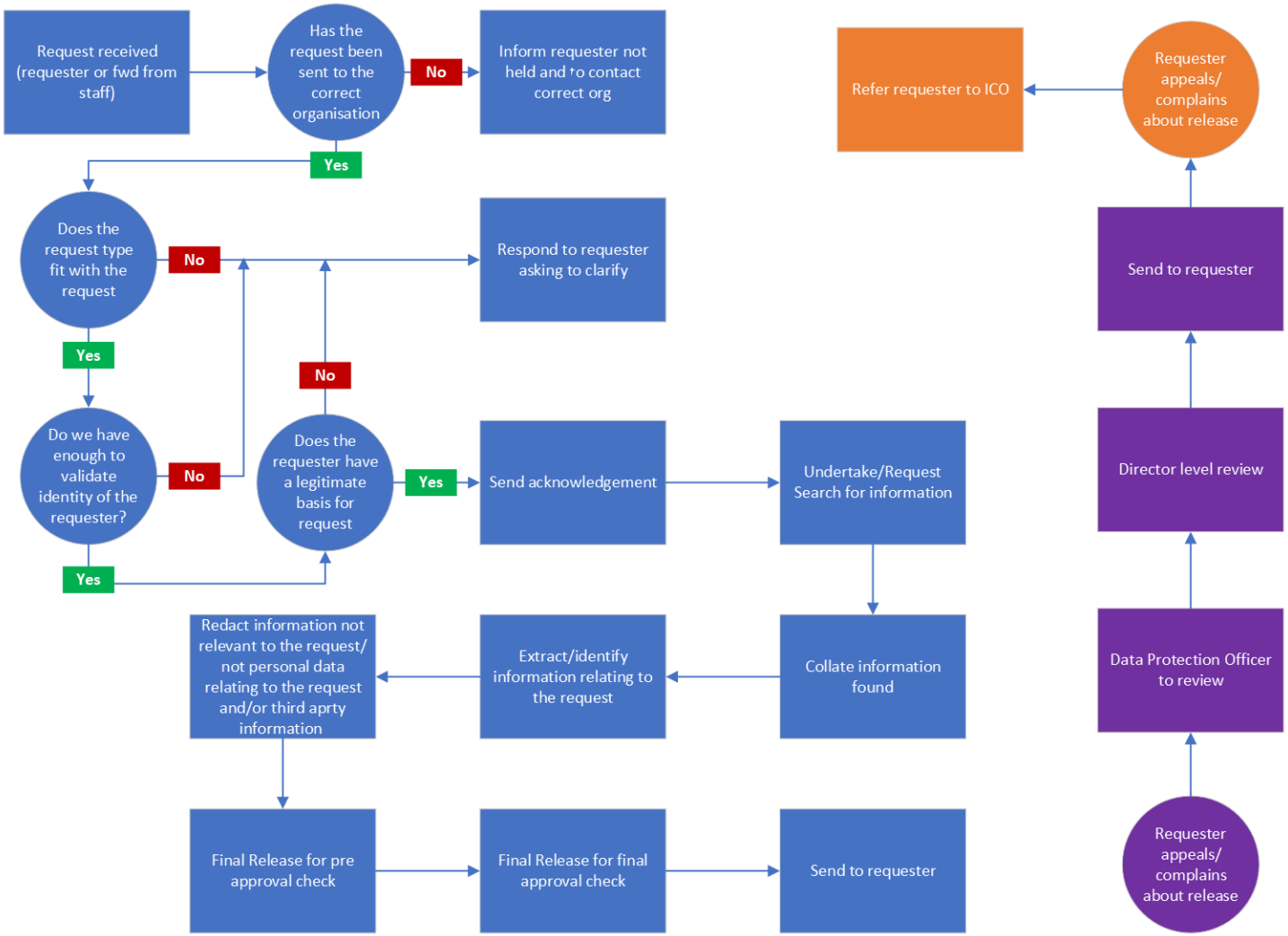
1. Will the policy result in the processing of personal identifiable information / data? This includes information about living or deceased individuals, including their name, address postcode, email address, telephone number, payroll number etc.	Yes
2. Will the policy result in the processing of sensitive information / data? This includes for living or deceased individuals, including their physical health, mental health, sexuality, sexual orientation, religious belief, National Insurance No., political interest etc.	Yes
3. Will the policy involve the sharing of identifiers which are unique to an individual or household? e.g., Hospital Number, NHS Number, National Insurance Number, Payroll Number etc.	Yes
4. Will the policy result in the processing of pseudonymised information by organisations who have the key / ability to reidentify the information? **Pseudonymised data -** where all identifiers have been removed and replaced with alternative identifiers that do not identify any individual. Re-identification can only be achieved with knowledge of the re-identification key. **Anonymised data -** data where all identifiers have been removed and data left does not identify any patients. Re-identification is remotely possible, but very unlikely.	No
5. Will the policy result in organisations or people having access to information they do not currently have access to?	Yes
6. Will the policy result in an organisation using information it already holds or has access to, but for a different purpose?	No

7.	**Does the policy result in the use of technology which might be perceived as being privacy intruding?** e.g., biometrics, facial recognition, CCTV, audio recording etc.	Yes
8.	**Will the policy result in decisions being made or action being taken against individuals in ways which could have a significant impact on them?** Including profiling and automated decision making. (This is automated processing of personal data to evaluate certain things about an individual i.e., diagnosis and then making a decision solely by automated means - without any human involvement)	No
9.	**Will the policy result in the collection of additional information about individuals in addition to what is already collected / held?**	Yes
10.	**Will the policy require individuals to be contacted in ways which they may not be aware of and may find intrusive?** e.g., personal email, text message etc.	No

Appendix 3: Request for Information flowchart



Appendix 4: Request for Information Internal Process



Appendix 5: Guide to redactions for requester

Under UK GDPR and Data Protection Act 2018 there are exemptions to data subject rights in relation to Article 15 Right of access by the data subject.

Within the document where information has been redacted an annotation will refer to this list to inform you of the reason for the redaction.

A. No personal information relating to request/data subject

i. Where content relates only to the business processes and does not include personal data
ii. Standard email head/footer content

B. Third party information: (DPA18- Sch2, Prt3, 16(1))

i. it would potentially disclose personal data of the requester to the third party that they were not already aware of
ii. it would be inappropriate for the third party to know that the requester has made a SAR.
iii. not staff member of organisation
iv. staff member not medical professional(admin)
v. Other type of individual

C. Health data- (DPA18- Sch3)

i. Serious Harm Test met (Prt2, 5(1))
ii. processed by court (Prt2, 3(1))
iii. Restriction of access- opinion of health professional not obtained (Prt2, 6(1))

D. Crime and taxation (DPA18- Sch2, Prt1, 2 (1))

E. Legal professional privilege (DPA18- Sch2, Prt4, 19)

F. Performance of tasks carried out by the Data Protection Officer (UK GDPR, Article 38(5)

These are some of the exemptions allowed by legislation and is not a definitive list.

Appendix 6: Response times and Extensions

Type of Request	Applicable legislation	Response time	Pause	Extensions
Freedom of Information (FOI) Request	Freedom of Information Act 2000 (FOIA)	Promptly and within **20 working days** from receipt of request.	Response time starts when all information to process the request has been received.	Where more time is required to determine whether the **balance of the public interest** lies in maintaining an exemption; or • further time to consider whether it would be in the public interest to confirm or deny whether the information is held is required. Time not specified but ICO recommends **no more than extra 20 working days.**
Environmental Information Regulation Request	Environmental Information Regulation (EIR)	**Within 20 working days** from receipt of request.	Response time starts when all information to process the request has been received.	Legislation has provision to extend the response time to 40 working days, but only for complex and voluminous requests.
Information Rights Requests including SARs	UK GDPR & Data Protection Act 2018 (DPA 2018)	Promptly and **within 1 calendar month** from date of receipt of the request; or within one month of receipt of any information requested to confirm the requester's identity.	Response time starts when ID has been received, however this should be requested promptly. Response time pauses where additional information is required.	Yes. By a further two months if the request is: complex; or you have received several requests from the individual – this can include other types of requests relating to individuals' rights. For example, if an individual has made a SAR, a request for erasure and a request for data portability simultaneously.
Access to Medical Records of deceased patients	Access to Health Records Act 1990 (AHRA)	If the records were updated during the 40 days before request, within 21 days. If the records were updated more than 40 days before the date of request, within 40 days.	More information must be requested within 14 days of request. Response time starts when necessary information is received.	