NHS
Central East
Integrated Care Board

Information Sharing Policy

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 Information Sharing within NHS Central East Integrated Care Board (ICB). 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 This document has been developed to aid staff with sharing information in line with the 7th Caldicott Principle "The duty to share information for individual care is as important as the duty to protect patient confidentiality" and the Information Commissioners Office (ICO) Data Sharing Code of Conduct.

1.3 This guidance is in relation to information sharing outside of the organisation and does not relate to the following requests:

- Requests for information under the Freedom of Information (FOI) Act 2000 - please refer to the ICB's FOI Policy.
- Subject Access Requests (also known as the Right of Access) or requests under the Access to Health Records (Deceased) Act – please refer to the ICB's Request for Information Policy.

2. Purpose and Scope

2.1.1 The purpose of this policy is to:

- To outline the principles of information sharing and the processes to be followed before sharing information.
- To ensure everyone working with information fully understands the importance of information sharing to support direct care, continuing health care, safeguarding adults and the protection of children.
- To ensure that only the minimum amount of information justified as necessary for the purpose is shared.
- To ensure that when information is shared it is done so lawfully and securely to ensure data subject's rights are respected and protected.
- To outline the importance and associated benefits of effective information sharing.

2.1.2 This policy applies to all NHS Central East ICB staff, Board members, contractors, and others involved in the sharing of pseudonymised and identifiable information held by the ICB about staff, patients and their families and the strict rules around the access, flow and sharing of information which the ICB holds and processes for the purposes outlined within the privacy notice via our website.

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 Anonymised

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.

4. Policy Statement

4.1 NHS Central East ICB is committed to ensuring all access and data flows of information in and out of the organisation meet the requirements set out in data protection law and NHS standards, including, but not limited to:

- Ensuring there is a legal basis for the ICB to share or receive the information.
- Ensuring that assurances are given when dealing with third party suppliers, contractors / service providers via contractual documentation.
- Using secure methods for the transfer of or access to information.

- Applying the UKGDPR requirement of Data Minimisation.
- Apply UKGDPR approved level of Pseudonymisation and Anonymisation when necessary.
- Applying National Data Opt-Outs requirements.
- Conducting a Data Protection Impact Assessment.
- Regularly reviewing Data Sharing Agreements (DSAs) which support the sharing of information.
- Regularly reviewing data processing agreements within contracts which supports the sharing of information for data processing via a supplier / service.
- Ensuring the sharing of information does not have a negative impact on the rights and freedoms of data subjects.

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

5. Roles and Responsibilities

5.1 The following have specific responsibilities in relation to this policy:

5.2 **ICB Board**

5.2.1 The Board is accountable for the effectiveness of the Information Governance Framework, the compliance to the relevant internal and external laws and regulations as part of the internal control system and for ensuring that the necessary support and resources are available for the effective implementation of the Data Protection Policy and this Information Governance (IG) Framework. It has responsibility for the IG agenda supported by identified senior roles which they are required to appoint including the Caldicott Guardian, Senior information Risk Owner and Data Protection Officer.

5.3 **Audit and Risk Committee**

5.3.1 The Audit and Risk Committee will receive regular IG Reports via the IG Group.

5.3.2 The Committee on behalf of the ICB, will have oversight on the assurance for the IG framework.

5.4 **Data Security & Information Governance (IG) Team**

5.4.1 The IG Team will receive and process all Data Protection Impact Assessments (DPIAs) and sharing agreements for approval by the Caldicott Guardian (sharing agreements) and by the DPO / SIRO for the DPIAs).

5.4.2 This department will also keep the information sharing and data protection impact assessments registers up to date and update the privacy notice as required.

5.5 **Head of Data Security & IG**

5.5.1 The Head of Data Security & IG is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG.

5.6 **Data Protection Officer (DPO)**

5.6.1 The DPO is to assist and monitor internal compliance, inform and advise on data protection obligations, provide advice regarding data protection impact assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority. This role should sign off any data flows.

5.7 **Senior Information Risk Owner (SIRO)**

5.7.1 This is an Executive Director who has overall responsibility for managing organisation information risk and ensuring appropriate assurance mechanisms exist. Any information related risks identified by IAOs should be entered onto the relevant departmental risk register to enable significant information risks to be reviewed by the SIRO and information governance group on a regular basis.

5.7.2 The SIRO is supported by the ICB's Caldicott Guardian, the Data Protection Officer and the IG Team.

5.8 **Caldicott Guardian**

5.8.1 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.

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

5.9 **Information Asset Owners (IAOs)**

5.9.1 An IAO is an individual within an organisation that has been given formal responsibility for the security of an asset (or assets) in their work area. They are responsible for the maintenance of the confidentiality of the data within that asset, ensuring that access to the asset is controlled and that the information is securely kept. They provide assurance that any risks to the data within the information asset are managed effectively. IAOs are directly accountable to the SIRO.

5.9.2 A central part of the IAO role is understanding what information is held, what is added and what is removed, how information is transferred, and who has access and why. That way you will understand what the risks are to your information assets and how these can be managed.

5.9.3 The IAO is responsible for protecting and preserving the confidentiality, integrity, authenticity, availability, and reliability of information contained within their information assets.

5.9.4 The IAOs are required to provide assurances that information is shared only amongst authorised persons or organisations and that the information is authentic, complete and accurate. They need to ensure that information is held and transferred securely. They also have to provide assurance that the systems responsible for delivering, storing and processing information are accessible when needed and by those who need them.

5.9.5 The IAOs are critical to ensuring information is appropriately handled. They are essentially the gatekeepers of information assets and in addition to the above are responsible for:

- Ensuring that a Data Protection Impact Assessment (DPIA) is completed for all new and amended 'information assets' which are information or which flow/support/enable the sharing of information.
- With the support of their Information Asset Administrators (IAAs) they are also responsible for ensuring their Information Asset Registers (IARs) are kept up to date on an ongoing basis with all new assets and flows added and assessed.

5.10 **Line Managers**

5.10.1 All line managers within the ICB are responsible for ensuring that their staff are aware of and comply with the ICB's IG policies and supporting standards and guidelines and for ensuring they are built into departmental processes and procedures.

5.11 **All Staff**

5.11.1 The majority of staff (including, but not limited to, permanent, temporary, contractors, volunteers) handle information in one form or another. All staff that in the course of their work create, use or otherwise process information have a duty to keep up to date with and adhere to the ICB's policies and national and local guidance on IG including information sharing.

5.11.2 There are very few departments within the ICB that process personal identifiable data about patients/service users, and these departments have processes and procedures in place to ensure that information is shared when it is lawful and appropriate to do so. However, these must remain in line with the principles and requirements of this policy and all other CEICB IG Policies.

5.11.3 Compliance with all CEICB policies, procedures, protocols, guidelines, guidance and standards is a condition of employment/contract. Breach of policy may result in disciplinary action or termination of service contract.

6. Processes and Procedures

6.1 The following processes must be followed to comply with this policy:

6.2 Information Sharing (starting the process)

6.2.1 Any information the ICB shares must be shared for a specified purpose e.g. to enable the ICB to meet a legal obligation, to safeguard or protect somebody, to meet the needs of a particular local or national sharing initiative, population health etc.

6.2.2 The frequency in which information is to be shared will vary between routine sharing, one off requests, individual requests, data access requests and requests for bulk data.

6.2.3 In all circumstances and regardless of the purpose for sharing information / providing access, the ICB must ensure the sharing of such information is lawful and in line with good practice. It is important therefore for staff who receive requests to share information or are involved in projects, initiatives or other pieces of work which involve sharing of information, to contact the Data Security & IG Team at the earliest opportunity with the following information:

- The purpose of sharing the information
- What information is to be shared e.g. identifiable, pseudonymised
- The method to be used to share/transfer the information
- How individuals will be informed about the sharing of their information e.g. information leaflet, already included in existing Fair Processing Notices, consent etc.
- Any background information e.g. links to national sharing initiative web pages, project background etc.

Staff providing this information might be asked to complete a DPIA.

6.2.4 Information sharing can be very complex, but the ICB's Data Security & IG Team will be able to assist you in identifying:

- If there is a legal basis for the ICB to share the information.
- If the method to be used to share/transfer the information is secure.
- If the UKGDPR requirement for Data Minimisation has been applied.
- If the UKGDPR Level of Pseudonymisation or Anonymisation has been applied.
- If National Data Opt-Out requirements have been met.
- If a Data Protection Impact Assessment is required.
- If a new Data Sharing Agreement (DSA) needs to be developed or if an existing ISA can be used.
- If the sharing meets the requirements of the GDPR & Caldicott Principles.

6.2.5 Adult Safeguarding, Child Protection, Complaints, Continuing Health Care, Medicine Management and Finance (as part of Invoice Validation and CHC/Individual Funding) share information on a daily basis. These departments are not required to contact the Data Security & IG Team every time they are asked to share information, as long as their

agreements, processes and procedures are up to date, in line with ICB Policies and are being complied with / by their staff. However, new information sharing arrangements must be assessed by the Data Security & IG Team.

6.3 Adult Safeguarding & Child Protection

6.3.1 Where there are concerns about a child, young person or adult who may be at risk of harm including, but not limited to, abuse or neglect, it is essential that these concerns are acted upon and information is given promptly to an appropriate person or statutory body, in order to prevent further harm occurring.

6.3.2 The best interests (safety & protection) of the child/children, young person(s) or adult(s) at risk must always guide decision-making.

6.4 Legal Basis to Share Information

6.4.1 Under UKGDPR and the Data Protection Act 2018, all organisations who process personal identifiable information, must not share the information they hold unless there is a legal basis which permits them to share it. These are listed in full in the ICB's Data Protection Policy.

6.4.2 In most cases ICB's lawful basis for processing and sharing information will be detailed within the privacy notice, which can be found on the ICB website. Further detail in relation to the legal basis to share information, can be found within the ICB Data Protection Policy.

6.4.3 Failure to share information in health and social care can be a breach of the Caldicott Principles, specifically Principle 7, which states that the duty to share information can be as important as the duty to protect patient confidentiality. Further details on the Caldicott Principles can be found within the ICB Data Protection Policy.

6.5 Secure Transfer/Flow of Information

6.5.1 Any information sharing method used to transfer information from ICB to another organisation MUST be in line with national and local IG standards as detailed in the ICB's policies.

6.5.2 Encryption is a standard requirement for all methods e.g. email, disc, system to system etc.

6.5.3 Sharing of information via email but be in line with email guidance within the ICB's policies available on the ICB Intranet.

6.6 Data Minimisation

6.6.1 Data protection legislation and national guidance require that when sharing information the amount of person-identifiable data should be limited to what is necessary to achieve the intended purpose. Excessive or irrelevant data should not be included.

6.6.2 Anonymised information should be used instead of identifiable information where it is sufficient to meet the purpose.

6.7 Anonymised or Pseudonymised

6.7.1 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 e.g.:

- UKGDPR does not apply to completely anonymised data (this is why anonymised information should always be considered over identifiable or pseudonymised information).
- Pseudonymised data falls fully within the scope of GDPR and must be treated with the same level of consideration as identifiable information in terms of security and processing. Pseudonymisation is effectively only a security measure. It does not change the status of the data as personal data.

6.7.2 Anonymised

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, GDPR*

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 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

6.7.3 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, GDPR*

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.

6.8 National Data Opt-out

6.8.1 The national data opt-out was introduced on 25 May 2018, enabling patients to opt out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

6.8.2 When a patient has set a national data opt-out, the ICB must make sure the patient's opt-out choice is respected.

6.8.3 Prior to releasing any information to ICB's (via Data Services for Commissioners Regional Office (DSCRO), NHS England removes Information about any individual who has opted-out as part of the National Data Opt-Out Rule.

6.9 Data Protection Impact Assessment (DPIA)

6.9.1 Before information can be shared a Data Protection Impact Assessment (DPIA) may be required. This includes (but is not limited to) where information is to be shared through

access to an IT system or use of an online system/portal. A DPIA must always be conducted for any new or change in process regarding personal data.

6.9.2 A DPIA will help to:

- Identify risks to the rights of data subjects
- Ensure person identifiable data is being processed securely and lawfully
- Identify risks and agree appropriate mitigation
- Identify all Information Assets and corresponding data flows
- Protect the ICB's reputation

6.9.3 A DPIA may not be required for one off information sharing requests e.g., a request from the Police regarding the whereabouts of an individual, request for information from the NHS Fraud Team etc. However, you must record what information was shared, with whom it was shared with, the legal basis and the method used to share or if you refuse to share the information, the rational for this.

6.10 Data Sharing Agreements

6.10.1 An Data Sharing Agreement (DSA), is an agreement between two or more organisations who have agreed to share information on a large scale or on a regular basis and sets out key elements e.g. the purpose for sharing the information, the method/s to be used for flowing the information, the legal bases, how data subjects' rights are going to be met etc.

6.10.2 An DSA should not be confused with a Data Processing Agreement (DPA) which is used to underpin a contract or Service Level Agreement (SLA) with a third-party data processor to detail the ICB's expectation e.g., how the information should be processed, how long it should be processed for, security arrangements, what should happen with the information at the end of the contract/SLA etc.

6.10.3 ICB staff who are approached by another organisation to sign an DSA must send it to the Data Security & IG Team who will assess the contents, identify if an existing agreement e.g. ICB DSA (see below) is sufficient for the purpose, identify if a DPIA is required or has been conducted and will arrange for the agreement to be approved (where necessary) by the ICB's Caldicott Guardian.

6.10.4 If the ICB has instigated the sharing then an DSA should be developed by the ICB – please contact the Data Security & IG Team for assistance with this.

6.11 Information Sharing for Secondary Uses

6.11.1 When a patient or service user is treated or cared for, information is collected which supports their treatment. This information is also useful to commissioners and providers of NHS-funded care for 'secondary' purposes - purposes other than direct or 'primary' clinical care - such as:

- healthcare planning
- commissioning of services

6.11.2 The ICB may receive requests for information where the information is going to be used for non-direct care; this is classed as ‘secondary use’, which fall into three broad categories:

- Use within the NHS for administration, planning, auditing, commissioning and payment by results (PbR).
- Use by agencies commissioned by the NHS to carry out such roles on its behalf.
- Use where identifiable information goes beyond health care provision in the NHS to include research and education.

6.11.3 Patient data may be shared and used for secondary purposes only when one or more of the following applies:

- The information has been effectively anonymised or pseudonymised and cannot be reversed
- The information is required by law
- The patient has given their explicit consent to the disclosure
- Disclosure is authorised by the Health Research Authority's Confidentiality Advisory Group for information sharing without consent under section 251 of the NHS Act.
- The ICB is satisfied that the legal and professional criteria for disclosure without consent in the ‘public interest’ have been met and has sought advice from the Caldicott Guardian.

6.11.4 If the information to be shared is information which has been obtained from NHS England (NHSE) as part of the Data Access Request Service (DSFC – see below), you must NOT share the information without prior approval from the DPO who may need to consult with NHS E.

6.12 Data Sharing Framework Contract and Agreement with NHSE

6.12.1 ICB as commissioners need information about the treatment of patients to review and plan current and future healthcare services. However, the law says commissioners are not allowed to access personal identifiable information because they are not providing direct patient care.

6.12.2 Section 251 of the Health and Social Care Act (2012) enables NHSE, to collect, analyse and disseminate patient level data to commissioners via an intermediary service called a DSCRO.

6.12.3 DSCROs specialise in processing, analysing and packaging patient information within a Secure environment into a format ICB's can legally use, anonymised patient level data. Anonymised patient level data allows a patient's 'events' to be linked without revealing the identity of that person.

6.12.4 Prior to flowing information to DSCROs, NHSE removes patients who have registered to opt-out as part of the national data opt-out program.

6.12.5 The ICB has a formal Data Sharing Framework Contract and Data Sharing Agreement in place with NHSE which enables the flow of information from the DSCRO to ICB's Commissioning Support Units (CSUs).

6.12.6 The information provided by NHSE is **strictly** for the purpose of:

- **Risk stratification**: a process that uses personal data from healthcare services to identify and support patients with long term conditions and to help minimise unplanned hospital admissions.
- **Invoice validation:** a process that uses personal data to make sure organisations providing care are paid correctly.
- **Commissioning** a process using data coded to hide the identity of patients. It is used by organisations to plan and commission healthcare services. This also includes Population Health Management.

6.12.7 The flow of information from NHSE is documented in the ICB's Privacy Notice.

6.12.8 The ICB cannot use data processors, flow data or use data for any purpose which is not documented in the formal Data Sharing Framework Contract (DSFC) and Data Sharing Agreement (DSA) it has in place with NHSE.

6.12.9 Any changes to the data processors used, the flow of data or to the uses/purposes of the data will require the ICB DPO, to submit a further application to NHSE via their Data Access Request Service (DARS) process.

6.12.10 In addition to the above, the ICB also has agreements in place for the flow of anonymised information from local providers e.g. acute Trusts, community services etc. This information flows directly from the provider organisation to the CSU.

6.13 Sub licensees

6.13.1 NHS E allows the ICB to share pseudonymised patient level data or aggregated data with our organisations that are part of the ICB's Integrated Care System and are one of the following organisation types:

- Local Authority
- NHS Trust
- GP
- Other Health Care Provider.

6.13.2 The purpose will be restricted to commissioning as per DSA. The sub-licensees must keep the pseudonymised data separate from other identifiable data they hold.

6.14 Information sharing with police

6.14.1 The police may ask health and care organisations to provide information about patients/service users to support their work. There are times when this information:

- must be provided to the police because law requires it, for example, information relating to a road traffic accident. You will usually be told of this type of sharing although this will not always be the case
- may be provided to the police because a sufficiently important reason has been given by the police. An example is in relation to the prevention or detection of a serious crime e.g. an assault where the victim has suffered serious harm.

6.14.2 There are times when it is not appropriate to inform or ask the data subject (patient/ service user / staff member) about the sharing. Examples of this would include where doing so would undermine a police investigation or put you or another person at risk of serious harm. Each request is considered carefully on a case-by-case basis.

6.14.3 Where a decision is made to share information with the police, health and care organisations will only share the minimum amount of information they require to investigate or prevent crime.

6.14.4 If you are a staff member responsible for responding to the police or deciding about sharing information, it is important that you are prepared in advance for any request.

6.14.5 You should remember the following in relation to any request for information from the police:

- Ask the police to provide further information, if required, to assist you in ensuring any disclosure you make is necessary and proportionate. For example, helping you identify the correct person from your organisation's records/sharing details of the incident to help establish whether there is a public interest justification for disclosing personal or confidential patient information.
- Consider if it is appropriate to seek explicit consent from the individual before disclosing information to the police e.g. seeking consent would not put the patient or another person at risk of serious harm, or undermine a police investigation by allowing a suspect to abscond.
- Only provide information that is necessary/relevant for the specific enquiry. For example, if the police want inpatient dates, only provide inpatient dates once you are satisfied with the validity of the request.
- Document what was requested, by whom, what was given and obtain a signature from the requester. This can be documented in the health and care record or a log or register of disclosures.
- Where time permits or you are not sure what to do, you should seek advice, for example, from a Caldicott Guardian, IG lead, or DPO.

6.14.6 When deciding whether to disclose information, there are several things to consider:

- if there is a legal duty to disclose
- whether the public interest served by disclosure outweighs the public interest served by protecting the confidentiality of the individual and the public interest served by providing a confidential service to the wider public
- whether it is necessary to disclose personal or confidential patient information.
- the minimum amount of data you need to share to support the police in their work.

7. Statutory and National Guidance

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

- UK GDPR
- Data Protection Act 2018
- Health and Social Care Act (2012)
- Caldicott Principles
- Common Law Duty of Confidentiality
- Information Commissioners Data Sharing Code of Conduct

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 ICB's 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:

- Data Protection Policy
- Information Governance Framework Policy
- Access to Records 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:	Information Sharing 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	No	

gender to another.		
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:	Information Sharing 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.	Yes
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.	No
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?**	No
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