NHS
Cheshire and Merseyside

Information Governance, Data Security and Protection Policies

NHS CHESHIRE AND MERSEYSIDE ICB

Contents

Consultation and Ratification Schedule

Document Name:	Information Governance, Data Security and Protection Policies
Policy Number/Version:	2.4
Name of originator/author:	NHS Cheshire and Merseyside ICB
Ratified by:	Integrated Care Board
Name of responsible committee:	Audit Committee
Date issued:	March 2025
Review date:	October 2026
Date of first issue:	October 2022
Target audience:	All staff, including temporary staff and contractors, working for or on behalf of: NHS Cheshire and Merseyside ICB
Purpose:	To set out the policy for Information Governance. To detail all staff responsibilities for Information Governance and the possible consequences of not following the guidance.
Action required:	For all staff to read and follow.
Cross Reference:	Information Governance Handbook Information Governance Staff Code of Conduct
Contact Details (for further information)	C&M ICB Information Governance Service a service provided by Mersey Internal Audit Agency (MIAA) infogov.cmicb@miaa.nhs.uk

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on NHS Cheshire and Merseyside ICBs internet site is the controlled copy. Any printed copies of this document are not controlled.

As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the internet.

Policy Review

This policy, including the policies with in, will be reviewed in two years or earlier if required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance.

Version Control

Policy Name: Information Governance, Data Security and Protection Policies					
Version	**Valid From**	**Valid To**	**Author**	**Changes**	**Approving group**
1.0	Sep 2022	Sep 2024	MLCSU IG Team	First release of document for ICB	Audit Committee
1.1 & 1.2	May 2023	Sep 2024	CAFG Team & MLCSU IG Team	Additions relating to data quality, contacts and IG framework updated.	Minor changes agreed at Information Governance Management Group 19/5/23 and version 2.0 produced. Audit Committee updated.
2.0	Jan 2024	Sep 2024	MLCSU IG Team	NHSE guidance on Disposal and Destruction of records	

2.1	Jul 2024	Sep 2024	CAFG Team	Change of IG provider	Minor change agreed by Associate Director - CAFG
2.2	October 2024	October 2026	MIAA IG Service	Full review and updates	Information Governance Group 23/10/24
2.3	November 2024	December 2026	MIAA IG Service	Added roles to support SIRO and Caldicott Guardian	Audit Committee 03/12/24
2.4	March 2025	December 2026	MIAA IG Service	Incorporated: Appropriate Policy Document for Processing Special Category Data and Criminal Offence Data for Safeguarding Purposes	Audit Committee 04/03/25

Glossary of Terms

Term	Acronym	Definition
Anonymisation	-	It is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.
Business Continuity Plans	BCP	Documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organisation to continue to deliver

		its critical activities at an acceptable defined level.
Caldicott Guardian	CG	A senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.
CareCERT	-	NHS Digital has developed a Care Computer Emergency Response Team (**CareCERT**). CareCERT will offer advice and guidance to support health and social care organisations to respond effectively and safely to cyber security threats.
Care Quality Commission	CQC	This is an organisation funded by the Government to check all hospitals in England to make sure they are meeting government standards and to share their findings with the public.
Code of Conduct	CoC	A set of rules to guide behaviour and decisions in a specified situation
Common Law	-	The law derived from decisions of the courts, rather than Acts of Parliament or other legislation.
Continuing Healthcare	CHC	CHC is health care provided over an extended period for people with long-term needs or disability / people's care needs after hospital treatment has finished
Data Controller	DC	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	DP	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Data Processing Agreement	DPA	The Data Controller has a legal responsibility to ensure that anyone they ask to process personal information on their behalf understands what their role is and what processing they can do. The controller is responsible for assessing that its processor is competent to process personal data in line with the UK GDPR's requirements. This assessment should take into account the nature of the processing and the risks to the data subjects. This is because Article 28(1) says a controller must only use a processor that can provide "sufficient guarantees" (in particular in terms of its expert knowledge, resources and reliability) to implement appropriate technical and organisational measures to ensure the processing complies with the UK GDPR and protects the rights of individuals.
Data Protection Act 2018	DPA18	Act replaced DPA 1998.
Data Protection Impact Assessment	DPIA	A method of identifying and addressing privacy risks in compliance with UK GDPR requirements.
Data Protection Officer	DPO	A role with responsible for enabling compliance with data protection legislation and playing a key role in fostering a data protection culture and helps implement essential elements of data protection legislation
Data Security and Protection Toolkit	DSPT	The DSPT is the standard for cyber and data security for healthcare organisations. Organisations measure performance against the NHS England standards.
Data Sharing Agreement	DSA	An Agreement outlining the information that parties agree to share and the terms under which the sharing will take place.

Data Subject	-	An identified or identifiable natural person who can be identified by their personal information
Freedom of Information Act 2000	FOI Act	The Freedom of Information Act 2000 provides public access to information held by public authorities
Individual Funding Requests	IFR	Application to fund treatment or service not routinely offered by NHS
Information Asset	IA	Includes operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications
Information Asset Administrator	IAA	The role of Information Asset Administrator is to ensure that policies and procedures are followed within their area, recognise actual or potential security incidents, consult with their IAO on incident management and ensure that information assets registers are accurate and up to date.
Information Asset Owner	IAO	Information Asset Owners are directly accountable to the SIRO and must provide assurance that information risk is being managed effectively in respect of the information assets that they 'own'.
Information Commissioner's Office	ICO	The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Information Governance Service	IG Service	The C&M ICB Information Governance Service is a service provided by Mersey Internal Audit Agency (MIAA)
Integrated Care Board	ICB	A statutory NHS organisation responsible for developing a plan for meeting the health needs of the population, managing the NHS budget and arranging for the provision of health services in the ICS area

Integrated Care Partnership	ICP	A statutory committee jointly formed between the NHS Integrated Care Board and all upper-tier local authorities that fall within the ICS area. The ICP will bring together a broad alliance of partners concerned with improving the care, health and wellbeing of the population, with membership determined locally. The ICP is responsible for producing an integrated care strategy on how to meet the health and wellbeing needs of the population in the ICS area
Integrated Care Systems	ICS	Integrated Care Systems are partnerships of organisations that come together to plan and deliver joined up health and care services, and to improve the lives of people who live and work in their area.
Key Performance Indicators	KPI's	Targets which performance can be tracked against
Pseudonymisation	-	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.
Record Lifecycle	-	Records lifecycle in records management refers to the stages of a records "life span": from its creation, to its preservation (in an archive) to its disposal/destruction.
Senior Information Risk Owner	SIRO	Board member with overall responsibility for: • The Information Governance, Data Security and Protection Policies

		• Providing independent senior board-level accountability and assurance that information risks are addressed • Ensuring that information risks are treated as a priority for business outcomes • Playing a vital role in getting the organisation to recognise the value of its information, and enabling its optimal effective use.
Subject Access Request	SAR	A subject access request (SAR) is simply a written or verbal request made by or on behalf of an individual for the information which he or she is entitled to ask for under the Data Protection Act 2018.
United Kingdom General Data Protection Regulation	UK GDPR	"GDPR" means UK GDPR. UK GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

Information Governance Policy

Purpose of Policy

This overarching Information Governance, Data Security and Protection Policy provides an overview of the organisation's approach to Information Governance and includes data protection and other related Information Governance policies, and details about the roles and management responsible for data security and protection in the organisation.

Introduction

Information is the most important asset available to an organisation and therefore all organisations must have robust arrangements for Information Governance (IG) which are reviewed annually and described in the Data Security and Protection Toolkit (DSPT).

It is of paramount importance to ensure that data and information is effectively managed and that appropriate policies, procedures, management accountability and structures provide a robust governance framework for information management.

The policies will provide assurance to the ICB and to individuals that personal data and information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

Through the action of approving the policy and its associated supporting documents, the Board provides an organisational commitment to its staff and the public that information will be handled within the identified framework.

The role of the ICB is to commission healthcare, both directly and indirectly, so that valuable public resources secure the best possible outcomes for patients. In doing so, the ICB will seek to meet the objectives prescribed in the NHS Act 2006 and the Health and Social Care Act 2012 and to uphold the NHS Constitution. The policy's objective is to ensure that people who work for the ICB understand how to look after the data and information they need to do their jobs, and to protect this information on behalf of patients.

UK General Data Protection Regulation 2021/Data Protection Act 2018

The UK General Data Protection Regulation 2021 (UK GDPR), which came in to effect on 1st January 2021, is the retained EU law version of the General Data Protection Regulation 2016 which first became directly applicable as law in the UK on 25th May 2018 and the Data Protection Act 2018 (DPA18) fills in the gaps of the UK GDPR, addressing areas in which flexibility and exemptions are permitted.

The UK GDPR/DPA18 are underpinned by a number of data protection principles which drive compliance.

Principles of the UK General Data Protection Regulation 2021/Data Protection Act 2018 (UK GDPR/DPA18)

1. **Lawful, fair and transparent processing** – this principle emphasises transparency for all UK data subjects. When the data is collected, it must be clear as to why that data is being collected and how the data will be used. Organisations also must be willing to provide details surrounding the data processing when requested by the data subject. For example, if a data subject asks who the data protection officer is at that organisation or what data the organisation has about them, that information needs to be available.

2. **Purpose limitation** – this principle means that organisations need to have a lawful and legitimate purpose for processing the information in the first place. Consider organisations that require forms with 20 data fields, when all they really need is a name, email, address and maybe a phone number. Simply put, this principle says that organisations should not collect any piece of data that does not have a specific purpose, and those who do can be out of compliance.

3. **Data minimisation** – this principle instructs organisations to ensure the data they capture is adequate, relevant and not excessive. In this day and age, businesses collect and compile every piece of data possible for various reasons, such as understanding customer buying behaviours and patterns or remarketing based on intelligent analytics. Based on this principle, organisations must be sure that they are only storing the minimum amount of data required for their purpose.

4. **Accurate and up to date** – this principle requires data controllers to make sure information remains accurate, valid and fit for purpose. To comply with this principle, the organisation must have a process and policies in place to address how they will maintain the data they are processing and storing. It may seem like a lot of work, but a conscious effort to maintain accurate customer and employee databases will help prove compliance and hopefully also prove useful to the business.

5. **Kept for no longer than necessary** – this principle discourages unnecessary data redundancy and replication. It limits how the data is stored and moved, how long the data is stored, and requires the understanding of how the data subject would be identified if the data records were to be breached. To ensure compliance, organisations must have control over the storage and movement of data. This includes implementing and enforcing data retention policies and not allowing data to be stored in multiple places. For example, organisations should prevent users from saving a copy of a customer list on a local laptop or moving the data to an external device such as a USB. Having multiple, illegitimate copies of the same data in multiple locations is a compliance nightmare.

6. **Appropriate security measures** – this principle protects the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security). An organisation that is collecting, and processing data is now solely responsible for implementing appropriate security measures that are proportionate to risks and rights of individual data subjects. Negligence is no longer an excuse under UK GDPR/DPA18, so organisations must spend an adequate amount of resources to protect the data from those who are negligent or malicious. To achieve compliance, organisations should evaluate how well they are enforcing security policies, utilizing dynamic access controls, verifying the identity of those accessing the data, and protecting against malware/ransomware.

Accountability and liability - The controller shall be responsible for, and be able to demonstrate compliance with these 6 Principles. All areas must be able to demonstrate to the ICB Board that they have taken the necessary steps comparable to the risk their data subjects face. To ensure compliance, organisations must be sure that every step within the UK GDPR is auditable and can be compiled as evidence quickly and efficiently. For example, UK GDPR requires organisations to respond to requests from data subjects regarding what data is available about them. The organisation must be able to promptly locate that data, if desired. Organisations not only need to have a process in place to manage the request, but also need to have a full audit trail to prove that they took the proper actions.

Caldicott Principles

The Caldicott Principles, first introduced in 1997, amended in 2013 and 2016, and then further amended with an additional Principle in 2020, are Information Governance guidelines applied widely across the field of health and social care to ensure that people's data is kept safe and used appropriately. Caldicott Guardians support the upholding of these principles at an organisational level.

Principle 1: **Justify the purpose for using confidential information** - Why is the information needed?
Principle 2: **Use confidential information only when it is necessary** – Can the task be carried out without identifiable information?
Principle 3: **Use the minimum necessary confidential information** – Can the task be carried out with less information?
Principle 4: **Access to confidential information should be on a strict need-to-know basis** – Only those who need access, should have access.
Principle 5: **Everyone with access to confidential information should be aware of their responsibilities** – Lack of knowledge is not acceptable.
Principle 6: **Comply with the law** – Every use of confidential information must be lawful.
Principle 7: **The duty to share information for direct care is as important as the duty to protect patient confidentiality.**

Principle 8: **Inform the expectations of patients and service users about how their confidential information is to be used** – Inform patients and service users about how their confidential information is used. A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this.

Appointment of Data Protection Officer

Under UK GDPR/DPA18, Data Protection Officers (DPOs) will be at the heart of the legal framework for all Health and Social Care organisations facilitating compliance with the provisions of the UK GDPR.

Within the NHS, it is mandatory for data controllers and processors to designate a DPO. It is especially important for organisations to nominate a DPO where it is processing personal and sensitive information on a large scale.

It would also be important to ensure that the DPO contact details are available in accordance with the requirements such as in fair processing/transparency notices.

For public authorities, DPOs are also required to have knowledge of administrative rules and procedures of the organisation.

The UK GDPR/DPA18 requires that organisations involve the DPO, "in all issues which relate to the protection of personal data". It is therefore crucial that the DPO is involved from the earliest stage possible in all issues relating to data protection.

In relation to Data Protection Impact Assessments (DPIA), the UK GDPR/DPA18 explicitly provides for the early involvement of the DPO and specifies that the controller shall seek the advice of the DPO when carrying out such impact assessments.

Ensuring that the DPO is informed and consulted at the outset will facilitate compliance with the DPA18, promote a privacy by design and privacy by default approach, and should therefore be standard procedure within an organisation's governance and procurement procedures.

In addition, it is important that the DPO be seen as a discussion partner within the organisation and that they are part of the relevant working groups dealing with data processing activities within the organisation.

Due to the large volume of high-risk sensitive data being processed within the NHS, the concept of the Data Protection Officer role is well embedded due to the mandated requirement to comply with the existing Data Protection Act through the Data Security and Protection Toolkit. This means that the roles, tasks and responsibilities are already undertaken within the ICB due to the maturity of Information Governance compliance in the ICB and the wider National Health Service.

Data Protection Officer

Within NHS Cheshire and Merseyside ICB, the DPO role has been delegated to Suzanne Crutchley, Head of Data Protection and Information Governance at Mersey Internal Audit Agency, a role which includes compliance responsibility for UK GDPR/DPA18, FOIA and Data Security.

Organisations should continue to ensure that the Data Protection Officer, or the designated representative:

- Is invited to participate regularly in meetings of senior and middle management where data processing activities are discussed, for example the Audit Committee.
- Are consulted where decisions with data protection implications are taken. All relevant information must be passed on to the C&M ICB Information Governance Service in a timely manner to allow them to provide adequate advice.
- The opinion of the IG Service and DPO should always be given due weight. In case of disagreement, the UK GDPR/DPA18 recommends, as good practice, to document the reasons for not following the DPO advice.
- The DPO/IG Service must be promptly consulted once a data breach or another incident has occurred, for example when incidents occur.

Resources

The UK GDPR/DPA18 requires that the organisation support the DPO function by providing resources necessary to carry out tasks and access to personal data and processing operations to maintain their expert knowledge, this could be through:

- Active support for the DPO function by senior management at Board Level.
- Sufficient time to fulfil their duties.
- Adequate support in terms of financial resources, infrastructure and premises.
- Official communication of the role and support.
- Continuous training to stay up to date within the field of Data Protection.
- It may also be necessary to set up a DPO team.

Scope

This suite of policies applies to all staff employed or who undertake work/volunteer, for the ICB.

Responsibilities:

Organisation (Chief Executive Officer)

Overall accountability for procedural documents across the organisation lies with the ICB Chief Executive Officer. As the Chief Executive Officer that has overall responsibility for establishing and maintaining an effective document management system and the governance of information,

meeting statutory requirements and adhering to guidance issued in respect of Information Governance and procedural documents.

SIRO

NHS Cheshire and Merseyside ICB have appointed the Prof. Rowan Pritchard-Jones , Medical Director as Senior Information Risk Owner (SIRO), who will:

- Take overall ownership of the organisation's Information Risk Policy.
- Act as champion for information risk on the Board and provide written advice to the Chief Executive Officer on the content of the organisation's annual governance statement regarding information risk.
- Understand how the strategic business goals of the ICB and how other NHS organisation's business goals may be impacted by information risks, and how those risks may be managed.
- Implement and lead the NHS Information Governance Risk Assessment and Management processes within the ICB. Advise the Board on the effectiveness of information risk management across the ICB.
- Receive training as necessary to ensure they remain effective in their role as SIRO.

Caldicott Guardian

NHS Cheshire and Merseyside ICB have appointed Christine Douglas, Director of Nursing and Care as the Caldicott Guardian for NHS Cheshire and Merseyside ICB, who will:

- Ensure that the ICB satisfy the highest practical standards for handling patient identifiable information.
- Facilitate and enable appropriate information sharing and make decisions on behalf of the ICB following advice on options for lawful and ethical processing of information, especially in relation to disclosures.
- Represent and champion Information Governance requirements and issues at Board level.
- Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS.

Information Asset Owners

Information Asset Owners are accountable for the application of this policy to the information assets that they 'own' and must:

- Lead and foster a culture that values, protects and uses information for the benefit of patients.
- Know what information comprises or is associated with the asset and understands the nature and justification of information flows to and from the asset.

- Know who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy.
- Understand and address risks to the asset and providing assurance to the SIRO.
- Ensure there is a legal basis for processing and for any disclosures.
- Refer queries about any of the above to the Data Protection Officer.

Information Asset Administrator

The role of Information Asset Administrator is to ensure that policies and procedures are followed within their area, recognise actual or potential security incidents, consult with their IAO on incident management and ensure that information assets registers are accurate and up to date.

Line Managers

Line managers will take responsibility for ensuring that these policies are implemented within their department or area of responsibility.

User

It is the responsibility of each employee to adhere to the policies.

All staff must make sure that they use the organisation's IT systems appropriately and in accordance with the IG Handbook/Code of Conduct.

Audit Committee

To monitor and co-ordinate implementation of the policies, the new Data Security and Protection Toolkit requirements and other information related legal obligations, NHS Cheshire and Merseyside ICB report to the responsible committee.

C&M ICB Information Governance Service

The Information Governance Service will provide expert advice and guidance to all staff on all elements of Information Governance. The team is responsible for:

- Providing advice and guidance on Information Governance issues to all staff.
- Developing Information Governance policies and procedures.
- Developing Information Governance awareness and training programmes for staff.
- Ensuring compliance with UK GDPR/DPA18, Information Security and other information related legislation.
- Providing support and advice to the team who handle freedom of information and subject access requests. Providing support to the Caldicott Guardian and Senior Information Risk Officer for Information Governance issues.

Information Governance Training

All staff are mandated to undertake annual Information Governance training, staff will undertake the IG refresher module online via ESR.

Some staff are required to undertake additional Information Governance training specific to their roles. This will be set out in the annual Information Governance Training Needs Analysis (TNA) and delivered through the associated training programme. This will include staff who are in contact with patients and/or staff who process patient data.

Data Protection Policy

Introduction

NHS Cheshire and Merseyside ICB need to collect personal confidential information about people with whom it deals in order to carry out its business and provide its services for healthcare. Such people include patients, employees (present, past and prospective), suppliers and other business contacts. The information includes name, address, email address, data of birth, private and confidential information, and sensitive information.

In addition, the ICB may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law. No matter how it is collected, recorded and used (e.g., on a computer or other digital media, on hardcopy, paper or images, including CCTV) this personal information must be dealt with properly to ensure compliance with UK GDPR/DPA18.

The lawful and proper treatment of personal information by the ICB is extremely important to the success of our business and in order to maintain the confidence of our service users and employees. We ensure that personal information is held lawfully and correctly and in line with this policy.

Keeping data subjects informed

We are required to let patients and other Data Subjects know what Information we collect about them, how we will use it and who we may share it with.
There are a number of methods for achieving this, for example information is posted on our public facing website.

Data quality and reuse

We will seek to maintain standards of information quality and avoid duplication, inaccuracy and inconsistencies across personal information. We will maintain comprehensive records management policies in order to help avoid excessive retention or premature destruction of personal information.

We will only use personal information where strictly necessary. Wherever it is possible to use anonymised data this will be preferred.

Data Subjects' Rights

We have a Records Management Policy which ensures that individuals can exercise rights over their own personal data in line with UK GDPR/DPA18. Access to the records of the deceased is also covered under the remit of this policy, though these fall outside of the UK GDPR/DPA18 and are dealt with in line with the Access to Health Records Act 1990.

Various Types of Consent

There are various consent types that are used namely:

a) Consent as a legal basis to process personal information ("UK GDPR Compliant Consent")
b) Consent to share information
c) Common Law Duty of Confidence (CLDC)
d) Consent to treatment

Which, if any, consent type is appropriate is dependent upon the work we undertake in our organisation. These consent types will now be explained in turn. Each will have their own procedures which are set out outside of this policy.

Consent as a Legal Basis to Process Personal Information

There are a number of legal bases for personal data processing under the UK GDPR, including Consent and Explicit Consent. Whenever processing personal data at least one lawful basis must apply under UK GDPR Article 6, plus at least one additional legal basis under UK GDPR Article 9 must apply if special category data is processed such as health data.

UK GDPR Compliant Consent may not be an appropriate legal basis if individuals cannot be offered a genuine choice over how their data is used, for example when data would still be processed under a different lawful basis if Consent were refused or withdrawn. This would be misleading and unfair as it presents the individual with a false choice and only the illusion of control.

Generally, Consent is unsuitable as a legal basis for the processing of healthcare data. Other legal bases such as 'public task' (UK GDPR Article 6(1)(e)) and 'medical purposes' (UK GDPR Article 9(2)(h)) may be more appropriate (and would not allow for the withdrawal of consent).

Should Consent be considered the correct legal basis, then a Controller must ensure that:

i) Consent is **freely given**. This means that individuals are offered real choice and control over how their data is used, that they can refuse Consent without detriment, and able to withdraw Consent easily at any time.
ii) Consent is **specific and informed**. Which means that individuals know who processes their data, for what purpose, how it will be processed, and also how they can withdraw their Consent at any time.
iii) Consent is **unambiguous**. It must be obvious that the individual has consented by way of clear affirmative confirmation and what exactly they have consented to.
iv) Consent (and any Consent Withdrawals) are **obtained, recorded, and managed**. Consent should be viewed as a dynamic part of an ongoing relationship of trust with individuals. It should be kept under regular review and may need refreshing if anything changes.

v) Individuals are able to **withdraw** their Consent easily and at any time.

Explicit Consent (for the processing of special category data) is not defined in the UK GDPR or the Data Protection Act 2018, but is not very different from the usual high standard of Consent under UK GDPR Article 6. The key difference is that 'Explicit' Consent must be positively affirmed in a clear statement (whether oral or written).

Consent should be considered when no other lawful basis obviously applies. Consent is likely needed for many types of marketing calls and messages, websites cookies, online tracking methods, and to install apps or other software on people's devices. As previously mentioned, in a healthcare context Consent is usually not the appropriate lawful basis under the UK GDPR, but this should be considered on a case-by-case basis.

Consent to Share Information

Sharing information is essential to provide the best possible care to a patient. The UK GDPR and Data Protection Act 2018 in combination with the Caldicott Principles provide a framework to share information for a patient's direct care.

In the healthcare sector, patient data is held under a duty of confidence. Health and care providers are able to share patient data for the purposes of direct care, without breaching confidentiality. In these circumstances the consent to share is considered to be implied.

Should a patient object to their confidential information being shared, this, in many cases, should be respected.

However, there may be times where, despite a patient's objection, information must be shared, for example when information about crime or abuse has come to light, if there are safeguarding concerns, where there is a requirement to report certain diseases, and anywhere else where there is a legal gateway as set out in UK GDPR's Artiles 6 and 9 that requires information to be shared without the consent of the patient. The 7th Caldicott Guardian principle refers to this in more detail and states that the duty to share information for individual care is as important as the duty to protect patient confidentiality.

Common Law Duty of Confidence

Common law is not written out in one document like an Act of Parliament (Statute). It is a form of law based on previous court cases decided by Judges (i.e. based on precedent).

As previously stated, health and care providers are able to share patient data for the purposes of direct care, without breaching confidentiality. When considering sharing patient data for non-direct

care/secondary purposes such as planning or research, the CLDC needs to be set aside to avoid breaching confidentiality.

When processing individual information for secondary purposes, compliance with the common law is achieved when one of the following circumstances applies:

i) Individuals have provided their Explicit Consent; or
ii) There is a statutory or other legal requirement; or
iii) The public interest served by disclosure outweighs the public interest of protecting confidentiality; or
iv) Approval under section 251 of the NHS Act 2006 is in place (most commonly for secondary uses this means the Health Research Authority's (HRA) Confidentiality Advisory Group (CAG) has given support under Regulation 5 of the Control of Patient Information Regulation 2002 (COPI) for a specific project).

Having UK GDPR legal bases for personal data processing does not remove the need to seek permission or an appropriate legal basis (e.g. Section 251 support) for using the data for secondary purposes. This links into the Data Protection Act principle of purpose limitation which means that you can only process data for the specified, explicit, and legitimate purposes and not further process it in a manner that is incompatible with those original purposes.

Consent to Treatment

Consent to treatment means a person must give permission before they receive any type of medical treatment, test or examination. For consent to be valid, it must be voluntary and informed, and the person consenting must have the capacity to make the decision. If an adult has capacity to make a voluntary and informed decision to consent to, or refuse, a particular treatment, their decision must be respected.

If a person does not have the capacity to make a decision about their treatment and they have not appointed a Lasting Power of Attorney (LPA), the healthcare professionals treating them should provide treatment if they believe it's in the person's best interests, taking into account all the circumstances, but Clinicians must take reasonable steps to discuss the situation with the person's friends/relatives before making these decisions if this is appropriate.

If they're able to, consent is usually given by patients themselves. But someone with parental responsibility may need to give consent for a child up to age 16 to have treatment. However, if a child is under the age of 16 and deemed to have the required competence and maturity to understand what they are being asked to consent to, then the child themselves may provide their consent. This is known as Gillick competency.

Being required to obtain a patient's consent to treatment is entirely separate from data protection obligations. Therefore a legal basis for the processing of the patient's personal data would still be

required; this could be on the basis of UK GDPR Compliant Consent or any of the other legal bases under Article 6 of UK GDPR.

Record of Processing Activities

As part of its compliance with UK GDPR/DPA18 and to provide assurance to its regulatory bodies we must maintains an internal record of processing activities which includes the following: -

- Purposes of the processing
- Description of the data processed
- Details of who we send personal data to
- Details of transfers to third countries including documentation of the transfer mechanism safeguards in place
- Description of technical and organisational security measures

Data Security

Personal data should be kept secure at all times. We ensure that there are adequate policies and procedures in place to protect against unauthorised access and against loss, destruction and damage.

Data Security and Protection Toolkit

In September 2024 the Data Security and Protection Toolkit (DSPT) changed to adopt the National Cyber Security Centre's Cyber Assessment Framework (CAF) as its basis for cyber security and IG assurance.

This change will lead to NHS Trusts, CSUs, ALBs and ICBs seeing a different interface when they log in, which sets out CAF-aligned requirements in terms of Objectives, Principles and Outcomes. Other organisations will retain the current interface and will continue to respond to a list of prescriptive controls, which will be mapped nationally 'in the background' against a CAF profile. Expectations for cyber security and IG controls should remain at a reasonably comparable level to the current DSPT, tightening only in areas where NHSE and DHSC believe the higher standard to be a necessary obligation.

Guidance has been produced, and webinars have been held to help organisations understand the content, approach and expectations of the CAF-aligned DSPT.
Further information is available at: News (dsptoolkit.nhs.uk)

The IG Service will ensure that supporting ICB policies and procedures to meet their Information Governance, data security and protection obligations are in place, to enable the ICB to fulfil their Information Governance responsibilities. These policies and procedures provide a framework to bring together all the requirements, standards and best practice that apply to the handling of confidential, business sensitive and personal information and include:

- Data Protection
- Data Quality
- Records Management
- Access to Information
- Freedom of Information
- IT/Network Security (Links to IT provider Policies)

Data Quality Policy

Introduction

NHS Cheshire and Merseyside ICB is committed to ensuring the quality of its data, to promote effective decision making and patient safety.
High quality information means better patient care and patient safety, and there could be potentially serious consequences if information is not correct and up to date, both for patients and for the ICB.
Management information produced from aggregate anonymised patient data is essential for the efficient running of the ICB and to maximise utilisation of resources for the benefit of patients and staff. It supports making effective decisions about the deployment of resources, and in demonstrating the value of the services provided by the ICB.

The ICB requires accurate, timely and relevant patient information to support:

- The delivery of effective, safe patient care
- The delivery of its core business objectives
- The monitoring of activity and performance for internal and external management purposes
- Clinical governance and clinical audit
- Service agreements and contracts
- Healthcare planning
- Accountability
- Compliance with Data Protection Act 2018 and UK GDPR 2021
- To be able to evidence compliance with regulatory requirements
- Support effective decision making with regards to the deployment of resources

The key obligations upon staff to maintain accurate records relate to:

- Department of Health and Social Care, Information Governance requirements
- Legal - UK GDPR and DPA18
- Freedom of Information Act (2000)
- Environmental Information Regulations (2000)
- Access to Health Records Act (1990)
- Contractual (contracts of employment)
- Ethical (Professional codes of practice)
- Policy (Records Management Policy, Information Governance Policy)
- NHS Constitution

NHS Cheshire and Merseyside ICB are committed to ensuring and improving where possible the quality of data it uses for all purposes.

Document Owner: Director of Corporate Affairs and Governance	Approval date: 3rd December 2024	First published: October 2022
	Next review date: December 2026	Version: 2.4

Purpose

The purpose of this policy is to set out what is required by all staff to ensure the quality of data used across the ICB.

It is the responsibility of all staff to ensure the information they generate is legible, complete, accurate, relevant, accessible and recorded in a timely manner. The quality of information produced can have a significant impact on the quality of services that we provide and commission.

Data Quality is essential for:

- Efficient delivery of patient care e.g., by ensuring that patients are given appointments and referrals are correctly processed.
- Clinical governance and minimising clinical risk e.g., wrong patient, wrong treatment.
- Management information to enable decisions to be made based on sound information, operational and strategic factors, together with local and national factors.
- Performance measurement against national trends and trends over time, so that we can continually plan improvements for our patients.
- As a foundation on which future investment and strategic decisions will be based.
- To support clinical audit and research and development, with a view to improving patient care in the future.

All staff need to be able to rely on the accuracy of the information available to them, to provide timely and effective services regardless of whether they are patient facing or central supporting functions.

To achieve this, all staff need to understand their responsibilities regarding accurate recording of patient data, whether on a computer system or on paper, e.g., case notes.

Data Quality Standards

The ICB Data Quality Standards are:

Accurate and up to date

All data must be correct and accurately reflect what happened. Therefore, all reference tables including GPs and postcodes must be updated regularly, usually within a month of publication. Every opportunity must be taken to check a patient's demographic details with the patient themselves at every contact, as inaccurate demographics may result in important letters being mis-delivered, or the incorrect identification of patients. However, it is important to note that the accuracy and timeliness of data does not just relate to patients.

Valid

Data should be within an agreed format which conforms to recognised national or local standards. Codes must map to national values and wherever possible, computer systems should be programmed to only accept valid entries.

Complete

Data should be captured in full. All mandatory data items within a data set should be completed and default codes will only be used where appropriate, not as a substitute for real data. The use of mandatory data items on the computer systems is to be encouraged, but only where this would not cause undue delay. For key data items which are not mandatory on the computer system, it is vital that a list of records with missing items can be produced, to be actioned later.

Timely

Data should be collected at the earliest opportunity, as recording of timely data is beneficial to the treatment of the patient. All data will be recorded to a deadline which will ensure that it meets national reporting and extract deadlines.

Defined and consistent

The data being collected should be understood by the staff collecting it and data items should be internally consistent. Data definitions should be reflected in procedure documents.

Coverage

Data will reflect the work of the ICB and not go unrecorded. Spot checks and comparison of data between months can highlight potential areas of incomplete data or loss. Staff should be cognisant that if something is not recorded there is no auditable proof that something occurred, and as such could be challenged.

Free from duplication and fragmentation

Patients should not have duplicated or confused patient records, and where possible data should be recorded once, and staff should know exactly where to access the data. Where a duplicate record is created, for example if a record is misplaced, records should be merged once the original is found.

Security and confidentiality

Data must be stored securely and processed in line with relevant legislation and local policy in relation to confidentiality. All staff must pay due regard to where they record information, what they record, how they store it and how they share information ensuring they comply with national and local requirements, policies and procedures.

How Data Quality can be improved

NHS Cheshire and Merseyside ICB acknowledge that good quality data can be achieved by careful monitoring and error correction, but it is more effective and efficient for data to be entered

correctly first time. To achieve this, good procedures must exist so that staff can be trained and supported in their work.

Information Asset Owners are responsible for ensuring that there are specific policies or procedures in place in relation to all information assets under their control, which set out as a minimum, when the information asset should be used, how it should be used and by whom and how the quality of data recorded will be monitored. Data quality audits must be completed annually as a minimum by Heads of Service or equivalent as in the IG Staff Handbook.

Where appropriate Information Asset Owners must ensure that training is available for staff to use the asset, and that information risks associated with each asset are actively identified, and being mitigated, ensuring that they provide assurance to the ICB SIRO.

Procedures need to be reviewed at least every two years or in response to changes in legislation, best practice etc., to take account of any changes in national standards and definitions.

Tight version control is essential so that staff in all parts of the ICB are using the same procedures which reflect current data definitions.

Records Management Policy

Introduction

This policy sets out the principles of records management for the ICB and provides a framework for the consistent and effective management of records that is standards based and fully integrated with other Information Governance initiatives within the ICB.

Records management is necessary to support the business of the ICB and to meet their obligations in terms of legislation and national guidelines.

The policy is based on guidance from the NHS Records Management Code of Practice 2023 and the retention schedules set out in the Code, which is available here. The Code provides guidelines for good practice in managing all types of NHS records and highlights the responsibilities of all staff for the records they create or use.

NHS Cheshire and Merseyside ICB have a statutory obligation to maintain accurate records of their activities and to make arrangements for their safe keeping and secure disposal. All records created in the course of the business of the ICB are public records under the terms of the Public Records Act 1958.

Effective records management is an essential requirement of the commissioning obligations of the ICB. It also recognises the importance of good records management practices to ensure:

- The right information is available at the right time.
- Authentic and reliable evidence of business transactions.
- Support for decision making and planning processes.
- Better use of physical and server space.
- Better use of staff time.
- Compliance with legislation and standards.
- Reduced costs.

Purpose and Scope

This policy applies to employees, agents and contractors working for, or supplying services to the ICB.

The ICB records are part of the organisation's corporate memory, providing the evidence of actions and decisions and representing a vital asset to support daily functions and operations, and to:

- Provide guidance to staff to carry out their corporate and personal record management responsibilities to support high quality patient care.
- Support the organisation and staff in meeting their obligations in terms of legislation and national good practice guidance.
- Provide effective governance arrangements for record management, also known as 'information lifecycle management'.

Definitions

Records: Recorded information in any form or medium, created or received and maintained by an organisation or person in the transaction of business or the conduct of affairs.

Health Records: Records which consists of information relating to the physical and/or mental health of an individual and has been made by or on behalf of a health professional in connection with that care.

Corporate Records: Records which relate to the corporate business of the ICB such as accounts, minutes, meeting papers, legal, and other administrative documents. They may contain personal identifiable information, for example personnel files, and should be treated with the same degree of care and security as patient/service user records.

Records Management: A discipline which utilises administrative systems to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound; whilst at the same time serving the operational needs of the ICB and preserving an appropriate historical record.

Records Lifecycle: A period a record exists from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as semi-active or closed records which may be referred to occasionally) and finally either confidential destruction or archival preservation.

Records Management

Records Creation

All records created in the ICB must be created in a manner that ensures that they are clearly identifiable, accessible, and can be retrieved when required.

All records created in the ICB must be authentic, credible, authoritative and adequate for the purposes for which they are kept. They must correctly reflect what was communicated, decided or undertaken.

Adequate records must be created where there is a need to be accountable for decisions, actions, outcomes or processes. For example, the minutes of a meeting, a clinician's examination of a patient, the payment of an account, or the appraisal of a member of staff.

Records Use and Maintenance

All staff have a duty for the maintenance and protection of records they use. Only authorised staff should have access to records.

The identification and safeguarding of vital records necessary for business continuity should be included in all business continuity /disaster recovery plans.

Any incidents relating to records, including the unavailability and loss, must be reported as an incident using the ICB incident reporting system.

Accuracy of statements i.e., record keeping standards, should pay attention to stating facts and not presenting opinions.

Records Tracking
Accurate recording and knowledge of the whereabouts of all records is essential if the information they contain is to be located quickly and efficiently. One of the main reason's records are misplaced or lost is that the next destination is not formally recorded.

All services/departments should ensure they have appropriate tracking systems and audit trails in place to monitor the use and movement of records.

Records Transportation
When records are being transported, whether they are electronic or paper, care should be taken to ensure the safe transition to the new location, whether this be temporary or permanent.

Records Storage
Records storage areas must provide storage, which is safe from unauthorised access, but which allows maximum accessibility to the records commensurate to its frequency of use.

The following factors must be considered:

- Compliance with Health and Safety and fire prevention regulations.
- Degree of security required.
- User needs.
- Type of records stored.
- Size and quantity of records.
- Usage and frequency of retrievals.
- Ergonomics, space, efficiency and price.

Inactive records sent for storage at the ICB approved facility must be boxed and include a retention date. The Information Asset Owner is responsible for keeping an accurate and up-to-date inventory of all records sent off-site.

Retention
The minimum length of time that a record is retained by the ICB depends on the type of record. The ICB has adopted the minimum retention schedules published in the NHS Records Management Code of Practice 2023.

Records, in whatever format they are held, may be retained for longer than the minimum retention periods, but should not normally be kept for more than 30 years.

Requests for extended preservation are subject to approval by the Audit Committee. This may only happen on grounds of historical archival value, relevance to research or other preserved records.

Information Asset Owners are responsible for determining if a record for which they are accountable should be retained for longer than the minimum retention period. This should be listed in a local

retention schedule and communicated to all Information Asset Assistants. Local retention schedules must be approved by the Audit Committee before implementation.

Disposal and destruction of records

For records that have reached their minimum retention period and there is no justification for continuing to hold them, they should be disposed of appropriately.

Paper records of a confidential nature should either be shredded using a cross shredder to DIN standard 4 or put in confidential waste that is appropriately destroyed by a company contracted to the organisation. Electronic records must be deleted from the device and not simply moved into the Trash folder, known as double deleting.

Access to Information Policy

(Subject Access Requests - SAR)

Introduction

All living individuals have the right under the Data Protection legislation (UK GDPR/DPA18), subject to certain exemptions, to have access to their personal records that are held by the ICB. This is known as a 'Subject Access Request' (SAR).

The UK GDPR/DPA18 only applies to living persons, but there are limited rights of access to personal health data of deceased persons under the Access to Health Records Act 1990.Requests may be received from members of staff, service users or any other individual who the ICB have had dealings with and holds data about that individual.

This will include information held both electronically and manually and will therefore include personal information recorded within electronic systems including emails, spreadsheets, databases or word documents and may also be in the form of photographs, x-rays, audio recordings and CCTV images etc.

Anyone making such a requested is entitled to be given a description of the information held, what it is used for, who might use it, who it may be passed on to, and where the information was gathered from.

Under UK GDPR individuals must also be provided with information on the expected retention periods of the information held, the right to request rectification or erasure of processing or raise and objection to the processing altogether.

UK GDPR/DPA18 changes to SAR

Under UK GDPR/DPA18 the right to make a SAR is very similar, with the key changes including:

- Abolition of the £10 administration fee (although "reasonable" fees can be charged for an excessive request or for further copies).
- Information must be provided without delay and at the latest within one month of receipt.
- Higher fines for failing to comply: the maximum fine that can be issued by the Information Commissioners Office (ICO) is £17.5 million or 4% of the total annual worldwide turnover in the preceding financial year, whichever is higher, and individuals also retain the right to pursue a claim in court.

Scope and Purpose

This policy applies to those members of staff that are directly employed by the ICB and for whom the ICB has legal responsibility. The policy also applies to all third parties and others authorised to undertake work on behalf of the ICB.

The purpose of this policy is to provide a guide to all staff on how to deal with subject access requests received and advise service users and other individuals on how and where to make requests.

Health Records

Although the ICB does not provide clinical services for direct patient care, it is recognised that the ICB does hold records on patients for other lawful reasons, which include;

- Continuing Health Care (CHC)
- Individual Funding Requests (IFR)
- Patient Experience
- Medicines Optimisation
- Apps used at Place for patients / Primary Care services
- Systems/software at Place for processing patient data
- Business Intelligence staff (BI)
- Emergency Planning and Responses (EPR)
- Staff who outsource services where patient data is processed

What is a SAR

Subject access is most often used by individuals who want to see a copy of the information an organisation holds about them. However, subject access goes further than this and an individual is entitled to be:

- Told whether any personal data is being processed.
- Given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people.
- Given a copy of the personal data.

Given details of the source of the data (where this is available)

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.

Some types of personal data are exempt from the right of subject access and so cannot be obtained by making a SAR. Other conditions to consider include:

- All clinical data should be reviewed by a clinician and consideration should be given to redacting any information likely to cause serious harm to the mental or physical health of any individual.
- Information supplied by third parties e.g., family members should usually be redacted.
- Data and information held from other agencies may be disclosable but should be discussed with the originating body first.
- Information should not be disclosed where there is a statutory or court restriction on disclosure e.g., adoption records.

- References written for current or former employees are exempt (but not those received from third parties).
- In the case of deceased records, information should not be disclosed where the entry in the records makes it clear that the deceased expected the information to remain confidential.
- A personal record may also contain reference to third parties and redaction should be considered by balancing the UK GDPR/DPA18 rights of all parties.

Recognising a SAR

A SAR can be made in writing or verbally; however, the requestor does not need to mention Data Protection/UK GDPR or state that they are making a SAR for their request to be valid. They may even refer to other legislation, for example, the Freedom of Information Act 2000, but their request should still be treated according to this policy.

The following are examples of formal Subject Access Requests:

- "Please send me a copy of my HR file, or occupational health records"
- "I am a solicitor acting on behalf of my client and request a copy of their medical record (an appropriate authority is enclosed)"
- "The police state that they are investigating a crime and provide an appropriate form requesting information signed by a senior police officer"

Requests should be dealt with within a maximum of one month under UK GDPR subject to the necessity to seek clarification. It is possible to extend this timescale by a further two months where requests are complex. However if this is the case the ICB must inform the individual within one month of the request and explain why the extension is necessary.

NHS best practice recommends disclosure within 21 days where a record has been added to in the last 40 days.

The Common Law Duty of Confidentiality extends beyond death. Certain individuals have rights of access to deceased records under the Access to Health Records Act 1990:

- The patient's personal representative (Executor or Administrator of the deceased's estate).
- Any person who may have a claim arising out of the patient's death.

A Next of Kin has no automatic right of access, but professional codes of practice allow for a clinician to share information where concerns have been raised. Guidance should be sought from the Caldicott Guardian in relation to requests for deceased records.

A SAR can be made via any of, but not exclusively, the following methods:

- Email
- Post
- Social media
- ICB website
- Verbally

- In person, at an agreed ICB office

Requests made about or on behalf of other individuals

A third party, e.g., solicitor, may also make a valid SAR on behalf of an individual.

Where a request is made by a third party on behalf of another living individual, appropriate and adequate proof of that individuals' consent or evidence of a legal right to act on behalf of that individual e.g., power of attorney, which must be provided by the third party.

Requests on behalf of a child

Even if a child is too young to understand the implications of subject access rights, information about them is still their personal information and does not belong to anyone else, such as a parent or guardian.

So, it is the child who has a right of access to the information held about them, even though in the case of young children these rights are likely to be exercised by those with parental responsibility for them.

Before responding to a SAR for information held about a child, you should consider whether the child is mature enough to understand their rights. If the clinician responsible for the child's treatment plan is confident that the child can be considered competent under Gillick and/or Fraser guidelines, has the capacity to understand their rights and any implications of the disclosure of information, then child's permission should be sought to action the request.

The Information Commissioners Office (ICO) has indicated that in most cases it would be reasonable to assume that any child that is aged 12 years or more would have the capacity to make a Subject Access Request and should therefore be consulted in respect of requests made on their behalf.

The Caldicott Guardian should also be consulted on whether there is any additional duty of confidence owed to the child or young person as it does not follow that just because a child has capacity to make a SAR, that they also have the capacity to consent to sharing their personal information with others, as they may still not fully understand the implications of doing so.

Requests for personal information – Police/HMRC

Requests for personal information may be made by the above authorities for the following purposes:

- The prevention or detection of crime.
- The capture or prosecution of offenders.
- The assessment or collection of tax or duty .

A formal documented request signed by a senior office from the relevant authority is required before proceeding with the request.

The request must make it clear that one of the above purposes is being investigated and that not receiving the information would prejudice the investigation.

These types of requests must be considered by a senior manager or the SAR team on a case-by-case basis before any decision or action is taken to release information.

Court Orders

All Court Order requesting personal information about an individual must be complied with.

Subject Access Request Process

Requests for information held about an individual must be directed to the MIAA SAR Team at: cmicb.sars@miaa.nhs.uk

The team will acknowledge the request and log it and notify the requestor of the next steps. The requestor may be asked to complete an application form to better enable the ICB to locate the relevant information.

It is important that a SAR is identified and sent to the MIAA SAR team quickly to ensure the request can be responded to within one month of receipt.

Responding to requests

A detailed Standing Operating Procedure has been produced which gives full details as to how the ICB responds to individual SARs.

It is essential though that a log of all requests received is maintained and includes:

- Date received
- Date response due (within one month)
- Applicant's details
- Information requested
- Exemptions applied, if applicable
- Details of decisions to disclose information without the subject's consent (if applicable)
- Details of information to be disclosed and the format in which they were supplied
- When and how supplied (for example, hard copy and by post)

Performance monitoring

The ICB will ensure that monitoring and evaluation of the implementation of SAR takes place on a regular basis. The Governance Team will report progress reports to the Audit Committee and will include following:

- Number of requests.
- Incidents/Breaches in response times (detailed exception reports).
- Complaints.

Freedom of Information (FOI) Policy

Introduction

The Freedom of Information Act (2000) came into effect for all public authorities in January 2005. Since then, all requests for information have had to be answered in accordance with the Freedom of Information (FOI) Act 2000 or the Environmental Information Regulations 2004 (EIR).

The Freedom of Information Act gives a general right of access to all types of recorded information held by public authorities. Disclosures are subject to the application of relevant exemptions contained within the Act.

Under the Act, NHS Cheshire and Merseyside ICB must consider all requests for recorded information it receives and must:

- Inform the applicant whether the information is held.
- And supply the requested information subject to the application of relevant exemptions contained within the Act.

We remain committed to promote a culture of openness and accountability to enable you to have a greater understanding of how we carry out our duties, how we make decisions and how we spend public money.

The FOIA is fully retrospective and covers all information held in a recorded format. The deadline for a public authority to respond to requests made under the Act is 20 working days, although there are some circumstances where this may be extended under the terms of the legislation.

A request for information under the general rights of access must be:

- FOI - Received in writing.
- EIR – Received verbally or in writing.
- State the name of the applicant and an address for correspondence .
- Clearly describe the information requested.

Requests can also be made electronically via email.

Exemptions

The rights within the Act may be limited by applying certain exemptions. Several sections of the Act confer an absolute exemption on information disclosure. There are 23 exemptions from the rights of access under the Act, 8 of which are absolute. These exemptions mark out the limits of the right of access to information under the Act. Further details about applying exemptions can be obtained from the FOI team.

Other sections of the FOI Act direct the ICB to weigh up whether the public interest in maintaining the bar on confirmation/denial or in maintaining the exemption is greater than the public interest in disclosing whether the public authority holds the information, or in disclosing the information at all. In some cases, if an exemption applies the ICB may be obliged to disclose the information if the public interest test outweighs the exemption.

Refusal of requests

The ICB are obliged to disclose information requested under the Act unless an exemption applies to the information requested. If the ICB refuses a request, the applicant should be informed, at the same time as notification of the exemption, including the procedure to follow if the requester is not satisfied. This procedure includes an internal review by the ICB, if the requester is not happy with the findings of the internal review, then they should be directed to make a complaint to the ICO. Further details of dealing with FOI refusals should be sought from: foi@cheshireandmerseyside.nhs.uk

If a request is made for information that is subject to a current piece of work and premature disclosure is not deemed in the public interest, then the ICB can withhold the information temporarily. If withheld, then an indication of when the information will be available should be given.

Release of employee names and details

As a public authority, there is a recognised justification for the disclosure of some employee names and contact details. Board member and other staff members whose name are already published on the ICB's website will be released without seeking additional consent.

Those staff with public facing roles will have work contact details routinely released however, for other staff, consent will normally be sought if release is deemed appropriate. Personal contact details (home address, home telephone number or personal email address) will **never** be released in response to a request under the Act.

Time limits for compliance with requests

The ICB has a statutory obligation to comply with the FOI Act and has established systems and procedures to ensure that the organisation complies with the Act and to provide the information requested within 20 working days of a request.

Compliance with the 20-day time limit arising from FOI requests is also monitored.

If the ICB chooses to apply an exemption to any information, or it exceeds the appropriate limit for costs of compliance, a notice shall be issued within twenty working days informing the applicant of this decision.

What to do if you receive a request for information

If a member of staff receives a request, it must be passed to the Governance Team immediately. Failure to do this may result in a delay in processing the request and complying with the Law.

All requests should be sent to: foi@cheshireandmerseyside.nhs.uk

Monitoring and Evaluation

The ICB will ensure that monitoring and evaluation of the implementation of FOI takes place on a regular basis. The Governance Team will report progress reports to the Audit Committee and will include following:

- Number of requests.
- Breaches in response times (detailed exception reports).
- Justification of exemptions.
- Complaints.
- Any requests escalated to the ICO.

Network and IT Security Policies

IT Provider policies

IT policies are in place and are available from the Midlands and Lancashire Commissioning Support Unit, Mid Mersey Digital Alliance and Informatics Merseyside upon request.

Registration Authority Policy and Procedure

Midlands and Lancashire Commissioning Support Unit, iMerseyside and Mid Mersey Digital Alliance provide Registration Authority services to NHS Cheshire and Merseyside ICB and each have policies available upon request.

Document Owner: Director of Corporate Affairs and Governance	Approval date: 3rd December 2024	First published: October 2022
	Next review date: December 2026	Version: 2.4

Appropriate Policy Document for Processing Special Category Data and Criminal Offence Data for Safeguarding Purposes

To note (March 2025):
This Policy was initially drafted in consultation with the ICB Safeguarding Service and ratified by the Quality & Performance Committee. It is now the responsibility of the Audit Committee, forming part of the ICB's suite of information governance policies. Approval by the Audit Committee follows endorsement by the Information Governance Management Group (IGMG) whose membership includes the ICB SIRO, the ICB Caldicott Guardian, and the ICB Data Protection Officer.

Document Owner: Director of Corporate Affairs and Governance	Approval date: 3rd December 2024	First published: October 2022
	Next review date: December 2026	Version: 2.4

Glossary of Terms

Term	Acronym	Definition
Anonymisation		It is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous.
Child Death Review		Carried out by a Child Death Overview Panel for the purpose of a review or analysis to identify matters relating to the death or deaths that are relevant to the welfare of children in the area or to public health and safety, and to consider whether it would be appropriate for anyone to take action in relation to any matters identified.
Clinical Commissioning Group	CCG	They were responsible for commissioning healthcare services in both community and hospital settings up to the 30th June 2022 when they were replaced by ICBs.
Code of Conduct		Policy document which sets out rules to guide behaviours and decisions in a specified situation.
Data Controller		The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor		A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
Data Protection Act 2018	DPA	An Act for the regulation of the processing of information relating to living individuals, including the obtaining, holding, use or disclosure of such information
Data Protection Impact Assessment	DPIA	A method of identifying and addressing privacy risks in compliance with GDPR requirements.

Data Protection Officer	DPO	A role with responsible for enabling compliance with data protection legislation and playing a key role in fostering a data protection culture and helps implement essential elements of data protection legislation
Data Security and Protection Toolkit	DSP Toolkit	The DSP Toolkit is the standard for cyber and data security for healthcare organisations. Organisations measure performance against the National Data Guardian's 10 data security standards.
Data Subject		The identified or identifiable living individual to whom personal data relates
Domestic Homicide Review	DHR	"Domestic Homicide Review" ("DHR") is a multi-agency review of the circumstances in which the death of a person aged 16 or over has, or appears to have, resulted from violence, abuse or neglect by a person to whom they were related or with whom they were, or had been, in an intimate personal relationship, or a member of the same household as themselves. A DHR is run by a "Community Safety Partnerships" ("CSP") which is made up of representatives from the Police, Local Authorities, and Health &c (who are "Responsible Authorities").

UK General Data Protection Regulation	UK GDPR	The UK GDPR 2021 is the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (EU GDPR) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419). The General Data Protection Regulation (EU GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. It replaced the Data Protection Directive 95/46/ect.
Information Asset Register	IAR	A register that records assets, systems and applications used for processing or storing personal data across the organisation
Integrated Care Boards	ICB	They replaced CCGs from the 1st July 2022 and they are responsible for commissioning healthcare services in both community and hospital settings.
Information Commissioner's Office	ICO	The Information Commissioner's Office (ICO) upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
Information Governance Handbook		Policy document outlining the standards and expectations of staff's compliance and expected code of conduct.

Information Governance and Data Security Protection Policy		An overview of the organisation's approach to information governance and includes data protection and other related information governance policies; and details about the roles and management responsible for data security and protection in the organisation.
Information Sharing Agreement	ISA	An Agreement outlining the information that parties agree to share and the terms under which the sharing will take place.
Pseudonymisation		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.
Personal Data		Any information by which a living individual (the "Data Subject") can be identified. Individual identification can be by information alone or in conjunction with other information.
Privacy Notice	PN	A public facing document which informs the data subject of how they should expect their personal information to be processed.
Record Management Code of Practice 2023		A guide to use in relation to the practice of managing records relevant to organisations working within, or under contract to, the NHS in England. This includes Public Health functions in local authorities and Adult Social Care where joint care is provided with the NHS. It provides a framework for consistent and effective records management based on established standards

Retention Schedules		A policy document that identifies and describes an organisation's records, usually at the series level, and provides instructions for the disposition of the records throughout their life cycle
Safeguarding Adults Boards	SAB	A group of partners whose responsibility is to help and safeguard adults with care and support needs by assuring itself that local safeguarding arrangements are in place as defined by the Care Act 2014 and statutory guidance.
Safeguarding Purposes		Processing data under a statutory duty to enable early intervention and preventative work for safeguarding and promoting welfare of those at risk of abuse and harm and for wider public protection, for all areas of adult and children's safeguarding

Introduction

This policy, established by the Cheshire & Merseyside ICB explains how the Cheshire & Merseyside ICB's, acting in their capacity as a Data Controller and/or through their Data Processors will:

- ensure compliance with the Data Protection Principles; and
- manage the retention and erasure of Personal Data and Special Category Data,

to comply with the following requirements of the Data Protection Legislation, including but not limited to the Data Protection Act 2018:

- Section 38 (Schedule 1) of the Data Protection Act 2018 which requires an Appropriate Policy Document where Data is Processed in reliance on a condition in Part 1, 2 or 3 of Schedule 1 of the Data Protection Act 2018 to provide a lawful basis,
- reliance under Section 18 and Section 19 of Schedule 1 of the Data Protection Act 2018 to provide a lawful basis under Article 9(2)(i) of the General Data Protection Regulations, in that processing data for safeguarding purposes is necessary for reasons of substantial public interest,
- reliance under Section 6 (Schedule 1) of the Data Protection Act 2018 to provide a lawful basis under Article 10 of General Data Protection Regulations, in that it is necessary for a function conferred by an enactment or rule of law (Section 9 of the Domestic Violence, Crimes and Victims Act 2004) and is necessary for reasons of substantial public interest,

so that the Cheshire & Merseyside ICB can process Special Category Data and Criminal Offence Data when undertaking its statutory duty to enable early intervention and preventative work for safeguarding and promoting welfare of those at risk of abuse and harm and for wider public protection, for all areas of adult and children's safeguarding.

The Data Protection Principles

Principles relating to processing of personal data

1.Personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

In addition, the controller shall be responsible for, and be able to demonstrate compliance with, the six Principles listed above ('accountability').

Conditions for the Processing of Special Category Data and Criminal Offence Data for Safeguarding Purposes for reasons of Substantial Public Interest

Child Safeguarding Practice Reviews

The processing of Personal Data by the ICB is lawful because:

- it is a partner of the local multi-agency safeguarding partnership within Cheshire &

Merseyside as set out in the Children Act 2004, as amended by the Children and Social Work Act 2017 and the purpose of such reviews is to explore how practice can be improved through changes to the system itself and seek to understand why mistakes were made and to comprehend whether mistakes made on one case frequently happen elsewhere and why; and

- it may request information from a person or organisation for the purposes of enabling or assisting the review and/or analysis process under Section 10,11 & 16D of the Children Act 2004; and
- under Section 18 of Schedule 1 of the Data Protection Act 2018, for the reasons of substantial public interest it is necessary to process the data for the purposes of protecting an individual (including a type of individual) from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual where that individual is aged under 18 where that processing is carried out without the consent of the data subject where consent cannot be given, or the data controller cannot reasonably be expected to obtain the consent of the data subject or obtaining consent would prejudice the provision of protection,

and so in accordance with Section 8 and 10 of the DPA the ICB meets the requirement under Article 6(1)(e) of the UK GDPR to process Personal Data, and Article 9(i) of UK GDPR to process Special Category Data for reasons of substantial public interest.

Rapid Review

The processing of Personal Data by the ICB is lawful because:

- it is a partner of the local multi-agency safeguarding partnership within Cheshire & Merseyside as set out in the Children Act 2004, as amended by the Children and Social Work Act 2017 and under Chapter 4 of the statutory guidance *Working Together to Safeguard Children 2018* are required to undertake a rapid review for serious child safeguarding purposes where abuse or neglect of a child is suspected and the child has died or has been seriously harmed; and the purpose of such reviews is to gather the facts about the case, as far as they can be readily

established at the time, discuss whether there is any immediate action needed to ensure children's safety and share any learning appropriately, consider the potential for identifying improvements to safeguard and promote the welfare of children, decide what the appropriate course of action is; and

- it may request information from a person or organisation for the purposes of enabling or assisting the review and/or analysis process under Section 10,11 & 16D of the Children Act 2004; and
- under Section 18 of Schedule 1 of the Data Protection Act 2018, for the reasons of substantial public interest it is necessary to process the data for the purposes of protecting an individual (including a type of individual) from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual where that individual is aged under 18 where that processing is carried out without the consent of the data subject where consent cannot be given, or the data controller cannot reasonably be expected to obtain the consent of the data subject or obtaining consent would prejudice the provision of protection,

and so in accordance with Section 8 and 10 of the DPA the ICB meets the requirement under Article 6(1)(e) of the UK GDPR to process Personal Data, and Article 9(i) of UK GDPR to process Special Category Data for reasons of substantial public interest.

Child Death Review

The processing of Personal Data by the ICB is lawful because:

- it is a partner of the Child Death Overview Panels within Cheshire & Merseyside as set out in the Children Act 2004, as amended by the Children and Social Work Act 2017 and the purposes of a review or analysis are to identify matters relating to the death or deaths that are relevant to the welfare of children in the area or to public health and safety, and to consider whether it would be appropriate for anyone to take action in relation to any matters identified; and
- it may request information from a person or organisation for the purposes of enabling or assisting the review and/or analysis process under Section 10 &

11 of the Children Act 2004; and

- under Section 18 of Schedule 1 of the Data Protection Act 2018, for the reasons of substantial public interest it is necessary to process the data for the purposes of protecting an individual (including a type of individual) from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual where that individual is aged under 18 where that processing is carried out without the consent of the data subject where consent cannot be given, or the data controller cannot reasonably be expected to obtain the consent of the data subject or obtaining consent would prejudice the provision of protection,

and so in accordance with Section 8 and 10 of the DPA the ICB meets the requirement under Article 6(1)(e) of the UK GDPR to process Personal Data, and Article 9(i) of UK GDPR to process Special Category Data for reasons of substantial public interest.

Safeguarding Adults Boards

The processing of Personal Data by the ICB is lawful because:

- under Section 18 and 19 of Schedule 1 of the Data Protection Act 2018, for the reasons of substantial public interest it is necessary to process the data for the purposes of protecting:
    - an individual (including types of individual from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual where that individual is aged over 18 and at risk where there is a reasonable cause to suspect that the individual has needs for care and support, is experiencing, or at the risk of neglect or physical, mental or emotional harm and as a result of those needs is unable to protect themselves against the neglect or harm or the risk of it; or
    - the economic well-being of an individual at economic risk who is aged 18 or over and the data is concerning health,

  where that processing is carried out without the consent of the data subject where consent cannot be given, or the data controller cannot reasonably be expected to

obtain the consent of the data subject or obtaining consent would prejudice the provision of protection; and

- may request or provide information to enable the Safeguarding Adults Board to exercise its functions;
- processing is a statutory responsibility under the above-mentioned legislation because the ICB is a member of the Safeguarding Adults Boards under Schedule 2 of the Care Act 2014 and so has a duty to help and safeguard adults with care and support needs by assuring itself that local safeguarding arrangements are in place as defined by the Care Act 2014,

and therefore in accordance with Section 8 and 10 of the DPA the ICB meets the requirement under Article 6(1)(e) of the UK GDPR to process Personal Data, and Article 9(i) of UK GDPR to process Special Category Data for reasons of substantial public interest.

Domestic Homicide Review

The processing of Personal Data by the ICB is lawful because it is:

- a relevant authority under the Crime & Disorder Act 1998 (as updated by the Health and Social Care Act 2012) and so has a statutory responsibility to work in partnership with other responsible authorities (police, council, fire and probation &c) to form Community Safety Partnerships (CSPs) to tackle crime, disorder, drugs and alcohol; and
- there is a statutory responsibility for CSPs to share relevant information in order to complete a Domestic Homicide Review (DHR) under Section 9 of the Domestic Violence, Crime and Victims Act (2004) when a case meets the criteria set out in Section 9(1) of said Act; and
- Processing is necessary under the above-mentioned legislation and so there is a reason to process the data under a substantial public interest under Section 6 (Part 2) of Schedule 1, and Section 36 (Part 3) of Schedule 1 of the Data Protection Act 2018,

and therefore the ICB in accordance with Section 10 of the DPA meets the requirement

under Article 10 of GDPR to process Personal Data relating to criminal convictions and offences.

Conditions for Processing

Under Section 38 (Part 4) of the DPA the ICB is required to have in place an Appropriate Policy Document in place when the Processing is carried out and:

- this document explains the ICBs procedures for securing compliance with the principles in Article 5 of GDPR in connection with the processing of personal data in reliance on the above conditions; and
- explains the ICB s policies as regards the retention and erasure of personal data processed in reliance on the above conditions, giving an indication of how long such personal data is likely to be retained; and
- explains that the processing is necessary to fulfil obligations or exercise rights in law in connection with special category of personal data (including Safeguarding Data) and Criminal Offence Data,

and that the above will be met by this Appropriate Policy Document.

How the ICB will meet the Data Protection Principles

Lawful and Fair

The ICB will communicate processing information to Data Subjects via the Privacy Notice on the ICB website. It will also make the same information available in other formats to Data Subjects on the collection of Personal Data from the Data Subject and/or on request, as appropriate.

The ICB will only undertake Processing of Personal Data where it has a lawful basis to do so and where the information is required for a specific reason.

Specified, Explicit and Legitimate Purposes

Processing of Personal Data will be restricted to only that which is necessary meet its statutory duty to enable early intervention and preventative work for safeguarding and

promoting welfare of those at risk of abuse and harm and for wider public protection, for all areas of adult and children's safeguarding.

Criminal Offence Data will be processed to conduct a Domestic Homicide Review and it will not be used for a matter which is not for that purpose unless that use is authorised by law. It may be used for another lawful purpose by the ICB or another organisation that is authorised to carry out the processing of Criminal Offence Data.

Adequate, Relevant and not Excessive

Any Personal Data collected for Safeguarding Purposes or for the conduct of a Domestic Homicide Review will be restricted to that which is necessary for the purposes of processing. Data will be subject to anonymisation, and where required, pseudonymisation. The data protection training undergone by all staff emphasise is this. Staff are also advised not to record their opinions unless that is a requirement.

Accurate and where necessary kept up to date

The ICB will ensure, as far as reasonably possible, that the Personal Data which the ICB holds is accurate and kept up to date. In some circumstances there may be a need to keep factually incorrect information e.g. in a statement from a victim, witness or alleged perpetrator.

All staff are made aware of the need for accuracy and are responsible for the accuracy of the Personal Data they process. Checks are carried out on the accuracy of Personal Data during audits and reviews.

Personal Data found to be inaccurate will be rectified or destroyed whenever possible. Where this is not possible, there will be an addendum on that Personal Data advising of the inaccuracy.

Kept for no longer than is necessary

The ICB will comply with the Records Management Code of Practice for Health and Social Care 2023 regarding the retention of Personal Data. From this the ICB has created their own local retention schedule.

All personal data kept for specific purposes is reviewed on a regular basis and will not be processed for longer than is necessary.

When an individual withdraws consent to the Processing (where consent has been previously requested and provided by the individual), that the Personal Data will be destroyed in line with the legislative requirements, if the ICB has no other lawful basis to continue Processing such Personal Data.

Appropriate Security

The ICB has developed and implemented appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Technical Measures

The ICB complies with the information security standards set by NHS Digital. The ICB publishes its Data Security Protection Toolkit on an annual basis which demonstrates compliance with those security standards. In addition, the Data Processor to the ICB, MLCSU, Informatics Merseyside and Mid Mersey Digital Alliance, implement technical measures which include encryption, firewalls, antivirus software, IT health checks, vulnerability assessment and penetration process, user authentication, role based and password-controlled access, technical assurance and technical audits and endpoint management.

Organisation Measures

All new staff are vetted prior to appointment and must are required to undertake mandatory data protection training on an annual basis.

Buildings are kept physically secure, with access only being granted to

individuals who require it. Further measures are out in the following policies:

- Information Governance and Data Security and Protection Policy
- Information Governance Handbook

- Information Governance Code of Conduct

Retention and Erasure of Personal Data

Destruction of Personal Data will be dealt with in accordance with the ICBs retention schedule and/or in accordance with the guidance provided by the Secretary of State.

Where Data is processed for Safeguarding Purposes (including Criminal Offence Data), where a review or a panel is involved, reports may be published. Such Published reports will not contain personal data. Each C&M Place Partnerships and Boards have their own process and timeframe for publication and archiving of the reports including the timeframe they will stay on each individual Partnership and Board website and how long after they will then archive.

Accountability

The ICB will demonstrate compliance with the data protection principles by:

- ensuring that records are maintained of all Personal Data processing activities and that such records are provided to the Information Commissioner's Office (ICO) on request; and
- carrying out a data protection impact assessment on any high-risk Personal Data processing and consulting the ICO if appropriate; and
- appointing a Data Protection Officer (DPO) to provide independent advice and monitoring of Personal Data handling; and
- having in place internal processes to ensure that Personal Data is only collected, used or handled in a way that is compliant with the data protection law.

Retention and Review of this Policy

This policy document will be retained in accordance with Section 40 (Schedule 1) of the DPA. It will be made available to the ICO on request.

The policy will be reviewed on an annual basis (or more regularly if circumstances require it).

Appendix A

Information Governance Management Framework

	Requirement	Detail
Senior Roles within the ICB	**Chief Executive Officer:** Graham Urwin	The Chief Executive Officer of the ICB has overall accountability and responsibility for Information Governance in the ICB and is required to provide assurance through the Annual Governance Statement that all risks to the organisation, including those relating to information, are effectively managed and mitigated.
	Senior Information Risk Owner and Executive IG Lead: Prof. Rowan Pritchard-Jones, Medical Director	The Senior Information Risk Owner (SIRO) is an Executive Director of the ICB Board. The SIRO is expected to understand how the strategic business goals of the ICB may be impacted by information risks. The SIRO will act as an advocate for information risk on the Board and in internal discussions and will provide written advice to the Accountable Officer on the content of their Annual Governance Statement regarding information risk. The SIRO will provide an essential role in ensuring that identified information security threats are followed up and incidents managed. They will also ensure that the Board and the Accountable Officer are kept up to date on all information risk issues. The role will be supported by a deputy SIRO at the ICB, together with a deputy SIRO at each Place.

	Requirement	Detail
		The SIRO will be supported through a network of Information Asset Owners and Assistants who have been identified and trained throughout the organisation. The SIRO is also appointed to act as the overall Information Governance lead for the ICB and co-ordinate the IG work programme. The Executive IG Lead role has been assigned as Department of Health response to the Caldicott 2 Review contains an expectation that organisations across health and social care strengthen their leadership on Information Governance. The Executive IG lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG, although the key tasks are likely to be delegated to an Operational IG Lead.
	Caldicott Guardian: Christine Douglas, Director of Nursing and Care	The Caldicott Guardian has responsibility for reflecting patients' interests regarding the use of patient identifiable information and to ensure that the arrangements for the use and sharing of clinical information comply with the Caldicott principles. The Caldicott Guardian will advise on lawful and ethical processing of information and enable information sharing. They will ensure that

	Requirement	Detail
		confidentiality requirements and issues are represented at Board level and within the ICB's overall governance framework. The role will be supported by a deputy Caldicott Guardian at the ICB, together with a Caldicott Champion at each Place.
	Data Protection Officer: Suzanne Crutchley MIAA Head of Data Protection & Information Governance	The Data Protection Officer (DPO) reports to the SIRO. This ensures the DPO can act independently, without a conflict of interest and report direct to the highest management level. The DPO is responsible for ensuring that the ICB and its constituent business areas always remain compliant with data protection, privacy & electronic communications regulations, freedom of information act and the environment information regulations. The DPO shall lead on the provision of expert advice to the organisation on all matters concerning the information rights law, compliance, best practice and setting and maintaining standards.

	Requirement	Detail
	ICB Information Governance Lead: Suzanne Crutchley MIAA Head of Data Protection & Information Governance	The key purpose of the role is to ensure the ICB successfully achieves the required level of compliance across all requirements of the NHS Digital Information Governance Toolkit. The post holder will support the ICB to ensure the establishment of corporate standards and a consistent ICB wide approach to Information Governance and will be responsible for assuring the implementation of a range of policies, processes, monitoring audits and training and awareness mechanisms to ensure a high level of compliance.
	Information Governance Organisational Lead: Matthew Cunningham, Associate Director of Corporate Affairs and Governance	The key purpose of the role is to ensure the ICB successfully implements a range of policies, processes, monitoring audits and training and awareness mechanisms to ensure a high level of compliance with Information Governance and Information Security. The post holder will ensure the implementation of corporate standards and a consistent organisation wide approach to Information Governance and Information Security.
Key Governance Bodies A group, or groups, with appropriate authority should have responsibility for the IG agenda.	**Audit Committee**	The Audit Committee is responsible for overseeing Information Governance issues, approving and maintaining policies, standards, procedures and guidance, coordinating and raising awareness of Information Governance in the ICB.

	Requirement	Detail
Resources Details of key staff roles	**Dedicated MIAA Information Governance Staff**	Various staff at MIAA provide support to the ICB Information Governance Service. IG Mailbox - infogov.cmicb@miaa.nhs.uk
Governance Framework Details of how responsibility and accountability for IG is cascaded through the organisation.	**Information Asset Owners**	Information Asset Owners are senior individuals involved in running the relevant business. The IAOs role is to: • Understand and address risks to the information assets they 'own'; and • Provide assurance to the SIRO on the security and use of these assets. Information Asset Owners have been nominated across the whole organisation and have received specialist information risk training to allow them to be effective in their role.
	Information Asset Administrators/Assistants	The Information Asset Administrators/Assistants role is to: • Ensure that policies and procedures are followed • Recognise potential or actual security incidents • Consult their IAO on incident management • Ensure that information assets registers are accurate and maintained up to date.

	Requirement	Detail
		Information Asset Owners have received specialist information risk training to allow them to be effective in their role.
	Employment Contracts	All staff and those undertaking work on behalf of the ICB need to be aware that they must meet Information Governance requirements and it is made clear to them that breaching these requirements, e.g., service user confidentiality, is a serious disciplinary offence. This is supported by the inclusion of clauses within staff contracts both for substantive and temporary staff that cover Information Governance standards and responsibilities regarding data protection, confidentiality, and information security.
	Contracts with Third Parties	The ICB must ensure that work conducted by others on their behalf meet all the required Information Governance standards. Where this work involves access to information about identifiable individuals it is likely that the ICB will be in breach of the law where appropriate requirements have not been specified in contracts and steps taken to ensure compliance with those requirements. Therefore, the ICB endeavours to ensure that formal contractual arrangements that include compliance with Information Governance

	Requirement	Detail
		requirements are in place with all contractors and support organisations.
Training and Guidance Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. The approach to ensuring that all staff receive training appropriate to their roles should be detailed.	**Information Governance Handbook**	Purpose of the Handbook: • To inform staff of the need and reasons for keeping information confidential • To inform staff about what is expected of them • To protect the organisation as an employer and as a user of confidential information The Handbook has been written to meet the requirements of: • The Data Protection Act 2018 • The UK General Data Protection Regulations 2021 • The Human Rights Act 1998 • The Computer Misuse Act 1990 • The Copyright Designs and Patents Act 1988 • A Guide to Confidentiality in Health and Social Care (NHS Digital) The Handbook has been produced to protect staff by making them aware of the correct procedures so that they do not inadvertently breach any of these requirements.

	Requirement	Detail
		If the Handbook is breached, then this may result in legal action against the individual and/or organisation as well as investigation in accordance with the organisation's disciplinary procedures.
	Training for all staff	All staff receive Induction training delivered face-to-face, which includes Information Governance. All staff are required to complete annual IG refresher training, which is conducted through ESR online.
	Specialist IG training	Specialist IG training is provided across the organisation for those staff that are given additional responsibility for IG within their areas. Specialist training includes: • Information Governance Leads and others • Caldicott Guardians and others • Senior Information Risk Owners and others • Information Asset Owners and Information Asset Administrators

	Requirement	Detail
Incident Management Clear guidance on incident management procedures should be documented and staff should be aware of their existence, where to find them, and how to implement them.	**Documented Procedures and Staff Awareness**	Incident Management in the ICB is covered in the following organisational policies and Procedures: • Information Governance, Data Protection and Security Policies • IG Handbook Staff awareness is raised through the following ways: • Staff Induction • Annual Information Governance Training • Specialist Training