NHS
Lancashire and
South Cumbria
Integrated Care Board

Information Governance and Data Security and Protection Policy

Ref:	Lancashire and South Cumbria ICB_Corp19
Version:	V3
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.
Supersedes:	V2
Author (inc. Job Title):	Information Governance Team mlcsu.ig@nhs.net / 01782 916875
Ratified by: (Name of responsible Committee)	Lancashire and South Cumbria Audit Committee
Cross reference to other Policies/Guidance	Information Governance Handbook Information Governance Staff Code of Conduct Anti-Virus Policy IT Acceptable Use Policy Asset Management Policy IT Encryption Policy IT Vulnerability Management Policy Network Security Policy User Account Management Policy Password Management Policy
Date of first issue and where published	1st July 2022 (website)
Date of Current Issue	January 2025
Date Current Issue Ratified:	18th December 2024
Review date:	18th December 2026
Target audience:	All staff, including temporary staff and contractors, working for or on behalf of the Lancashire & South Cumbria ICB

Action required	To read
Contact details for further information	Information Governance Team mlcsu.ig@nhs.net 01782 916875

Document Status

This is a controlled document. Whilst this document may be printed, the electronic version posted on Lancashire & South Cumbria 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.

Version Control

Policy Name: Information Governance & Data Security and Protection Policies			
Version	Valid From	Valid To	Comments
1.0	01/07/2022	18/12/2024	Full review for new ICB organisation
2.0	19/12/2024	18/12/2026	Full review and approved by Audit Committee

Contents

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.
Commissioning Support Unit	CSU	A Commissioning Support Unit (CSU) is an Organisation. Commissioning Support Units provide ICBs with external support, specialist skills and knowledge to support them in their role as commissioners, for example by providing Business intelligence services.
Code of Conduct	CoC	A set of rules to guide behaviours and decisions in a specified situation.
Continuing Healthcare	CHC	Continuing Healthcare 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.
Common Law		The law derived from decisions of the courts, rather than Acts of Parliament or other legislation.
Care Quality Commission	CQC	This is an organisation funded by the Government to check all hospitals, Primary Care, and other health and care providers in England are meeting government standards and to share their findings with the public.
Corporate Records		Records which relate to the corporate business of the ICB such as accounts, minutes and meeting papers and 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.
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	A legally binding agreement outlining the responsibilities of the Data Controller and the Data Processor when a Data Processor is appointed on behalf of a Data Controller.
Data Protection Act 2018	DPA18	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 UK GDPR requirements.
Data Protection Officer	DPO	A role with responsibility 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 or DSP Toolkit	The Data Security Protection Toolkit is an online self-assessment tool that allows organisations that have access to NHS patient data and systems to provide assurance that they are practising good data security, and that personal data is handled correctly.
Data Subject		An identified or identifiable living individual to whom personal data relates.
Data Sharing Agreement	DSA	A non-legally binding agreement outlining the information that Data Controllers agree to share and the terms under which the sharing will take place.
Freedom of Information Act 2000	FOI	The Freedom of Information Act 2000 provides public access to information held by public authorities
Health Records		Records which consist of information relating to the physical or mental health of an individual and has been made by or on behalf of a health professional in connection with that care.
Information Asset Administrator	IAA	Information Asset Administrators work with the Information Asset Owners to implement the Information Risk Work Programme, updating the information asset registers and data flow maps, and ensuring policies are being properly adhered to.
Information Asset Owner	IAO	Information Asset Owners are directly accountable to the Senior Information Risk Owner and must provide assurance that information risk is being managed effectively in respect of the information assets that they ‘own’.
Information Assets		Includes records and documents that contain key information to the organisation’s business.

Information Commissioner’s Office	ICO	The Information Commissioner’s Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
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 Partnerships	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 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 System	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.
Individual Funding Requests	IFR	Application to fund treatment or service not routinely offered by NHS.
Key Performance Indicators	KPIs	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.
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.
Record 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		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.

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 institution to recognise the value of its information, 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.
United Kingdom General Data Protection Regulation	UK GDPR/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 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 Data Security and Protection or Information Governance 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. It is important that Information governance and data security and protection is not treated as an isolated subject but instead is part of the holistic approach which should be applied to data security and protection. This means that influences and policies from other disciplines such as Digital, Cyber, Human Resources, Procurement/Contracting and Communications and Engagement (this in a not an exhaustive list) should be referred to also in harmonisation with Information Governance policies and procedures.

Introduction

Information is a very useful to an organisation, but it is important that organisations have robust arrangements for Information Governance (IG) in place that are reviewed annually as described in the Data Security and Protection Toolkit (DSPT).

It is of paramount importance to ensure that 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 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 & Social Care Act 2022 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 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) is the retained EU law version of the General Data Protection Regulation 2016 which became directly applicable as law in the UK in 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 is underpinned by several data protection principles which drive compliance.

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

1. Lawful, fair, and transparent processing,
2. Purpose limitation,
3. Data minimisation,
4. Accurate and up to date,
5. Kept for no longer than necessary,
6. Appropriate security measures,
7. Accountability and liability.

Caldicott Principles

The Caldicott Principles, first introduced in 1997, amended in 2013, and then further amended with an additional Principle in 2020, are guidelines applied widely across the field of health and social care information governance 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 - Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users.
- **Principle 8:** Inform the expectations of patients and service users about how their confidential information is to be used – Steps should be taken to ensure no surprises for patients and service users about how and why their confidential information is used, and what choices they have about this.

Appointment of Data Protection Officer

It is an essential requirement of UK GDPR/DPA18 that the organisation has a Data Protection Officer (DPO) who will ensure the provisions of the UK GDPR are fully adhered to.

The ICB is required to designate a Data Protection Officer as it is likely to be processing personal and sensitive information on a large scale.

The Data Protection Officer contact details should be made available for those who may wish to raise queries or issues such as in fair processing notices.

The UK GDPR/DPA18 suggests that organisations should involve the Data Protection Officer in all issues which relate to the protection of personal data; so it is therefore crucial that the Data Protection Officer is involved from the earliest stage possible when considering new projects or changes to existing projects requiring a level of data protection.

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

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.

Responsibilities:

Organisation (Accountable Officer)

The ICB accountable officer is the Chief Executive Officer and has overall accountability for information governance requirements across the organisation and overall responsibility for establishing and maintaining an effective document management system and the governance of information, meeting statutory requirements and adhering to guidance.

Senior Information Risk Owner

The Senior Information Risk Owner (SIRO), 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 Senior Information Risk Owner.

Caldicott Guardian

The Lancashire and South Cumbria ICB Caldicott Guardian 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.

Data Protection Officer

The Data Protection Officer role includes compliance responsibility for UK GDPR/DPA18, FOIA and Data Protection.

Organisations should continue to ensure that the Head of Information Governance, 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 Information Governance Team in a timely manner to allow them to provide adequate advice.
- The opinion of the Information Governance Team 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 Data Protection Officer's or Information Governance Team's advice.
- The Data Protection Officer/ Information Governance Team must be promptly consulted once a data breach or another incident has occurred.

The UK GDPR/DPA18 requires that the organisation support the Data Protection Officer 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 Data Protection Officer 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 Data Protection Officer team.

Information Asset Owners

Information Asset Owners (IAOs) 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 Senior Information Risk Owner.
- Ensure there is a legal basis for processing and for any disclosures.
- Refer queries about any of the above to the Head of Information Governance.

Information Asset Administrators

The role of Information Asset Administrator (IAA) 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.

Users

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 Information Governance Handbook/Code of Conduct. The IT policies are as follows:

Anti-Virus Policy,
IT Acceptable Use Policy,
Asset Management Policy,
IT Encryption Policy,
IT Vulnerability Management Policy,
Network Security Policy,
User Account Management Policy,
Password Management Policy.

Audit Committee

The Audit Committee is responsible for considering, approving and ratifying the policies in respect of information governance on behalf of the ICB, Subsequently the Audit Committee will oversee the assurance of compliance with information governance standards and the approved ICB policy and the Data Security and Protection Toolkit.

Information Governance Team

The Information Governance Team 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 to the team who handle freedom of information and subject access requests,
- Providing support to Caldicott Guardians and Senior Information Risk Officer for information governance issues.

Information Governance Training

All staff are mandated to undertake information governance training within 1 working week where possible and should not be accessing personal data until this has been actioned, staff will undertake the Information Governance refresher module online or where appropriate a bespoke training offer that is recognised as a suitable alternative.

All new employees to the ICB are also required to attend an Information Governance Induction, read the Information Governance Handbook, and read and sign the Information Governance Code of Conduct (CoC) as part of their induction process. Staff should liaise with their Line Manager if they have any queries regarding this.

Data Security and Protection Toolkit

The Data Security and Protection Toolkit (DSP Toolkit) forms part of a framework for assuring that organisations are meeting their statutory obligations on data protection and data security. The DSP Toolkit is aligned to the National Cyber Security Centre's Cyber Assessment Framework (CAF). The DSP Toolkit is designed to:

1. Emphasise good decision-making over compliance,

2. Support a culture of evaluation and improvement.

3. Create opportunities for better practice.

When considering data security as part of the well-led element of their inspections, the Care Quality Commission (CQC) will look at how organisations are assuring themselves in relation to data security and protection.

The Data Security Protection Toolkit requirements in alignment to the Cyber Assurance Framework are as follows.

Within the requirements of the toolkit there are 46 spanning 18 principles across 5 objectives.

Objective	Principles
Objective A – Managing Risk	A1 – Governance A2 – Risk Management A3 – Asset management A4 – Supply chain

Objective B – Protecting against cyber-attack and data breaches	B1 – Policies, processes and procedures B2 – Identity and access control B3 – Data security B4 – System security B5 – Resilient networks and systems B6 – Staff awareness and training
Objective C – Detecting cyber security events	C1 – Security monitoring C2 – Proactive security event discovery
Objective D – Minimising the impact of incidents	D1 – Response and recovery planning D2 – Lessons learned
Objective E – Using and sharing information appropriately	E1 – Transparency E2 – Upholding the rights of individuals E3 – Using and sharing information E4 – Records management

This policy is one of a number that help the ICB meet their information governance, data security and protection obligations. When read in conjunction with the other policies below they provide a framework bringing 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.

Policy Review

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

Data Protection Policy

Introduction

Lancashire & South Cumbria ICB needs to collect personal confidential information about Data Subjects with whom it deals in order to carry out its business and provide its services for healthcare. Such Data Subjects include patients/service users, employees (present, past and prospective), suppliers and other business contacts. This information can include 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 processed in compliance with UK GDPR/DPA18.

The lawful and proper treatment of personal information by the ICB is extremely important to the success of the business and in order to maintain the confidence of Data Subjects. The ICB must ensure that personal information is held lawfully and correctly and in line with this policy.

Data Protection Principles

There are 7 Data Protection Principles within the DPA18. These are set out below:

> **Lawful, fair and transparent processing** – this principle emphasises transparency for all UK data subjects. As part of the lawfulness, the ICB must also be able to identify a legal basis for the processing of personal data. This means, it must be able to justify why the personal data is being processed in accordance with the legal basis within UK GDPR (Article 6). Where special category data (such as health data) is also being processed an additional legal basis under UK GDPR Article 9 also needs to be identified.
>
> 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.
>
> **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.
>
> **Data minimisation** – this principle instructs organisations to ensure the data they capture is adequate, relevant and not excessive. Currently, 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.
>
> **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.

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.

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 excuse under UK GDPR/DPA18, so organisations must spend an adequate amount of resource 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 – this principle ensures that organisations can demonstrate compliance. ensure compliance, organisations must be sure that every step within the UK GDPR strategy 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 remove 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.

Compliance

All staff, including temporary staff and contractors, working for or on behalf of the Lancashire and South Cumbria ICB must comply with the following:

- The Data Principles set out above.
- Provide clear information to Data Subjects about the purpose(s) for which their information will be used.
- Only process relevant and adequate personal data.
- Keep personal data accurate and up to date.
- Retain personal data only for as long as necessary.
- Respect individual's rights in relation to their personal data.
- Keep all personal data, in whatever format, secure.
- Employ appropriate technical and organisational security measures to safeguard personal information.
- Only transfer information outside the UK in circumstance where it can be adequately protected.
- Ensure that third party processors of personal data have adequate controls and security measures in place and are appropriately documented.
- Report all data breaches and/or incidents (including near misses) to the Information Governance Team upon discovery and act upon any mitigations to minimise the adverse impact(s).

- Where personal data is being processed, to consider the need for information governance documentation including but not limited to Data Protection Impact Assessments (DPIAs), Data Processing Agreement (DPA), Data Sharing Agreements (DSA), Data Protection Assurance Checklists (DPAC), updates to privacy notices and liaise with the Information Governance Team.

Retention of Data

Personal data should not be kept longer than is necessary for the purpose it was obtained. This means that data should be destroyed or erased from ICB systems when it is no longer required. For further information see the Records Management Policy.

Data Subjects' Rights

Under the DPA18, Data Subjects have several rights available to them set out as follows:

1. **The right to be informed –** Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.
2. **The right of access** – Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
3. **The right to rectification** – Enables individuals to have inaccurate personal data rectified, or completed, if it is incomplete.
4. **The right of erasure** – enables individuals to have personal data erased.
5. **The right to restrict processing –** enables individuals to request the restriction or suppression of their personal data.
6. **The right to data portability** – enables individuals to obtain and reuse their personal data for their own purposes across different services.
7. **The right to object –** enables individuals to object to the processing of their personal data in certain circumstances.
8. **Rights related to automated decision-making including profiling** – enables individuals to not be subject to a decision based solely on automated processing, including profiling

Only some of the above rights are absolute and others will only be applicable dependent on the legal basis (reason) for processing.

Security

Personal data should be always kept secure. The ICB must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. The DPA18 requires the ICB to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Where personal data is to be transferred to a third-party data processor, the third-party data processor should comply with those procedures and policies or have in place their own adequate controls and security measures which meet the requirements of the ICB.

Please refer to the ICB's IT/cyber security policies around information security.

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 2021 and NHS England's Corporate Records Retention and Disposal Schedule 2019 which provide 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.

Lancashire and South Cumbria ICB has a statutory obligation to maintain accurate records of their activities and to decide 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.

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.

Record of Processing Activities

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

- Purposes of the processing,
- Description of the data processed,
- Details of who we may send any 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.

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. A major reason that 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 Records Management Code of Practice for Health and Social Care 2021. Where a record does not align with the Records Management Code of Practice than a localised retention schedule should be created in collaboration with the Information Governance Team.

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.

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.

Records of Commissioned Services That Are Discontinued

The ICB should not agree to store records for other providers whom we are not the data controller for e.g. previously commissioned services that are to be discontinued/no longer contracted. It is the responsibility of the Data Controller (the Provider of the service) to find a solution for their records and this should be properly documented in the Data Protection Impact Assessment and associated contract and/or Data Sharing/Processing Agreement.

The ICB is unable to act as a repository for stranded records because the ICB has no:

- Justification (legal basis) for holding the records and should not be processing personal data in relation to these records.
- Dedicated resource for managing the records, including responding to Subject Access Requests.

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 applies only to living persons but there are limited rights of access to personal 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. A third party, e.g., solicitor, may also make a valid SAR on behalf of an individual with their permission.

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

Scope

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.

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.

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 medical records"
- "I am a solicitor acting on behalf of my client and request a copy of their medical record (an appropriate authority is enclosed)"

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.

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 person, 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 must be provided by the third party.

(Freedom of Information - FOI)

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, Lancashire and South Cumbria 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.

The ICB remains committed to promote a culture of openness and accountability to enable individuals to have a greater understanding of how the ICB's duties are carried out, and how they make decisions and how they spend public money.

The FOI Act 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.

Refusal of Requests

Lancashire & South Cumbria 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, of 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 mlcsu.foiteam@nhs.net

Time Limits for Compliance with Requests

The ICB has a statutory obligation to comply with the Freedom of Information 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 20 working days informing the applicant of this decision.

Network and IT Security Policies

IT Provider Policies

The following policies are in place and are available from the Lancashire and South Cumbria IT provider, that being Blackpool Teaching Hospitals Trust, upon request.

- Anti-Virus Policy,
- IT Acceptable Use Policy,
- Asset Management Policy,
- IT Encryption Policy,
- IT Vulnerability Management Policy,
- Network Security Policy,
- User Account Management Policy,
- Password Management Policy.

Registration Authority Policy and Procedure

NHS Midlands and Lancashire Commissioning Support Unit provide Registration Authority services to Lancashire and South Cumbria ICB and the Local Registration Authority Policy is available upon request.

Appendix A

Information Governance Management Framework (IGMF)

	Requirement	Detail
Senior Roles within the ICB	**Chief Executive Officer:** Kevin Lavery Chief Executive	The Chief Executive 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 Information Governance Lead: Asim Patel Chief Digital Officer **Deputy Senior Information Risk Owner** Joe McGuigan Director of Digital Operations and Assurance	The Senior Information Risk Owner (SIRO) is an Executive Director of the ICB Board. The Senior Information Risk Owner is expected to understand how the strategic business goals of the ICB may be impacted by information risks. The Senior Information Risk Owner 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 Senior Information Risk Owner 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 the Information Governance Team and the Caldicott Guardian, although ownership of the Information Risk Agenda will remain with the Senior Information Risk Owner. The Senior Information Risk Owner

	Requirement	Detail
		will be supported through a network of Information Asset Owners and Assistants who have been identified and trained throughout the organisation. The Senior Information Risk Owner is also appointed to act as the overall Information Governance lead for the ICB and co-ordinate the Information Governance work programme. The Executive Information Governance 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 Information Governance lead is accountable for ensuring effective management, accountability, compliance, and assurance for all aspects of Information Governance, although the key tasks are likely to be delegated to an Operational Information Governance Lead.
	Caldicott Guardian: David Levy ICB Medical Director **Deputy Caldicott Guardian:** Sarah O'Brien Chief Nursing Officer	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 confidentiality requirements and issues are represented at Board level and within the ICB's overall governance framework.

	Requirement	Detail
	Data Protection Officer: Hayley Gidman - Head of Information Governance	The Data Protection Officer (DPO) reports to the Senior Information Risk Owner. This ensures the Data Protection Officer can act independently, without a conflict of interest and report directly to the highest management level. The Data Protection Officer is responsible for ensuring that the ICB and its constituent business areas always remain compliant with data protection, privacy and electronic communications regulations, freedom of information act and the environment information regulations. The Data Protection Officer 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.
Key Governance Bodies A group, or groups, with appropriate authority should have responsibility for the Information Governance agenda.	**Audit Committee**	To provide assurance to the Board that there is an effective framework in place for the management of risks associated with information governance. To receive assurance on Information Governance compliance (including uptake and completion of data security training), data breaches and any related issues and risks. To review the adequacy of the annual Senior Information Risk Owner (SIRO) report, the submission for the Data Security and Protection Toolkit and relevant policies, reports and action plans. To ensure the adequacy of audits to assess information and IT security arrangements, including the annual Data Security and Protection Toolkit audit.

	Requirement	Detail
Resources Details of key staff roles	**Dedicated Information Governance Staff**	Senior Information Governance Consultant Name: Bronwyn Casey Email: bronwyn.casey@nhs.net Information Governance Consultant Name: Ken Douglas Email: Ken.Douglas2@nhs.net Senior Information Governance Officer Name: Lucie Jones Email: lucie.jones9@nhs.net Strategic Information Governance Lead Name: Charlotte Mountford Email: charlotte.mountford@nhs.net Head of Information Governance Name: Hayley Gidman Email: Hayley.gidman@nhs.net Information Governance Hub – first point of contact for queries Email: mlcsu.ig@nhs.net Tel: 01782 916875
Governance Framework Details of how responsibility and accountability for Information Governance 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 Senior Information Risk Owner 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.

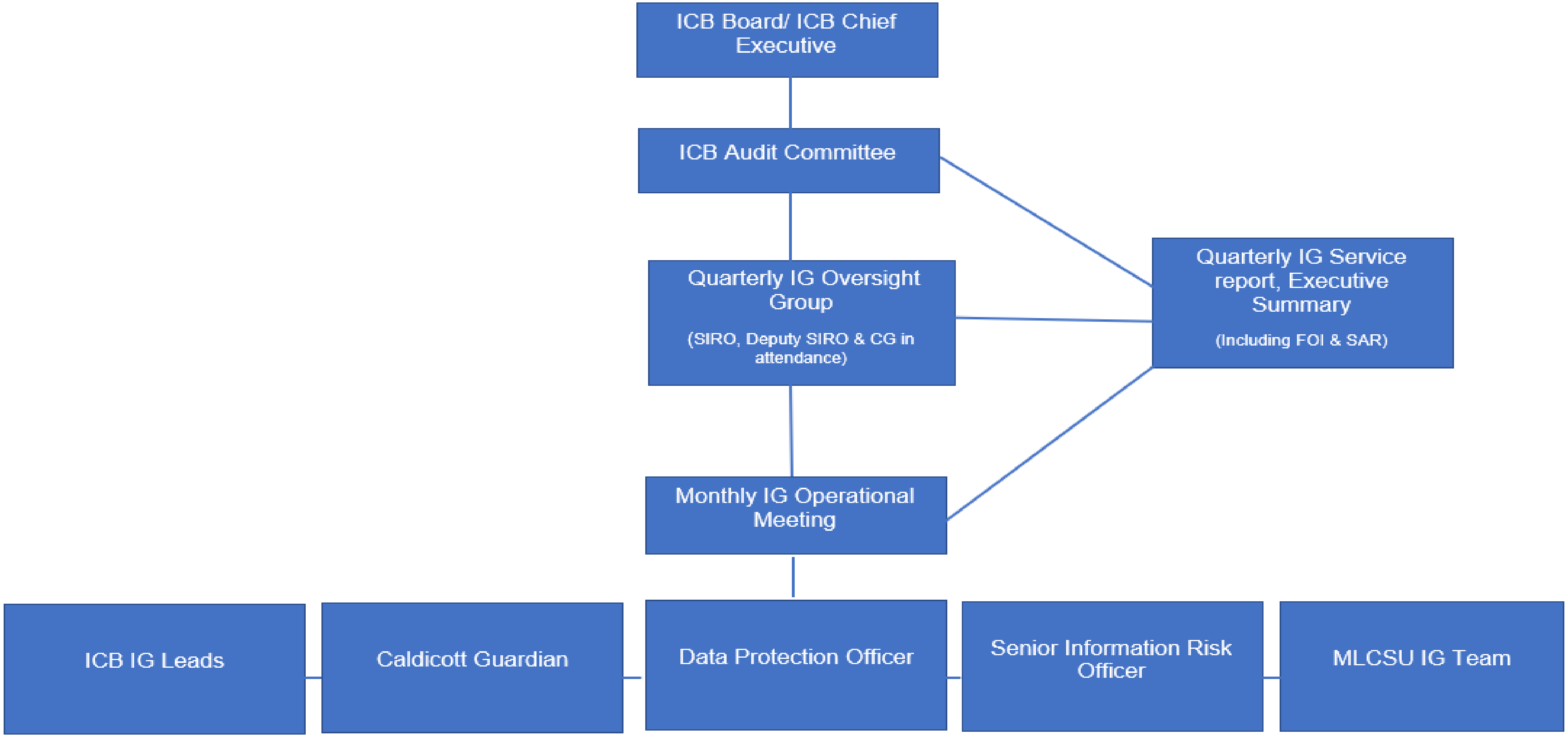
	Requirement	Detail
	Information Asset Administrators/Assistants	The Information Asset Administrators/Assistants' role is to: • Ensure that policies and procedures are followed, • Recognise potential or actual security incidents, • Consult their IAO on incident management, • Ensure that information assets registers are accurate and maintained up to date. 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, results in disciplinary proceedings in accordance with the organisation's policies. 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 meets 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.

	Requirement	Detail
		Therefore, the ICB endeavors to ensure that formal contractual arrangements that include compliance with information governance 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 Information Governance Handbook: • To inform staff of the need and reasons for keeping information confidential, • To inform staff about what is expected of them and how to implement this, • To protect the organisation as an employer and as a user of confidential information. The Information Governance Handbook was 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 Information Governance 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. If the Information Governance Handbook is breached, then this may result in legal action against the individual and/or organisation as well as investigation in accordance with

	Requirement	Detail
		the organisation's disciplinary procedures.
	Training for all staff	All staff receive basic Information Governance Induction training delivered online by the Information Governance Team via Teams. Annual Information Governance refresher training will then be conducted through ESR online.
	Specialist Information Governance training	Specialist Information Governance training is provided across the organisation for those staff that are given additional responsibility within their areas. Current specialist training includes: • Information Risk Training, • DPIA, • FOI, • SAR, • Breaches. Specialist training of dedicated Information Governance roles is also provided for the following: • SIRO, • Caldicott Guardian.
Data Incident Management Clear guidance on incident management procedures should be documented and staff	**Documented Procedures and Staff Awareness**	**Incident Management in the ICB is covered in the Information Governance Handbook** Staff awareness is raised through the following ways:

	Requirement	Detail
should be aware of their existence, where to find them, and how to implement them.		• Staff Induction, • Information Governance Training, • Specialist Training, • Newsletters and Communications.

Information Governance Management Framework



ICB Board/ ICB Chief Executive

ICB Audit Committee

Quarterly IG Oversight Group

(SIRO, Deputy SIRO & CG in attendance)

Quarterly IG Service report, Executive Summary

(Including FOI & SAR)

Monthly IG Operational Meeting

ICB IG Leads

Caldicott Guardian

Data Protection Officer

Senior Information Risk Officer

MLCSU IG Team