NHS
Nottingham and Nottinghamshire
Integrated Care Board

Information Governance Management Framework

March 2025 - March 2028

CONTROL RECORD	
Title	Information Governance Management Framework
Reference Number	IG-001
Version	3.0
Status	Final
Author	Head of Information Governance
Sponsor	Director of Corporate Affairs
Team	Information Governance Team
Amendments	Reviewed to ensure accessibility requirements met.
Purpose	Ensures compliance with legal and regulatory requirements, defines roles and responsibilities, standardises policies and procedures, mitigates risks, promotes staff awareness, enables secure information sharing, and provides assurance that data is managed lawfully, securely, and effectively.
Superseded Documents	N/A
Audience	All staff within the NHS Nottingham and Nottinghamshire Integrated Care Board, including those working in a temporary capacity.
Consulted with	Information Governance Steering Group
Equality Impact Assessment	N/A
Approving Body	Audit and Risk Committee
Date approved	March 2025
Date of Issue	April 2025
Review Date	March 2028
This is a controlled document and whilst this policy may be printed, the electronic version available on the ICB's document management system is the only true copy. As a controlled document, this document should not be saved onto local or network drives.	

NHS Nottingham and Nottinghamshire Integrated Care Board (ICB's) policies can be made available on request in a range of languages, large print, Braille, audio, electronic and other accessible formats from the Engagement and Communications Team at nnicb-nn.comms@nhs.net.

Contents

1. Introduction

1.1 Information governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. It provides a consistent way for employees to deal with the many different information handling requirements including:

- Information governance management.
- Clinical information assurance for safe patient care.
- Confidentiality and data protection assurance.
- Corporate information assurance.
- Information security assurance.
- Secondary use assurance.
- Respecting data subjects' rights regarding the processing of their personal data.

1.2 NHS Nottingham and Nottinghamshire ICB's Information Governance Management Framework (IGMF) provides a structured approach to managing information governance activities. It ensures compliance with relevant legislation and standards, identifies and mitigates information risks, and outlines accountability for information governance. The framework promotes continuous improvement, includes training and awareness programs, and establishes procedures for incident management, ultimately supporting the secure and effective handling of patient data and enhancing the quality of commissioned services.

1.3 The Information Governance Management Framework (IGMF) ensures compliance with key legal requirements, including the Data Protection Act 2018, the UK General Data Protection Regulation (UK GDPR) 2016, the Common Law Duty of Confidence, the Human Rights Act 1998, and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

It also aligns with the NHS Data Security and Protection Toolkit (DSPT) and the National Cyber Security Centre's Cyber Assessment Framework (CAF). By adhering to these regulations and frameworks, the IGMF ensures that the ICB manages information securely, protects patient confidentiality, and meets all statutory and regulatory obligations.

2. Purpose

2.1 To outline the strategic framework for managing and supporting the information governance agenda of the ICB. The IGMF provides a solid basis upon which information governance and all its component parts will be implemented throughout the ICB.

2.2. To describe the roles and responsibilities of those who are tasked with overseeing that information governance is appropriately supported and to describe the information governance responsibilities of all staff.

2.3. The ICB will ensure:

- Regulatory and legislative requirements will be met.
- Confidentiality of information will be assured.
- Information will be protected against unauthorised access.
- Quality and integrity of information will be maintained.
- Business continuity plans will be produced, maintained and tested.
- Information governance training will be available to all staff.
- All information governance breaches, actual or suspected, will be reported to, and investigated by the Information Governance Team, in conjunction with the Data Protection Officer.
- The mandatory requirements of the annual CAF-aligned Data Security and Protection Toolkit are met.

2.4. To inform and support staff to protect the organisation’s essential functions through effective information asset management.

2.5 To help ensure that the ICB can demonstrate personal data is:

- Held securely and confidentially.
- Processed fairly and lawfully.
- Obtained for specific purpose(s).
- Recorded accurately and reliably.
- Used effectively and ethically.
- Shared and disclosed appropriately and lawfully.

3. Scope

3.1 This Information Governance Management Framework applies to:

- All staff – This includes all individuals employed by the ICB and those working within the ICB in a temporary capacity, including agency staff; seconded staff; students and trainees; self-employed consultants or other individuals working for the ICB under contract for services individuals appointed to the Integrated Care Board and its Committees and any other individual directly involved with the business or decision-making of the ICB.

- Systems – ICB systems include, but are not limited to, discrete systems such as those holding information relating to patients, finance, risk, complaints, incidents, corporate records, human resources and payroll; less technical systems such as excel spreadsheets held on the network, and paper-based systems such as complaints files.
- Information – All information processed (electronic and paper based) in relation to any ICB activity whether by employees or other individuals or organisations under a contractual relationship with the ICB.
- Networks – the infrastructure that provides the means to connect computers, servers and devices to facilitate communications and the sharing of data.

4 Information Governance Policy and Strategy Framework

4.1 The ICB has a number of key policy and strategy to ensure that compliance with all relevant legal and regulatory frameworks is achieved, monitored, and maintained. These are outlined in the table below:

Document	**Description**
ICB Policies	
Confidentiality and Data Protection Policy (IG-002)	Sets out the roles and responsibilities for compliance with the Data Protection Act and lays down the principles that must be observed by all who work within the ICB and have access to personal or confidential business information in line with common law obligations of confidentiality and the NHS Confidentiality Code of Practice.
Information Security Policy (IG-003)	This policy is to protect, to a consistently high standard, all information assets. The policy defines security measures applied through technology and encompasses the expected behaviour of those who manage information within the organisation.
Internet and Email Policy (IG-004)	Ensures ICB staff understand their responsibilities for correctly accessing the internet and understand what the ICB deems to be acceptable use of the email system via the organisation's IT systems, while on ICB premises, working remotely and when acting in representation of the organisation.
Data Quality Policy (IG-005)	Sets out a clear policy framework for maintaining and increasing high levels of data quality within the ICB in order to ensure reliable, complete and accurate data for analysis and decision-making and which is in line with data protection and other legislation and standards.
Records Management Policy (IG-009)	Promotes the effective management and use of information, recognising its value and importance as a resource for the delivery of corporate and service objectives.

Document	Description
Freedom of Information Policy (IG-010)	Sets out the roles and responsibilities for compliance with the Freedom of Information Act and Environmental Information Regulations.
Risk Management Policy (GOV-001)	Describes the ICB's approach to the management of strategic and operational risks specifically including information risks across the ICB. It references the SIRO's role in information risk management.
Incident Reporting and Management Policy (H&S 004)	Describes the approach to the reporting, management and investigation of all corporate incidents (including accidents and near misses) that occur within the ICB including data security and other Information Governance incidents.
Emergency Planning and Preparedness Policy (EPRR-001)	Outlines how the ICB will have plans and arrangements in place to act in accordance with the Civil Contingencies Act 2014 (CCA), the Health and Social Care Act 2012 (H&SCA) and to comply with the requirements of the NHS England EPRR Core Standards, links into business continuity which is closely connected to information security and the protection of essential functions.
Nottinghamshire Health Informatics Services (NHIS) Policies *(required to be followed by ICB staff)*	
Network Security Policy	
Account Management and Access Policy	
Removable Media Policy	
Registration Authority Policy	
Audit Logging and Monitoring Policy	
Strategies	
Nottingham and Nottinghamshire ICS Cyber Security Strategy	
Digital, Data and Technology Strategy Digital Notts Strategy I Digital, Data & Technology (DDaT)	

5 Roles and Responsibilities

5.1 Senior level ownership and understanding of information risk management is vital and ensures a clear link to the overall risk management culture of the organisation. Senior leadership demonstrates the importance of the issue and is critical for ensuring information security remains high on the agenda of the ICB and that resource requirements needed to support this agenda are understood.

The table below provides high level descriptions of the information governance responsibilities within the ICB and more detailed descriptions for the key roles can be found at **Appendix A.**

Role	Responsibilities
Board	The Board has overall responsibility for ensuring that the ICB complies with information governance standards, including the protection of data in accordance with all relevant legislation. It is also responsible for overseeing development and implementation of a comprehensive cyber security strategy, ensuring the resilience of digital infrastructure against evolving cyber threats.
Audit and Risk Committee	The Audit and Risk Committee is responsible for overseeing the ICB's compliance with the regulatory requirements for information governance (including data protection and cyber security).
Information Governance Steering Group	The Information Governance Steering Group (IGSG) has operational responsibility for developing, monitoring, and implementing comprehensive and effective information governance arrangements within the organisation. The IGSG drives the information governance agenda within the ICB and provides a focal point for the discussion and resolution of information governance risks and issues.
Chief Executive	The Chief Executive is accountable for ensuring the ICB adheres to information governance, data protection and cybersecurity standards, driving a culture of compliance and risk management across the ICB.
Senior Information Risk Owner (SIRO)	The SIRO operates at Board level and is responsible for ensuring that organisational information risk is properly identified and managed, and that appropriate assurance mechanisms exist to support the effective management of information risk.
Caldicott Guardian	The Caldicott Guardian operates at Board level and is responsible for ensuring that personal information and patient information in particular is used legally, ethically and appropriately, and that confidentiality is maintained.
Data Protection Officer (DPO)	The Data Protection Officer has a direct reporting line to the ICB's Board and will assist in the monitoring of internal compliance, inform and advise on data protection obligations and risks, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner's Office. The ICB will ensure that the Data Protection Officer has sufficient support to carry out their role independently, ensuring that they are not penalised for performing their tasks. *Article 38 of the GDPR provides that the controller and the processor shall ensure that the DPO is 'involved, properly and in a timely manner, in all issues which relate to the protection of personal data'.* *Article 39(1)(b) entrusts DPOs with the duty to monitor compliance with the GDPR. Recital 97 further specifies that the DPO 'should*

Role	Responsibilities
	assist the controller or the processor to monitor internal compliance with this Regulation.
Chief Digital Officer *supported by IT function and Nottinghamshire Health Informatics Service (NHIS)*	The Chief Digital Officer is responsible for leading the development and execution of the ICB's digital strategy, ensuring that cybersecurity is integrated into all digital initiatives and innovations. They work to align digital transformation with robust security frameworks, safeguarding systems, data and infrastructure from emerging cyber threats.
Director of Corporate Affairs *supported by the Risk, Information and Assurance Team*	The Director of Corporate Affairs advises the Board on information governance matters, ensuring that polices related to data protection, transparency and accountability are effectively communicated and adhered to across the ICB. They also oversee compliance with legal and regulatory requirements.
Information Asset Owners (IAOs) *(Executive / Senior Leadership Level)*	Information Asset Owners (IAOs) are responsible for ensuring that information assets under their control are managed securely, in compliance with data protection and information governance policies. They oversee the use, protection and retention of data, ensuring that risks are mitigated and access is appropriately controlled.
Information Asset Managers (IAMs) *aka. Information Asset Administrators (IAAs)*	Information Asset Managers are responsible for the data integrity of applications, user access including auditing of access, ensuring that there are appropriate operational procedures that include backup, business continuity planning. They liaise with system suppliers, where appropriate, to ensure that the asset is maintained and 'fit for purpose'. IAMs are responsible for ensuring their asset information is up to date on the ICB's Information Asset Register (IAR).
All staff	All staff, as defined by the scope of the IGMF, must be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, and information security management and information quality. This is cascaded through employment contracts, third party contracts, policy and processes and staff awareness and training.
Information Governance Team	The IG Team develops and delivers the Information Governance Annual Work Plan and supports key roles like the SIRO, Caldicott Guardian, and DPO. Their main responsibilities include: • Ensuring compliance with information governance targets, data protection, Caldicott principles, and information security. • Implementing robust security and encryption for electronic resources.

Role	Responsibilities
	• Managing records storage, archiving, and security for personal data. • Mapping personal information flows and maintaining a register of information assets. • Identifying and reporting information governance risks. • Providing advice on information governance, data protection, and related legislation. • Developing and maintaining documentation and policies. • Delivering communications and training to staff. • Supporting the Information Governance Steering Group (IGSG). • Advising on tendering and procurement processes to ensure robust information governance.
Corporate Assurance Team	The Corporate Assurance Team is responsible for ensuring compliance with NHS corporate record standards, managing corporate records, and overseeing Freedom of Information (FOI) process. They also handle policy management, ensuring that all ICB policies are up-to-date, accessible, and aligned with legal and regulatory requirements. The Corporate Assurance Team also project manages delivery of the CAF-aligned Data Security and Protection Toolkit.

6 Staff Awareness

6.1 The ICB has a robust Staff Training, Awareness and Communications Plan, which sets out how the ICB will ensure that all staff are appropriately trained and aware of their responsibilities regarding data security and protection. The plan serves as a strategic framework for raising awareness and promoting a culture of data security throughout the ICB and sets out the specific training requirements for staff across various roles within the organisation, ensuring staff are competent and well-equipped to handle personal and sensitive data securely, in compliance with relevant laws and guidelines.

6.2 The plan is supported by a comprehensive Training Needs Analysis (TNA). As part of this, all staff are mandated to complete data security awareness training on an annual basis.

6.3 Any individual who has comments regarding the content of this IGMF or has difficulty understanding how this framework relates to their role, should raise this with their line manager or contact the Information Governance team at: nnicb-nn.igteam@nhs.net

Appendix A: Key Role Descriptions

Senior Information Risk Owner (SIRO)	Caldicott Guardian
Accountability: Holding Information Asset Owners accountable for managing information assets and related risks. **Leadership:** Leading efforts to protect and use information effectively for the success of the Integrated Care Board (ICB) and its population. **Security Oversight:** Overseeing assurance of information governance and cyber security compliance among commissioned service providers. **Advisory Role:** Advising the ICB on information risk, system-wide issues, performance, and conformance with risk management requirements. **Policy Ownership:** Owning and ensuring consistent implementation of the ICB's information risk policy and risk assessment processes. **Incident Management**: Owning the ICB's information incident management framework and ensuring effective communication and execution of risk management approaches. **Governance Advice:** Providing written advice to the Chief Executive on information risk for the Annual Governance Statement. **Incident Response:** Establishing mechanisms for responding to and reporting serious information governance incidents. **Collaboration:** Working closely with the Caldicott Guardian, Head of Information Governance, and Data Protection Officer. **Training:** Undertaking Information Risk management training and maintaining knowledge of the organisation's business, goals, and essential functions.	**Championing Information Governance (IG):** Advocate for IG requirements and confidentiality issues at the Integrated Care Board level. **Organisational Conscience:** Act as the 'conscience' of the ICB, enabling appropriate information sharing while ensuring ethical practices. **Policy Integration:** Ensure confidentiality issues are reflected in ICBal strategies, policies, and staff procedures. **Leadership and Guidance:** Provide leadership and informed guidance on complex matters involving confidentiality and information sharing. **Oversight of Information Sharing:** Oversee arrangements, protocols, and procedures for sharing confidential personal information with external bodies, including those responsible for social care and safeguarding. **Collaboration:** Work closely with the Senior Information Risk Owner, Head of Information Governance, and Data Protection Officer. **Data Security Standards:** Have oversight of the implementation of the National Data Guardian's 10 Data Security Standards. **Training and Knowledge:** Undertake biennial training and maintain strong knowledge of confidentiality and data protection matters. **Ethical Use of Data:** Ensure that personal confidential data is handled legally, ethically, and responsibly1. **Strategic Role:** Represent and champion information governance issues at senior management and board levels. **Compliance with Caldicott Principles**: Apply the eight Caldicott Principles wisely, ensuring high standards for handling person-identifiable information. **Support for Digital Systems**: Play a key role in the governance of information management and technology, especially in the implementation of digital and paperless systems.

Appendix A: Key Role Descriptions

Data Protection Officer (DPO)	Information Asset Owner (IAO)
Monitoring Compliance: Assist with monitoring internal compliance with GDPR and other data protection laws, as well as internal and local data protection policies. Raise awareness on relevant data protection topics, ensure adequate and appropriate training for staff, and participate in relevant audits. **Advisory Role:** Inform and advise staff and Integrated Care Board (ICB) management on data protection obligations. **DPIA Guidance**: Provide advice regarding Data Protection Impact Assessments (DPIAs). **Contact Point:** Act as a contact point for data subjects and the Information Commissioner's Office. **Risk Consideration:** Consider information risks associated with processing operations, taking into account the nature, scope, context, and purposes of processing by the organisation. **Accountability:** Help demonstrate compliance as part of an enhanced focus on accountability. **Collaboration:** Work closely with the Caldicott Guardian, Information Governance Team, and Senior Information Risk Owner. **Knowledge Maintenance:** Ensure expert knowledge is kept up to date with relevant changes to legislation, national policy, and guidance. **Incident Management:** Oversee the information incident management framework, ensuring effective communication and execution of risk management approaches.	**Leadership and Culture:** Lead and foster a culture that values, protects, and uses information for the success of the Integrated Care Board (ICB) and the benefit of its population, while maintaining individuals' data protection and confidentiality rights. **Data Flow Understanding:** Understand the nature and justification of data flows, including personal data, to and from information assets and systems. **Access Management:** Know who has logical access to the asset or system and ensure that access is monitored and compliant with relevant legislation and guidance. **Risk Identification:** Identify and understand information assets and systems, address risks, and provide assurance to the Senior Information Risk Owner (SIRO). **Collaboration:** Liaise with the Information Governance Team to update and maintain the Information Asset and Data Flow Mapping Registers, either directly or through nominated Information Asset Managers. **Incident Response**: Participate in the response to information governance incidents, ensuring that appropriate measures are taken to mitigate risks.