NHS
Nottingham and Nottinghamshire
Clinical Commissioning Group

Information Governance Management Framework

2021-2023

Version:	2.0
Approved by:	Governing Body
Date approved:	December 2021
Date of issue (uploaded to Website):	December 2021
Next review date:	June 2023
Document author:	Head of Information Governance

CONTROL RECORD			
Reference Number IG-001	**Version** 2.0	**Status** Final	**Author** Head of Information Governance
			Sponsor Associate Director of Governance
			Team Information Governance
Title	Information Governance Management Framework		
Amendments	Review for Data Security and Protection Toolkit assertions changes.		
Purpose	To outline the strategic framework for managing the information governance agenda across the Nottingham and Nottinghamshire CCG. To meet the Data Security and Protection Toolkit assertions.		
Superseded Documents	Version 1.2		
Audience	All employees of the Nottingham and Nottinghamshire CCG (including all individuals working within the CCG in a temporary capacity, agency staff, seconded staff, students and trainees, and any self-employed consultants or other individuals working for the CCG under contract for services), individuals appointed to the Governing Body, Committees and any other individual directly involved with the business or decision making of the CCG.		
Consulted with	Audit and Governance Committee		
Equality Impact Assessment	Not required for Framework		
Approving Body	Governing Body	**Date approved**	December 2021
Date of Issue	December 2021		
Review Date	June 2023		
This is a controlled document and whilst this policy may be printed, the electronic version available on the CCG's document management system is the only true copy. As a controlled document, this document should not be saved onto local or network drives.			

Nottingham and Nottinghamshire CCG'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 nnccg.team.communications@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. The Information Governance Management Framework (IGMF) outlines how the information governance agenda will be addressed by the aligned Nottingham and Nottinghamshire CCG (the CCG).

1.3. The IGMF is based upon the legal requirements of the Data Protection Act 2018, the General Data Protection Regulation 2016, the Common Law Duty of Confidence, the Human Rights Act 1998, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and the NHS Data Security and Protection Toolkit (DSPT) which is based on the National Data Guardian's 10 Data Security standards.

2. Purpose

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

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 CCG 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 Data Security and Protection Toolkit will be met.

2.4. To inform staff to maximise the organisational information assets by ensuring that the CCG 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 CCG and those working within the CCG in a temporary capacity, including agency staff, seconded staff, students and trainees, and any self-employed consultants or other individuals working for the CCG under contract for services), individuals appointed to the Governing Body and its Committees and any other individual directly involved with the business or decision-making of the CCG.
- **Systems** – CCG systems include, but are not limited to, discrete systems such as those holding information relating to patients, finance, risk, complaints, incidents, freedom of information 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 CCG activity whether by employees or other individuals or organisations under a contractual relationship with the CCG. All such information belongs to the CCG unless proven otherwise.

4. Policies

4.1. The CCG will establish and maintain policies to ensure that compliance with all relevant legal and regulatory frameworks is achieved, monitored, and maintained.

4.2. The following table sets out the CCG policies supporting the IGMF.

Policies	**Description**
Confidentiality and Data Protection Policy	This policy 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 CCG and have access to personal or confidential business information in line with common law obligations of confidentiality and the NHS Confidentiality Code of Practice.
Freedom of Information Policy	This policy sets out the roles and responsibilities for compliance with the Freedom of Information Act and Environmental Information Regulations.
Information Security Policy	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.
Records Management Policy	This policy is to promote the effective management and use of information, recognising its value and importance as a resource for the delivery of corporate and service objectives.

5. Roles and Responsibilities

5.1. Overview

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 Governing Body and that resource requirements needed to support this agenda are understood.

The following sections provide high level descriptions of the information governance responsibilities within the CCG and more detailed descriptions for the key roles can be found at **Appendix A**.

5.2. Governance and Accountability

Organisational Roles	Responsibilities
The CCG's Governing Body	Ultimate accountability for information governance rests with the CCG's Governing Body; which must ensure that it receives an appropriate level of assurance in relation to the information governance duties that are delegated to the Information Governance Steering Group and key officers. It must ensure that: Details of serious incidents requiring investigation (SIRIs) involving actual loss of personal data or breach of confidentiality are published in the CCG's annual reports and reported in line with national notification guidance and data protection legislation. Any shortfalls in meeting the requirements of the Data Security and Protection Toolkit are addressed
The Audit and Governance Committee	The Audit and Governance Committee, as a subcommittee of the Governing Body, approves Information Governance policies and receive updates on IG performance, legal compliance as well as risks and serious incidents. The SIRO is an attendee of the Audit and Governance Committee and is responsible for updating the Governing Body on IG matters.

The Information Governance Steering Group	The Information Governance Steering Group is accountable to the Governing Body through the Audit and Governance Committee and will oversee the extent to which the principles and primary objectives of information governance are embedded within the CCG. This will include through a comprehensive work plan monitoring progress towards achieving full compliance with the requirements of the Data Security and Protection Toolkit and GDPR.
The Accountable Officer	The Accountable Officer has overall responsibility for the CCG's Information Governance Management Framework.

Individual Roles	Responsibilities
Senior Information Risk Owner (SIRO)	The SIRO operates at Governing Body 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. The SIRO is supported by a Deputy SIRO, who is nominated to provide advice and assurance to the SIRO in relation to their key areas of responsibility.
Caldicott Guardian	The Caldicott Guardian operates at Governing Body 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. The Caldicott Guardian is supported by a Deputy Caldicott Guardian, nominated to provide resilience to the CCG in the delivery of this function.

Data Protection Officer (DPO)	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 assist the controller or the processor to monitor internal compliance with this Regulation’. The Data Protection Officer has a direct reporting line to the CCG’s Governing Body and will assist in the monitoring of internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the Information Commissioner’s Office. The CCG 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.
Associate Director of Governance	The Associate Director of Governance has lead management responsibility for ensuring that robust arrangements are in place with regard to information governance. This role is supported in the delivery of the Information Governance Annual Work Plan by the Information Governance Team and Corporate Governance Team (see sections 5.3 and 5.4).
Information Asset Owners (IAOs)	Senior staff at Executive Director/Director and/or Deputy Director/Head of Department level will be required to act as Information Asset Owners as relevant to the information assets within their remit. They are directly accountable to the SIRO and will provide assurance that information risk is managed effectively for the information assets within their remit.
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 mandatory and role based training.

5.3. Information Governance Team

The Information Governance Team is responsible for development and delivery of the Information Governance Annual Work Plan. The Team is also responsible for supporting the SIRO, Caldicott Guardian and DPO in the delivery of their responsibilities.

The Team's key responsibilities include:

- Ensuring that the CCG meets the required information governance targets and expectations, both internal and external, specifically bringing together through the Information Governance Annual Work Plan, obligations and best practice in data protection, Caldicott principles, information lifecycle management and information security.
- Ensuring that the Data Security and Protection Toolkit submissions are completed and reported to the Audit and Governance Committee for approval.
- Ensuring robust security of electronic resources and encryption is implemented in line with Department of Health and Social Care guidelines set out by NHS Digital and NHSx and relevant local policies.
- Ensuring appropriate records storage, archiving and security arrangements for data.
- Ensuring that the CCG complies with the requirements for mapping personal information flows.
- Identifying and reporting information governance risks.
- Providing advice and guidance on all aspects of information governance and on all matters related to the Data Protection Act 2018 and other related privacy legislation.
- Developing and maintaining comprehensive and appropriate documentation that demonstrates commitment to, and ownership of, information governance responsibilities, such as IGMF and associated policies and procedures.
- Ensuring that appropriate training is available to all staff and delivered in line with mandatory requirements.
- Maintaining a level of expertise required in order to provide guidance to staff.

- Ensuring (through implementation of the IGMF and associated information governance policies) that all staff understand their personal responsibilities for information governance.

- Supporting the Information Governance Steering Group (IGSG) to discharge its information governance responsibilities.

- Providing advice and guidance to commissioning staff regarding tendering and procurement processes to ensure that all services and contracted services have robust information governance arrangements in place.

- Periodically reviewing the CCG’s inventory of information assets.

5.4. Corporate Governance Team

The Corporate Governance Team is responsible for ensuring compliance with the Freedom of Information Act 2000 and the NHSx Records Management Code of Practice 2021.

6. Communication, Monitoring and Review

6.1. The CCG will establish effective arrangements for communicating the requirements of this policy and will provide guidance and support to line management in relation to their responsibilities.

6.2. This IGMF will be monitored and maintained and on an annual basis reviewed by the IGSG.

6.3. The CCG’s Governing Body will be responsible for the scrutiny and approval of the IGMF. Once approved the IGMF will be submitted to the Governing Body for assurance.

6.4. Any individual who has queries regarding the content of this IGMF, or has difficulty understanding how this framework relates to their role, should contact the Information Governance Team.

7. Staff Training

7.1. As a minimum, all staff will need to complete the e-Learning for Healthcare Data Security Awareness Level 1 training module on an annual basis, maintaining compliance at all times. At least 95% of all staff will have completed their training in the period set out annually in the DSPT (currently between 1 July to 30 June).

7.2. The Information Governance Team will review training needs analysis on an annual basis to identify specific data security and protection training required for the key roles (documented in Section 5) supporting the information governance agenda.

8. References

- Information Commissioner's Office.
- National Information Governance Board for Health and Social Care.
- NHS England Information Governance Operating Model 2020-2022.
- NHS Care Record Guarantee.
- Data Protection Act 2018.
- EU General Data Protection Regulation 2016.
- NHS Act 2006
- Health and Social Care Act 2012
- Heath and Social Care (National Data Guardian) Act 2018
- Data Security and Protection Toolkit (NHS Digital)
- Records Management Code of Practice 2021. (NHSx Data Policy Hub 2021)
- Guide to the Notification of Data Security and Protection Incidents. (NHS Digital 2018)
- Data Handling Review (Cabinet Office 2012).
- NHS Information Risk Management (Department of Health 2009).
- Information Security Management: Code of Practice (Department of Health 2007).
- Heath and Social Care (National Data Guardian) Act 2018
- 'Caldicott 2' Review 'To share or not to share' (2013).
- Confidentiality: NHS Code of Practice (Department of Health 2003).
- National Data Guardian's Review of Data Security, Consent and Opt-Outs (2016).
- Guide to Confidentiality (NHS Digital 2013)
- Manual for Caldicott Guardians (UK Caldicott Guardian Council).

Appendix A:

Key Role Descriptions

Role of the Senior Information Risk Owner (SIRO)

The SIRO is responsible for:

- The management of information risk within the organisation.
- Holding Information Asset Owners to account for the management of information assets and related risks and issues.
- Leading and fostering a culture that values, protects, and uses information for the success of the CCG and benefit of its population.
- Ensuring that information and cyber security are dealt with at the highest level of management.
- Overseeing assurance in respect of commissioned service providers' information governance and cyber security compliance.
- Advising the Governing Body on information risk, system-wide issues, performance, and conformance with information risk management requirements and recommend mitigation.
- Owning the CCG's overall information risk policy and risk assessment processes, ensuring they are implemented consistently by Information Asset Owners and agreeing action in respect of any organisational risks.
- Owning the CCG's information incident management framework, ensuring that the CCG's approach to information risk management is effective in terms of clear lines of responsibility and accountability, resources, commitment and execution and that this approach is communicated to all staff.
- Providing written advice to the Accountable Officer on the content of their Annual Governance Statement in regard to information risk.
- Ensuring that effective mechanisms are established and publicised for responding to and reporting perceived or actual serious information governance incidents.
- Working closely with the Caldicott Guardian, Head of Information Governance and Data Protection Officer.
- The SIRO is also required to undertake Information Risk management training at least annually and must maintain sufficient knowledge and experience of the Partnership's business and goals with particular emphasis on the use of and dependency upon internal and external information assets.

Role of the Caldicott Guardian

The Caldicott Guardian is responsible for:

- Championing IG requirements and confidentiality issues at Governing Body level.
- Acting as both the ‘conscience’ of the organisation and as an enabler for appropriate information sharing.
- Ensuring that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff.
- Provide leadership and informed guidance on complex matters involving confidentiality and information sharing
- Overseeing all arrangements, protocols and procedures where confidential personal information may be shared with external bodies and others with responsibilities for social care and safeguarding.
- Working closely with the Senior Information Risk Owner, Head of Information Governance and Data Protection Officer.
- Having oversight of the implementation of the National Data Guardian’s 10 Data Security Standards.
- The Caldicott Guardian is also required to maintain a strong knowledge of confidentiality and data protection matters.

Role of the Data Protection Officer (DPO)

The Data Protection Officer is responsible for:

- Assisting with monitoring internal compliance with the GDPR and other data protection laws, our data protection policies, awareness-raising, training, and audits.
- Informing and advising on data protection obligations.
- Providing advice regarding Data Protection Impact Assessments (DPIAs).
- Acting as a contact point for data subjects and the Information Commissioner’s Office.
- Having regard to the risk associated with processing operations, and take into account the nature, scope, context and purposes of processing by the organisation when carrying out its duties.
- Helping to demonstrate compliance as part of an enhanced focus on accountability.
- Working closely with the Caldicott Guardian, Information Governance Team and Senior Information Risk Owner.

Role of the Information Asset Owner (IAO)

Information Asset Owners are responsible for:

- Leading and fostering a culture that values, protects, and uses information for the success of the CCG and for the benefit of its population while maintaining individual’s data protection and confidentiality rights.

- Understanding the nature and justification of data flows (including personal data) to and from information assets/systems.

- Knowing who has logical access to the asset/system.

- Ensuring access to the information asset or system is monitored and compliant with relevant legislation and guidance.

- Identifying and understanding their information assets/systems and identify and addressing risks and providing assurance to the SIRO.

- Liaising with the Information Governance Team to update and maintain the Information Asset and Data Flow Mapping Registers.

- Completing relevant training as require for their IAO role.