GB 18 083h

NHS Rushcliffe Clinical Commissioning Group
NHS Nottingham City Clinical Commissioning Group
NHS Nottingham North and East Clinical Commissioning Group
NHS Nottingham West Clinical Commissioning Group

Information Governance Management Framework

July 2018 – June 2019

Version:	**0.1 (DRAFT)**
Approved by:	**CCG Governing Bodies**
Date approved:	**July 2018**
Date of issue (communicated to staff):	***Tbc***
Next review date:	**June 2019**
Document author:	**Head of Information Governance**

CONTROL RECORD				
Reference Number	**Version** 0.1	Status DRAFT	**Author** Head of Information Governance	
			Sponsor Corporate Director	
			Team Information Governance	
Title	Information Governance Management Framework			
Amendments	Amended to reflect the establishment of the Greater Nottingham Clinical Commissioning Partnership. Amended to reflect requirements of EU General Data Protection Regulation, Data Protection Act 1998 and Data Security and Protection Toolkit.			
Purpose	To outline the strategic framework for managing the information governance agenda within the Greater Nottingham Clinical Commissioning Partnership. To meet the Data Security and Protection Toolkit assertion 1.2.1.			
Superseded Documents	• NHS Nottingham City CCG IG Management Framework v1.4 • South Nottinghamshire CCGs IG Management Framework v5.4			
Audience	All employees of the four Greater Nottingham CCGs (including all individuals working within the CCGs in a temporary capacity, including agency staff, seconded staff, students and trainees, and any self-employed consultants or other individuals working for the CCGs under contract for services), individuals appointed to the Governing Bodies and their committees and any other individual directly involved with the business or decision-making of the CCGs.			
Consulted with	N/A			
Equality Impact Assessment				
Approving Body	Greater Nottingham CCGs' Governing Bodies	**Date approved**		
Date of issue				
Review Date				

Greater Nottingham Clinical Commissioning Partnership policies can be made available on request in a range of languages, large print, Braille, audio, electronic and other accessible formats from the Communications Team at ncccg.team.communications@nhs.net

Contents

1. Introduction

1.1. This Framework outlines how the information governance agenda will be addressed within NHS Nottingham City CCG, NHS Nottingham North and East CCG, NHS Nottingham West CCG and NHS Rushcliffe CCG (subsequently referred to in this document as **'the CCGs'**).

1.2. It is based upon the legal requirements of the Data Protection Act 2018, the Common Law Duty of Confidence, the Human Rights Act 1998 and the NHS Data Security and Protection Toolkit, which includes the National Data Guardian's ten data security standards.

1.3. It defines the CCGs' intention to provide assurance on all matters relating to information governance. The CCGs are committed to fulfilling all statutory and legal obligations in relation to information governance, particularly where personal, sensitive and confidential information is used, stored and created by the organisations.

1.4. This Framework is underpinned the CCGs' information governance policies, procedures and processes.

1.5. An annual self-assessment against the requirements of the Data Security and Protection Toolkit will be completed, which will enable the CCGs to plan and implement standards of best practice and to measure and report on compliance. The CCGs will aim to continuously comply with all of the mandatory Toolkit assertions as a minimum.

2. Purpose

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

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.

3. Scope

3.1. This Framework applies to:

- All staff – This includes all individuals employed by the CCGs and those working within the CCGs in a temporary capacity, including agency staff, seconded staff, students and trainees, and any self-employed consultants or other individuals working for the CCGs under contract for services), individuals appointed to the Governing Bodies and their committees and any other individual directly involved with the business or decision-making of the CCGs.

- Systems – CCGs' 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 CCGs. All information stored on facilities owned or managed by or on behalf of the CCGs. All such information belongs to the CCGs unless proven otherwise.

4. Definitions

4.1. The following table sets out the definitions of key terms used within this Framework.

Key Term	Definition
Information governance	Information governance is the way in which an organisation processes or handles information, including person-identifiable data, corporate information and business data.
Information asset	Identifiable and definable records/systems owned or contracted by an organisation which are 'valuable' to the business of that organisation.
Toolkit (previously known as Information Governance Toolkit, now Data Protection and Security Toolkit)	NHS Digital Self-Assessment tool for measuring and monitoring performance and compliance with key IG requirements, submitted at least annually to Department of Health/ NHS Digital.
Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

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 Bodies 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 CCGs and more detailed descriptions for the key roles can be found at **Appendix A**.

5.2. Governing Bodies

Ultimate accountability for information governance rests with the CCGs' Governing Bodies; each must ensure that they receive an appropriate level of assurance in relation to the information governance duties that are delegated to the IGMT Committee and key officers. In particular, each 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.

5.3. Information Governance Management and Technology Committee

The Information Governance Management and Technology (IGMT) Committee will oversee the extent to which the principles and primary objectives of information governance are embedded within the CCGs. This will include monitoring progress in achieving full compliance with the requirements of the Data Security and Protection Toolkit.

5.4. Accountable Officer

The Accountable Officer has overall responsibility for the CCGs' Information Governance Management Framework.

5.5. 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 Deputy SIROs, nominated to provide advice and assurance to the SIRO in relation to their key areas of responsibility.

5.6. **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 CCGs in the delivery of this function.

5.7. **Data Protection Officer (DPO)**

The Data Protection Officer has a direct reporting line to the CCGs' Governing Bodies 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 CCGs 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.

5.8. **Information Governance Team**

The Head of Information Governance leads an Information Governance Team that 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 CCGs meet 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 IGMT Committee for approval.
- Ensuring robust security of electronic resources and encryption is implemented in line with Department of Health guidelines and relevant local policies.
- Ensuring appropriate records storage, archiving and security arrangements.
- Ensuring that the CCGs comply with the requirements for mapping information flows and other records management initiatives.
- 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 legislation.

- Developing and maintaining comprehensive and appropriate documentation that demonstrates commitment to, and ownership of, information governance responsibilities, such as the Information Governance Management Framework 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 Information Governance Management Framework and associated information governance policies) that all staff understand their personal responsibilities for information governance.
- Supporting the IGMT Committee 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 CCGs' inventory of information assets.
- Ensuring compliance with the Freedom of Information Act 2000.

5.9. Information Asset Owner (IAO)

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.

5.10. All Staff

All staff as defined by the scope of this Framework must be aware of their own individual responsibilities for the maintenance of confidentiality, data protection, information security management and information quality.

6. Principles of Information Governance

6.1. Overview

The CCGs are committed to the four key principles of information governance, which are described within the following sections.

6.2. **Openness**

- Non-confidential information relating to the CCGs and the services they commission will be available to the public through a variety of media.
- The CCGs will establish and maintain policies to ensure compliance with the Freedom of Information Act 2000.
- Patients will have ready access to information relating to their own health care, their options for treatment, and their rights as patients.
- Clear information will be provided to patients and their families and carers about how their personal information is recorded, handled, stored, and shared.
- The CCGs recognise the need for an appropriate balance between openness and confidentiality in the management and use of information.

6.3. **Compliance with Legal and Regulatory Framework**

- The CCGs will establish and maintain policies to ensure that compliance with all relevant legal and regulatory frameworks is achieved, monitored, and maintained.
- The CCGs will regard all identifiable personal information relating to patients and staff as confidential, and as such, takes steps to ensure that the handling of such information complies with the Data Protection Act 2018 (except where there is a legal requirement to override the Act).
- The CCGs will establish and maintain policies and procedures for the controlled and appropriate sharing of patient information with other agencies, taking account of all relevant legislation. This will include the completion of Data Protection Impact Assessments for all new systems and services to determine whether there is any potential impact on information security, confidentiality, or integrity prior to implementation.
- The CCGs will ensure that the requirement for good information governance standards is embedded within all service specifications and contracts.

6.4. **Information Security**

- The CCGs will establish and maintain policies and procedures for the effective and secure management of its information assets and resources. This will include the maintenance of an Information Asset Register.
- The CCGs will establish robust arrangements for the assessment and management of information risks.
- The CCGs will ensure that its information technology provider has appropriate policies and procedures to ensure the maintenance, monitoring, and review of network security controls. These will include encryption controls, access

controls, anti-virus / malicious code detection, removal and prevention procedures, and environmental controls to protect network equipment.

- The CCGs will ensure that all flows of person-identifiable and sensitive information have been identified, mapped and risk assessed to confirm appropriateness and ensure security of the data transfer.
- The CCGs will ensure that business continuity plans are up to date and tested for all critical information assets to ensure that information required for operational purposes is held securely and is available to and able to be accessed by those who need it.
- The CCGs will maintain and review appropriate incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
- The CCGs will ensure the use of pseudonymised and anonymised data wherever possible for contract monitoring purposes.

6.5. **Information Quality Assurance**

- The CCGs will establish and maintain policies and procedures for information quality assurance and the effective management of records.
- The CCGs will ensure that information is organised and managed in accordance with mandated and statutory standards and kept confidential where appropriate.
- The integrity of information will be assured, monitored, and maintained, to ensure that it is of quality and reliable for use for the purposes that it is collected and used.

7. Communication, Monitoring and Review

7.1. This Framework will be reviewed on an annual basis and approved by the CCGs' Governing Bodies.

7.2. Compliance with the Framework will be monitored by the IGMT Committee, which will oversee the production and delivery of the Information Governance Annual Work Plan.

7.3. All supporting information governance policies outline their individual monitoring and review arrangements.

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

8. Staff Training

8.1. 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. At least 95% of all staff will have completed their training in the period 1 April to 31 March.

8.2. The Information Governance Team will undertake 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.

9. Equality and Diversity Statement

9.1. The CCGs are committed to commissioning services that embrace diversity and that promote equality of opportunity including the aims of the public sector equality duty.

9.2. As employers, the CCGs are committed to equality of opportunity and to valuing diversity within the workforce. The CCGs' goal is to ensure that these commitments are embedded in day-to-day working practices with our populations, colleagues and partners.

9.3. The CCGs will provide equality of opportunity and will not tolerate unlawful discrimination on grounds of age, disability, gender identity, marriage or civil partnership, pregnancy or maternity, race, religion or belief, sex, sexual orientation, or as a result of being any of the following: people with caring responsibilities', people experiencing economic and social deprivation, vulnerable migrants, homeless people, sex workers or gypsies and travelers.

10. References

- NHS Digital Data Security and Protection Toolkit 2018/19
- Data Protection Act 2018
- EU General Data Protection Regulation
- Draft NHS Digital Guide to the Notification of Data Security and Protection Incidents
- Information Commissioner's Office
- National Information Governance Board for Health and Social Care
- NHS Care Record Guarantee
- Data Handling Review (Cabinet Office 2012)
- Confidentiality: NHS Code of Practice (Department of Health 2003)
- Information Security Management: Code of Practice (Department of Health 2007)

- Health and Social Care Records Management Code of Practice (2016)
- NHS Information Risk Management (Digital Information Policy, DH, 2009)
- DH: NHS IG - Information Risk Management - Good Practice Guide 2009
- Caldicott2 Review ‘To share or not to share’ April 2013
- NHS Digital’s ‘A Guide to Confidentiality’ 2013
- Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation, May 2015
- Caldicott 3 Review
- NHS England Information Governance Operating Model 2016/17
- A Manual for Caldicott Guardians: Produced by the UK Caldicott Guardian Council 2017

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 CCGs and benefit of their populations.
- Ensuring that information and cyber security are dealt with at the highest level of management;
- Overseeing assurance in respect of commissioned service provider's information governance and cyber security compliance;
- Advising the Governing Bodies on information risk, system-wide issues, performance, and conformance with information risk management requirements and recommend mitigation;
- Owning the CCGs' 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 CCGs' information incident management framework, ensuring that the CCGs 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 Statements 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 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 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;
- 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, Head of Information Governance 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 CCGs and for the benefit of their populations;
- Understanding the nature and justification of information flows to and from information assets;
- Knowing who has logical access to the asset and why and whether it is a system or information;

- Ensuring access to the asset is monitored and compliant with relevant legislation and guidance;
- Identifying, understanding and addressing risks to their information assets, and providing assurance to the SIRO;
- Liaising with the Information Governance Team to update and maintain the Information Asset Register;
- Completing relevant training as required for the role.