NHS
Nottingham North and East
Clinical Commissioning Group

NHS
Nottingham West
Clinical Commissioning Group

NHS
Rushcliffe
Clinical Commissioning Group

Information Governance Management Framework

V5.4 FINAL

September 2017 – August 2018

CONTROL RECORD			
Reference Number IG33	**Version** 5.4	**Status** FINAL	**Author** Paul Gardner, Head of Information Governance
			Sponsor Andy Hall, Director of Outcomes and Information
Amendments	Adoption of NHS Nottingham City CCG's Information Governance Management Framework. Minor amendments to paragraphs 2.6, 4.2 and 5.5 to reflect changes in legislation and national guidance. Further minor changes to paragraphs 3.6 and 5.7 regarding delivery of training. Changes from Health and Social Care Information Centre (HSCIC) to NHS Digital (NHSD) and Information Governance training to Data Security Awareness Level 1 training.		
Purpose	To outline the strategic level framework for managing the Information Governance agenda within the organisation. To meet the Information Governance Toolkit requirements, standard 15-130.		
Audience	All staff, including CCG employees and non-CCG employees who work within the three South Nottinghamshire CCG's or under contract to them. This includes, but is not limited to, staff on secondment to the CCG, students on placement, and people working in a temporary capacity.		
Consulted with	Director of Corporate Development and Nottingham City CCG Senior Information Risk Owner. CCG IG Leads		
Equality Outcome Assessment	N/A		
Approving Body	IGMT Committee	**Date approved**	22 September 2017
Date of issue	September 2017		

Review Date	August 2018

The CCGs will do their utmost to support and develop equitable access to all policies and procedures. Therefore, any individual who requires access to this policy in another language or format (such as Braille or large print), can do so by contacting the CCGs' Governance Teams

Contents

1. Introduction

1.1. Information Governance (IG) is the way in which an organisation processes or handles information, including person-identifiable data, corporate information and business data. Information plays a key part in the CCGs' governance arrangements, and the quality of service planning, performance measurement, assurance and financial management relies upon accurate and available information.

1.2. Robust IG requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

1.3. This Information Governance Management Framework (IGMF) sets out how NHS Nottingham North and East, NHS Rushcliffe and NHS Nottingham West Clinical Commissioning Groups will deliver against these requirements.

1.4. Standards for IG and the management of information risk are incorporated into the NHS Information Governance Toolkit (IGT), which covers all aspects of information governance, including:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance
- Secondary Use Assurance
- Corporate Information Assurance

1.5. An annual self-assessment against the requirements of the IGT 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 achieve as a minimum a 'satisfactory' (level 2) assessment against all toolkit criteria, which represents legal and NHS requirements and best practice for handling personal and confidential information.

1.6. The CCGs will also aim to ensure that all organisations that they have contracted to provide clinical services also achieve a 'satisfactory' level of compliance with IGT requirements. This will be monitored via provider Quality Panels.

2. Scope

2.1. This Information Governance Management Framework applies to:

- **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 requests, 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 collected or accessed (electronic and paper based) in relation to any CCG activity whether by CCG employees or individuals and organisations under a contractual relationship with the CCGs and all information stored on facilities owned or managed by the CCGs or on behalf of the CCGs. All such information belongs to the CCGs unless proven otherwise.
- **Staff** - All staff, including CCG employees and non-CCG employees who work within NHS Nottingham North and East, NHS Rushcliffe and NHS Nottingham West Clinical Commissioning Groups or under contract to them. This includes, but is not limited to, staff on secondment to the CCGs, students on placement, and people working in a temporary capacity.

3. Principles of Information Governance

3.1. The four key strands to information governance are:

- Openness
- Legal compliance
- Information security
- Information quality assurance

3.2. The South Nottinghamshire CCGs recognise the need for an appropriate balance between openness and confidentiality in the management and use of information. The CCGs fully support the principles of corporate governance and recognise their public accountability, but equally place importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

3.3. The South Nottinghamshire CCGs also recognise the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest. This provides assurance that information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

3.4. The South Nottinghamshire CCGs believe that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision-making processes.

3.5. The South Nottinghamshire CCGs will establish and maintain policies and procedures to ensure compliance with requirements contained in the NHS Information Governance Toolkit.

3.6. It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability provide a robust governance framework for information management across the following legislation and work areas:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Information Security Standard: ISO/IEC 27002: 2005
- Information Security NHS Code of Practice
- Confidentiality NHS Code of Practice
- Health and Social Care Records Management Code of Practice 2016
- Caldicott Guidance (including the Caldicott2 Review ‘To Share or Not to Share’ 2013)
- NHS Digital’s ‘A Guide to Confidentiality’ 2013
- Public Records Act 1958
- Mental Capacity Act 2005
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- National guidance and best practice from the Information Commissioners Office

4. Strategic Aims

4.1. The aim of this Information Governance Management Framework is to set out how the CCGs will effectively manage Information Governance. The CCGs will achieve compliance through delivery of the following commitments:

4.2. **Openness**

- Non-confidential information relating to the South Nottinghamshire 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.

4.3. **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, take steps to ensure that the handling of such information complies with the Data Protection Act 1998 (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 Privacy 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.

4.4. **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 held locally by each CCG.
- Robust arrangements for the assessment and management of information risks will have been established.
- The CCGs will ensure that their 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 are committed to the use of pseudonymised and anonymised data wherever possible for contract monitoring purposes.

4.5. **Information Quality Assurance**

- The CCGs will establish and maintain policies and procedures for information quality assurance and the effective management of records.
- Information will be 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.

4.6. Staff Education, Training and Awareness

- The CCGs recognise that Information Governance education, training and awareness are essential for developing and improving staff members' Information Governance knowledge and skills. Data Security Awareness training must extend beyond basic confidentiality and security awareness in order to develop and follow best standards of practice. Staff need to understand the value of information and their responsibility for it, including data quality, information security, records management, confidentiality, legal duty, information law, rights of access and patients' rights in terms of a right of privacy and choice.
- Data Security Standard 3 in the Caldicott 3 Review requires that all staff undertake appropriate annual data security training and pass a mandatory test. Therefore, if non-permanent staff have access to personal information they also need to complete annual training.
- The CCGs have classified Data Security Awareness Level 1 training as mandatory for all staff, whether permanent, temporary or contracted. All new starters will be provided with Data Security Awareness Level 1 training as part of their induction programme, with refresher training being required on an annual basis. Training will mainly be delivered via ESR and NHS Digital's Online Training Tool. However, alternative training methods such as face-to-face sessions will be available on request.
- A training needs analysis will be completed in order to identify the additional training requirements specific to the roles set out below in Section 5.
- The CCGs are committed to sustaining an effective organisational culture through the provision of clear advice and increased awareness and promotion of information governance requirements. In addition to annual training, this will be achieved through ongoing staff briefings. This will highlight the importance of complying with the organisation's information governance policies, procedures and guidance, including the consequences of failing to comply.

5. Duties and Responsibilities

5.1. Key forums and individuals with overarching responsibility for addressing the Information Governance agenda are detailed below. Individuals responsible for specific information governance roles, such as data protection, information security and data quality, are detailed in the organisation's relevant information governance policies.

5.2. Governing Body

Ultimate accountability for Information Governance rests with each CCG's Governing Body, which must ensure that it receives an appropriate level of assurance in relation to the Information Governance duties that it has delegated to the Information Governance, Management and Technology Committee and key officers. In particular it must ensure that:

- Details of serious incidents requiring investigation involving actual loss of personal data or breach of confidentiality are published in the CCG's annual reports and reported to the Information Commissioner's Office in line with its national notification guidance. Serious incidents requiring investigation which are graded level 2 or above as per NHS Digital's '*Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation, May 2015*' must be reported via the IGT incident reporting tool.
- Any shortfalls in the requirements of the IGT are being addressed.

5.3. Information Governance, Management and Technology Committee (IGMT)

The Information Governance duties of the IGMT Committee are to:

1) Ensure that an appropriate comprehensive information governance framework and systems are in place throughout the constituent organisations in line with national standards.

2) Receive regular action plans with regard to the organisations' progress on the annual Information Governance Toolkit submission.

3) Ensure that information is effectively managed, and that appropriate policies, procedures and management accountability are provided and approved in relation to confidentiality, security and records management.

4) Ensure that information risks are identified, assessed and managed in line with the Information Governance Assurance Framework and recommend actions to the CCGs' Senior Information Risk Owners (SIRO) to ensure risks are mitigated.

5) Ensure that information incidents for commissioned services, including GP practices are identified and managed in line with National Serious Incident Framework, NHS England, March 2015. This will include incidents that result in a serious breach in confidentiality or data loss.

6) Assure the CCGs' Governing Bodies that all person identifiable information is processed in accordance with the Data Protection Act and that all staff are aware and comply with the NHS Code of Confidentiality and other professional codes of conduct.

7) Ensure that new or proposed changes to organisational processes or information assets are identified and risk assessed, considering any impact on information quality and identifying any new security measures that may be required.

8) Provide oversight and monitoring of provider IG Toolkit compliance on behalf of the CCGs, advising the relevant Quality Scrutiny Panels regarding any areas of concern.

9) Ensure that all locally-developed clinical information systems are accredited and signed off by the IM&T Clinical Safety Officer as laid out by statute and the relevant Information Standard Notices.

10) Receive regular compliance reports on the processing of Freedom of Information requests; determining exemptions as appropriate.

11) Develop an information governance training programme and monitor the progress of the staff training and awareness in line with the National Department of Health requirements.

12) Support the Caldicott function, working with the Caldicott Guardian to ensure work related to confidentiality and data protection is appropriately carried out and any risks reported appropriately.

13) Work with independent contractors and commissioned services to ensure their compliance with the Information Governance Toolkit.

5.4. Chief Officer

Locally, the Chief Officer has overall responsibility for each organisation's Information Governance Management Framework and has established the following management arrangements to ensure that it is implemented effectively.

5.5. Caldicott Guardian

The Caldicott Guardian is a senior clinician responsible for:

- Overseeing the development and implementation of those CCG policies and procedures designed to ensure that all routine use of person-identifiable information is identified, justified, documented and monitored.
- Overseeing the development and implementation of criteria and process for dealing with ad hoc requests for use of person-identifiable information for non-clinical purposes.
- Ensuring standard procedures and protocols are in place to govern access to person-identifiable patient information.

- Providing advice and guidance where required to the organisation's research and clinical audit processes and personnel to ensure protocols for releasing information for research and audit are in line with applicable Information Governance standards.
- Understanding and applying the principles of confidentiality and data protection as set out in the Confidentiality NHS Code of Practice and, where current practice falls short of the requirements, to agree challenging and achievable improvement plans.
- Have oversight of the implementation of the relevant recommendations as outlined in the Caldicott2 Review 'To Share or Not to Share' April 2013.

5.6. Senior Information Risk Owner (SIRO)

The SIRO is a Governing Body member responsible for ensuring that organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist to support the role of SIRO.

The SIRO's responsibilities can be summarised as:

- Leading and fostering a culture that values, protects and uses information for the success of the CCGs and benefit of their population/s.
- 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 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.
- Ensuring that effective mechanisms are established and publicised for responding to and reporting perceived or actual serious IG incidents.

The SIRO is required to undertake information risk management training at least annually to ensure their skills and capabilities are up to date and relevant to the needs of the CCG.

The SIRO is also required to maintain sufficient knowledge and experience of the CCG's business and goals with particular emphasis on the use of and dependency upon internal and external information assets.

5.7. Information Asset Owners (IAOs)

Information Asset Owners have been identified for each Information Asset. They will:

- Lead and foster a culture that values, protects and uses information for the success of the CCGs and for the benefit of their population/s.
- Understand the nature and justification of information flows to and from information assets, which will support ongoing work to identify flows of person identifiable information.
- Know who has logical access to the asset and why, whether it is a system or information, to ensure access is monitored and compliant with relevant legislation and guidance.
- Understand and address risks to the asset, and provide reporting and assurance to the SIRO.
- Complete and or attend training around information asset management and responsibilities.

5.8. Information Asset Support Staff

Traditionally the information asset management structure has IAO's supported by Information Asset Administrators (IAA's). IAA's would ordinarily be operational staff with day to day responsibility for managing risks to their information assets.

It is recognised that due to the small number of staff within the CCGs this structure of accountability would not necessarily work and therefore the key link will be between the SIRO and IAO's. However, where possible an IAA will be identified for each information asset.

The Head of Information Governance will provide an integrated information asset management risk report to the Information Governance, Management and Technology Committee annually.

IAO's will in any event seek support from staff within their area with regards to the day to day management of information assets.

5.9. Head of Information Governance

The Head of Information Governance leads the work within the Information Governance agenda, supported by the nominated Information Governance Lead within the CCGs. Together, they are responsible for ensuring the effective management, accountability, compliance and assurance for all aspects of Information Governance.

Key responsibilities include:

- Ensuring that IG targets and expectations, both internal and external, are met, specifically bringing together and prioritising work on initiatives including data protection, Caldicott principles, information lifecycle management, and information security.

- Ensuring robust security of electronic resources and encryption is implemented in line with DH guidelines and relevant local policies.
- Records storage, archiving and security, and ensuring that the organisation complies with the requirements for mapping information flows and other records management initiatives.
- Supporting the work of the Caldicott Guardian and the SIRO.
- Identifying and reporting Information Governance risks.
- Providing advice and guidance on all aspects of IG and on all matters related to the Data Protection Act and 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 deliver guidance and awareness to staff.
- Ensuring (through implementation of the Information Governance Management Framework and associated Information Governance policies) that all staff employed by the CCG (including agency staff, individuals on honorary contracts, management consultants and students who use and have access to information) understand their personal responsibilities for Information Governance and comply with the law.
- Ensuring that IGT returns are completed and reported to the IGMT Committee for approval.
- 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 in place.
- Periodically reviewing the CCGs’ inventory of information assets.

5.10. **All staff**

All staff, whether permanent, temporary or contracted, must be aware or their own individual responsibilities for the maintenance of confidentiality, data protection, information security management and information quality.

6. Supporting Policies

6.1. The Information Governance Management Framework is supported by, and should be read in conjunction with, the suite of Information Governance policies established by the CCG to provide comprehensive guidance on the Information Governance agenda and the responsibilities of its staff, including:

- Confidentiality and Data Protection Policy
- Information Security Policy
- Network Security Policy
- Records Management Policy
- Freedom of Information and Environmental Information Regulations Policy
- Electronic Remote Working Policy
- Internet and Electronic Mail Use Policy
- Incident Reporting and Management Policy / Serious Incident Reporting and Management Policy
- Data Quality Policy
- Access to Staff and Patient Information Using Smart Card Policy
- Safe Haven Policy

7. Monitoring and Review

7.1. This Information Governance Management Framework will be reviewed on an annual basis and ratified by the IGMT Committee. Compliance with the Information Governance Management Framework will be monitored by the IGMT Committee which will oversee the production and delivery of an annual improvement plan.

7.2. An annual report detailing levels of compliance will be presented to IGMT Committee.

7.3. All supporting Information Governance policies outline their individual monitoring and review arrangements.

8. References

- NHS Digital Information Governance Toolkit
- 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 (sets out responsibilities of SIROs, IAOs and IAAs)
- 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