NHS
North Yorkshire
Clinical Commissioning Group

Information Governance Framework and Strategy

November 2020

Authorship:	Senior Information Governance Officer, NECS
Committee Approved:	NHS North Yorkshire CCG Audit Committee
Approved date:	November 2020
Review Date:	November 2021
Equality Impact Assessment:	Yes
Sustainability Impact Assessment:	Yes
Target Audience:	Governing Body and its Committees and Sub-Committees, CCG Staff, agency and temporary staff & third parties under contract
Policy Number:	NY-204
Version Number:	1.1

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.1	Senior Information Governance Specialist	First Draft	IGSG (Nov 2020)	
0.2	Senior Information Governance Specialist	Second Draft revised for amendments from IG Steering Group		
1.0	Senior Information Governance Specialist		Approved by NHS North Yorkshire CCG Audit Committee (Nov 2020)	December 20
1.1	Senior Information Governance Specialist	Requirement for new starters to complete Data Security training within first week of starting employment	IGSG (May 2021)	May 2021

Contents

1.0 Introduction

Information is a vital asset within the CCG, in terms of the effective commissioning and management of services and resources. It plays a key part in clinical governance, service planning and performance management. It is important that information is managed within a framework that ensures it is appropriately managed and that policies, procedures, management accountability and structures are in place.

This strategy sets out the approach to be taken within the CCG to provide a robust Information Governance (IG) Framework and to fulfil its overall objectives. Information Governance requirement ensure that best practice is implemented and on-going awareness is evident across the CCG. The CCG is committed to ensuring that all records and information are dealt with legally, securely, efficiently and effectively.

Information Governance is a "framework for handling information in a confidential and secure manner to appropriate ethical and quality standards in modern health services". It brings together within a singular cohesive framework, the interdependent requirements and standards of practice. It is defined by the requirements within the Data Security & Protection Toolkit (DSPT) against which the CCG is required to publish an annual self-assessment of compliance. This strategy is supported by a DSPT Action Plan.

Within this agenda the CCG will handle and protect many classes of information:

- Some information is confidential because it contains personal details. The CCG must comply with regulation which regulates the holding and sharing of confidential personal information. Changes to the way in which patient confidential data can be processed came about as a result of the Health & Social Care Act 2012. It is important that relevant, timely and accurate information is available to those who are involved in the care of service users, but it is also important that personal information is not shared more widely than is necessary.
- Some information is non-confidential and is for the benefit of the CCG and the general public. The CCG and its employees share responsibility for ensuring that this type of information is accurate, up to date and easily accessible to the public.
- The majority of information about the CCG and its business should be open to public scrutiny although some, which is commercially sensitive, may need to be safeguarded.

2.0 Purpose

The Information Governance Framework will underpin the CCG's strategic goals and ensure that the information needed to support and deliver their implementation is readily available, accurate and understandable. Information Governance has four fundamental aims:

- To support the provision of high quality care by promoting the effective and appropriate use of information.
- To develop responsible staff who can work closely together, preventing duplication of effort and enabling efficient use of resources.

- To develop support arrangements and provide staff with appropriate tools and support to enable them to carry out their responsibilities to consistently high standards.
- Ensure the CCG understands its corporate IG responsibilities & requirements, its risks and mitigations.
- To enable the CCG to understand its own performance and manage improvement in a systematic and effective manner.

3.0 Definitions / Explanation of Terms

3.1 Personal information

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number, National Insurance number, pseudonymised data, biometric and genetic data, and online identifiers and location data, etc. Any data or combination of data and other information, which can indirectly identify the person, will also fall into this definition. Whenever possible, anonymised data, that is data where all personal details have been removed and which therefore cannot identify the individual, should be used. Note however that even anonymised information can only be used for justified purposes.

Information that identifies individuals personally must be regarded as confidential, and should not be used unless absolutely necessary. The appropriate legal basis under Article 6 of the General Data Protection Regulation must be identified and recorded in the CCG Information Asset Register to be able to legally process personal identifiable information.

3.2 Special Category Data

Special category data includes, Health Data, Trade Union membership, Political opinions, Religious or philosophical beliefs, Racial or Ethnic Origin, Sex life and sexual orientation, Biometric Data and Genetic Data.

In addition to having identified a legal basis under Article 6 of the General Data Protection Regulation to legally process personal identifiable information, to legally process special category information the CCG must identify the condition under Schedule 1 of the current Data Protection Act and the legal basis under Article 9(2) and record these on the information asset register.

3.3 Corporate Information

A corporate record is a record of activity within the CCG. This will include both information collected for business purposes and information created within the CCG, the processing of that information and reports produced from that information. Where this does not contain and is not linked to personal information no legal basis need be identified for processing purposes. However the CCG will need to consider whether this information is to be published into the public domain or whether it is corporately sensitive and implement controls to manage it appropriately.

3.4 Data Controller

A natural or legal person, public authority, agency or other body alone or jointly with others, determines the purposes and means of the processing of personal data.

3.5 Data Processor

A natural or legal person, public authority, agency or other body which processes data on behalf of the controller.

3.6 Processing

Any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by any means, alignment or combination, restriction, and destruction.

3.7 Information Formats

Information can be in many forms, including (but not limited to):

- Structured record systems – paper and electronic;
- Transmission of information –e-mail, post and telephone; and
- All information systems purchased, developed and managed by/or on behalf of the organisation.

3.8 Personal Data Breach

A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, or access to, personal data transmitted, stored or otherwise processed.

4.0 Scope of the Policy

The framework and strategy applies to NHS North Yorkshire CCG and all its employees and must be followed by all those who work for the organisation, including the Governing Body, those on temporary or honorary contracts, secondments, pool staff, contractors and students.

5.0 Duties, Accountabilities and Responsibilities

The CCG has developed clear lines of accountability with defined responsibilities and objectives.

5.1 Accountable Officer

The Accountable Officer has overall accountability and responsibility for IG across the CCG and is required to provide assurance, through the Annual Governance Statement, that all risks to the CCG are mitigated.

5.2 Audit Committee

The CCG Audit Committee has responsibility for overseeing and reporting to the Governing Body and for providing assurance on governance and risk management, IG, research governance and quality and diversity issues.

5.3 Information Governance Steering Group

The CCG has an Information Governance Steering Group (IGSG) which has responsibility for overseeing the implementation of this strategy. The IGSG reports to the CCG's Audit Committee.

5.4 SIRO

The Senior Information Risk Owner (SIRO) holds responsibility for ensuring that information is processed and held securely throughout the CCG. The role covers all the aspects of information risk, the confidentiality of patient and service user information and information sharing. The DSPT sets out clear responsibilities of the SIRO in relation to risks surrounding information and information systems, which also extend to business continuity and the role of Information Asset Owners. This Post is held by the Chief Finance Office

5.5 Caldicott Guardian

The Caldicott Guardian has an advisory role and is responsible for ensuring that the principles of confidentiality and data protection set out in the Caldicott Guidelines and the Data Protection Legislation are implemented systematically. This post is held by the Chief Nurse.

5.6 Corporate Services Manager (IG lead)

The Corporate Services Manager works with the North of England Commissioning Support Unit (NECS) IG Team to ensure systems are developed and implemented. The IG Lead is responsible for the co-ordination of the implementation of appropriate information governance processes and systems within the CCG and that these are fully documented and communicated to staff.

5.7 Line Managers

Line Managers are responsible for ensuring that their staff, both permanent and temporary are aware of:

- all information security policies and guidance and their responsibility to comply with them;
- their personal responsibilities in respect of information security;
- where to access advice on matters relating to security and confidentiality; and
- the security of physical environments where information is processed or stored.

5.8 All Staff

All members of staff have a responsibility to ensure they are aware of all information security policies and guidance and comply with them. Staff must be aware of their personal responsibility for the security and confidentiality of information which they use. Staff are responsible for reporting any possible or potential issues whereby a breach of security may occur

5.9 Data Protection Officer

The CCG is supported and advised by the Data Protection Officer (DPO) who assists the CCG to monitor internal compliance, informs and advises on our data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority. DPO for the CCG is provided externally by NECS.

5.10 Senior Information Governance Officer

The DPO is supported by the Senior Governance Officer (Information Governance) provided externally by NECS to provide IG expertise and will liaise directly with the responsible person within the CCG for specific issues and projects.

6.0 Responsibilities for Approval

Audit Committee is responsible for the review and approval of this Framework and Strategy.

7.0 Framework Procedural Requirements

7.1 Strategic Aims

The strategic aims will be achieved by ensuring the effective management of Information Governance by:

- Ensuring that the CCG meets its obligations under the Data Protection Act 2018, the Human Rights Act 1998, the Freedom of Information Act 2000 and the Health and Social Care Act 2012
- Ensuring that effective action planning is in place so that the CCG maintains GDPR compliance.
- Establishing, implementing and maintaining policies for the effective management of information.
- Ensuring that Information Governance is a cohesive element of the internal control systems within the CCG
- Recognising the need for an appropriate balance between openness and confidentiality in the management of information
- Ensuring that Information Governance is an integral part of the CCG culture and its operating systems (privacy by Design)
- Ensuring maintenance of year on year improvement within DSPT self assessment.
- Reducing duplication and looking at new ways of working effectively and efficiently

- Minimising the risk of breaches of personal data
- Minimising inappropriate uses of personal data
- Ensuring that Service Level Agreements and Data Sharing Agreements between the CCG and other organisations are managed and developed in accordance with IG principles
- Ensuring that contracted bodies are monitored against Information Governance standards
- Protecting the services, staff, reputation and finances of the CCG through the process of early identification of information risks and where these risks are identified ensuring sufficient risk assessment, risk control and management is undertaken
- Ensuring there is provision of sufficient training, instruction, supervision and information to enable all employees to operate within information governance requirements
- Ensuring that information governance is embedded within the CCG and monitored via regular checks
- Ensuring the CCG understands its processing activities including maintaining a record that details each use or sharing of personal information including the legal basis for the processing and if applicable, whether national data opt outs have been applied.
- Ensuring that a data security and protection breach reporting system is in place

8.0 Public Sector Equality Duty

In developing this policy an Equality Impact Analysis (EIA) has been undertaken. As a result of the analysis, the framework and strategy does not appear to have any adverse effects on people who share protected characteristics and no further actions are recommended at this stage.

NHS North Yorkshire CCG aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

9.0 Consultation

This Strategy and Framework has been reviewed by Information Governance Steering Group prior to approval by the Audit Committee.

10.0 Training

Training and education are key to the successful implementation of this framework and strategy and embedding a culture of IG management in the organisation. Staff will have the opportunity to develop more detailed knowledge and appreciation of the role of IG through:

- Policy/strategy
- Induction

- Line manager
- Specific training courses
- Statutory and Mandatory training workshops
- Information Asset Administrator and Information Asset Owner workshops
- Communications/updates from the IG Lead
- The IG Handbook

Mandatory training sessions will be delivered online via the NHS Digital (formerly the Health and Social Care Information Centre) Data Security Level 1 e-learning package. These sessions are mandatory and must be completed every year. Data Security Standard 3 within the Caldicott 3 review requires that all staff undertake appropriate annual data security training and pass a mandatory test. Therefore, non-permanent staff must also complete annual training.

Awareness will be monitored via regular checks and gaps in knowledge will be addressed via further bespoke training materials and/or targeted training sessions provided by the NECS IG service.

11.0 Monitoring Compliance with the Document

11.1 Data Security and Protection Toolkit

An updated action plan for improving and implementing the requirements of the DSPT will be submitted to the Information Governance Steering Group annually.

The CCG's progress will be reported to the Audit Committee at regular intervals by the SIRO. The action plan and monitoring will be via the Information Governance Steering Group.

The CCG will comply with the NHS Digital deadlines for submission of updates and the final data security and protection toolkit assessment.

Annual IG performance will be summarised in the Information Governance Annual Report.

An internal audit of the DSPT will be undertaken annually in quarter 4 of the financial year as part of the CCG's internal audit plan.

12.0 Arrangements for Review

This framework and strategy will be reviewed at least annually and in accordance with the following as and when required:

- legislative changes,
- good practice guidance,
- case law,
- significant incidents reported,

- new vulnerabilities, and
- changes to organisational infrastructure.

13.0 Dissemination

This Framework and Strategy will be published via the CCG Internet. All staff will be made aware of this via the CCG Newsletter.

The implementation of this Framework and Strategy is reflected through the completion of the DSP Toolkit and the confirmation of all mandatory assertions therein. It is also supported by a detailed reporting structure through the CCG's committees which are described in the Strategy. Directors and senior leads will be responsible for ensuring the Framework and Strategy is implemented in their areas of responsibility**.**

14.0 Associated Documentation

- Data Protection & Confidentiality Policy
- Confidentiality: Code of Conduct Policy
- Records Management policy
- Mobile working policy
- Information Security Policy
- Subject Access Request Policy
- Acceptable Computer Use Policy
- Email Policy
- IAO Role and Responsibilities
- Data Protection Impact Assessment

15.0 References

The Information Governance agenda encompasses the following areas:

- Caldicott and National Data Guardian Reports
- NHS Confidentiality Code of Practice
- *Data Protection Act 2018*
- *Freedom of Information Act 2000*
- *Health and Social Care Act 2012*
- *Human Rights Act 1998*
- *Care Act 2014*

16.0 Appendices

Appendix A: Information Governance Steering Group Terms of Reference.

17.0 Appendix A – Information Governance Steering Group Terms of Reference

Reviewed and Approved by:	Information Governance Steering Group (IGSG)
Review Date:	One Year from Approval
Ratified By:	NHS North Yorkshire CCG Audit Committee
Ratified Date :	29 April 2020

1. Role

Information Governance is the discipline which, through the means of a formal framework, robust practices and procedures for handling personal confidential and corporately sensitive information is implemented.

The Information Governance (IG) Steering Group has been established to oversee and monitor the implementation of the Clinical Commissioning Group (CCG) Information Governance Framework, including identifying lines of accountability and to ensure that information governance practices and procedures are embedded throughout the CCG.

The group's main role is:

- ensuring organisation-wide engagement in the Information Governance Agenda in line with NHS Digital Data Security and Protection Toolkit;
- ensuring that the Information Governance Assurance Framework is documented and embedded across the organisation;
- providing a local forum for Information Governance team leads, disseminating national guidance and best practice; and
- to receive concerns, issues and problems with a view to determining appropriate resolutions.

2. Remit

The Information Governance Steering Group will be the organisation's forum with delegated authority to oversee the implementation of Information Governance practices, resolution of issues, development and implementation of appropriate work plans, in order to provide appropriate assurance on behalf of the CCG.

The group will liaise closely with Commissioning Support Information Governance Team who co-ordinate operational Information Governance services on behalf of the organisation.

This will be achieved by the monitoring of key areas including;

- Confidentiality and Consent;
- Data Protection;
- Data Quality;

- Information Management;
- Information Disclosure and Sharing;
- Information Security;
- Records Management;
- Registration Authority and access control;
- Information Governance Incident Reporting and investigation; and
- Freedom of Information.
- Completion of Data Security and Protection Toolkit.

3. Specific Responsibilities

The group will achieve its remit through the following specific responsibilities:

- The review of Information Governance Policies, which will be ratified by the Audit Committee
- Ensuring that agreed information governance strategies, policies and procedures are embedded within the culture and practice of the organisation and adhered to;
- Cascade national guidance and advice;
- Lead on local implementation of guidance and advice;
- Receive and action the Data Protection Officers Report and other Information Governance performance reports produced by the Commissioning Support, Information Governance Team;
- Receive and review Information Governance policies and procedures;
- Ensuring that local operational leads are assigned for specific areas of the information governance agenda as appropriate, who will be responsible for providing evidence to support Data Security and Protection Toolkit compliance and reviewing and approving toolkit scores in their designated area(s);
- Receive reports of information governance incidents and take forward lessons learned resulting from the investigation of those incidents; and
- Monitoring compliance of statutory and mandatory training in respect of Information Governance
- Monitoring Registration Authority, Freedom of Information and Subject Access Requests compliance
- Completion of Data Flow Mapping and risk assessment.
- Monitoring of the Information Asset Register
- Review and ratification, alongside the SIRO and Information Asset Owners, of decisions to destroy records which have reached their retention period
- Monitoring implementation of IG requirements within the Contracting Process through the receipt of a sample of contract checklists for Primary Care and Acute services.
- Monitoring the completion of Data Protection Impact Assessments for new projects and services and actions required from the risk assessments.
- Monitoring of Primary Care completion of the Data Security and Protection Toolkit.

4. Reporting Arrangements and Administration

- Corporate Services Manager/ Information Governance Specialist are responsible for drafting the agenda with the support from the Secretariat.

- All papers submitted to the group should include a front sheet that indicates if they are for approval, assurance or discussion report.
- Executive Leads and report authors can assume that their reports have been read and that no verbal summary of these reports is needed. The Steering Group will proceed direct to questions, except when the report author wishes to advise the Committee about new or updated information or areas of concern.
- Key Messages of the Steering Group will be provided to the Audit Committee. The Chair of the Steering Group shall draw attention to any significant issues or risks relevant to that CCG.
- Papers must be circulated at least 5 working days prior to the meeting. Any urgent papers can be submitted with prior agreement with the Chair.

5. Accountability

The IG Steering Group is accountable to the Audit Committee and is authorised to:

- Investigate any activity within its terms of reference
- Seek any information it requires from any employee and all employees are directed to co-operate with any request made by the CCG. This remit extends to those working on any of the statutory bodies' behalf; and
- Co-ordinate and implement activities in line with these terms of reference, as part of the Information Governance work programme.
- Review and ratification, alongside the SIRO and Information Asset Owners, of decisions to destroy records which have reached their retention period.
- The review of Information Governance Policies for approval by the Audit Committee.
- The review of recommendations made by IG specialists to the group.
- Accountable for reporting at least annually to the Audit Committee to give assurance on IG.

6. Membership Core Membership:

- Chief Finance Officer - SIRO (Chair)
- Chief Nurse - Caldicott Guardian (Co-Chair) *
- Director of Corporate Services, Governance and Performance*
- Deputy Chief Finance Officer/Deputy SIRO • Commissioning Support IG Lead
- Corporate Services Manager
- CCG IG Lead
- Additional Members as Required
- Information Asset Owners/Administrators
- Data Protection Officer

*Nominated deputies may attend where core members are not able to attend, **subject to prior approval from the Chair.**

Other employees of the CCG may be invited to attend all or part of the committee to provide advice or support particular discussion from time to time as required.

7. Quorum

The IG Steering Group shall be quorate with three Members present and must include:

- The CFO (SIRO) or Deputy CFO (Deputy SIRO) and
- Chief Nurse (Caldicott Guardian) or nominated deputy and
- One member of the Commissioning Support Information Governance Team

8. Information Governance Working Group

The IG Steering Group is supported by the work of the IG Steering Group.

The IG Steering Group does not have any authority to delegate authority to the working group and exists only to support the work of the IG Steering Group.

9. Confidentiality and Conflicts of Interest / Standards of Business Conduct

All Members are expected to adhere to the CCG Constitution and Standards of Business Conduct and Conflicts of Interest Policy.

In circumstances where a potential conflict is identified the Chair of the Committee will determine the appropriate steps to take in accordance with the CCG's Conflicts of Interest decision-making matrix. This action may include, but is not restricted to, withdrawal from the meeting for the conflicted item or remaining in the meeting but not voting on the conflicted item.

All Members shall respect confidentiality requirements as set out in the CCG Constitution.

10. Meeting Frequency

The IG Steering Group will meet a minimum of 4 times a year.

If, for any reason, decisions are required as a matter of urgency and it is not considered necessary to call a full meeting, the committee may choose to convene a telephone conference or other virtual meeting or to review and take decisions via email. The meeting is still required to be fully quorate where decisions are required to be made. These decisions will be recorded by the secretariat and confirmed at the next available committee meeting. 11 Conduct of the Committee • The Group will conduct its business in accordance with any national guidance and relevant codes of conduct / good governance practice, for example, Nolan's seven principles of public life. • Any resulting changes to the Terms of Reference should be approved by the Audit Committee

11. Conduct of the Committee

The Group will conduct its business in accordance with any national guidance and relevant codes of conduct / good governance practice, for example, Nolan's seven principles of public life.

Any resulting changes to the Terms of Reference should be approved by the Audit Committee.