NHS
North East Lincolnshire
Clinical Commissioning Group

Information Governance Framework and Strategy

Document Title:	Information Governance Framework and Strategy
Version No:	4.0
Latest version issued:	November 2020
Supersedes:	All previous Information Governance Framework and Strategy policies
Name of Author (s):	Corporate Assurance Officer
Consultation:	IG Steering Group N3i – Information Governance Specialist
Approved by:	Governing Body
Approval date:	TBC
Review date:	TBC
Equality Impact Assessment Date:	N/A
Target Audience:	CCG Staff & Members
Dissemination:	NELCCG intranet & weekly bulletin

Version	Description of Amendments	Date
0.1	First draft for comment	
1.0	Approved version SMT	Feb 14
1.1	Integrated Governance & Audit Committee approved review date to be changed to 04/04/2015	Dec 14
1.2	Amendments to reflect NHS Digital Guidance and Caldicott 2	Feb 16
1.3	Addition of Impact Analysis Sections. Minor Amendments to reflect change from CSU to EMBED. More details on accountability processes and organisational structure. Training & Guidance removed reference to current training tool. Improved guidance on incident reporting and investigations with flow chart.	Mar 17
1.4	Annual Review - Amendments to reflect current Data Protection Legislation and the General Data Protection Regulations (EU) 2016/679	Mar 18
2.0	This is an annual review. Minor tweaks and updated Annex B to reflect the 2018 Act principles.	Oct 19
3.0	Amended to improve accessibility	May 2020
4.0	Annual review	Nov 2020

The on-line version is the only version that is maintained and valid. If this document has been printed or saved to another location, the reader must check that the version number matches that of the on-line version.

Contents

1. Introduction and Purpose

The purpose of this framework is to describe the management arrangements that will deliver Information Governance (IG) assurance within North East Lincolnshire Clinical Commissioning Group (afterwards referred to as NELCCG). Information Governance is a framework that enables the organisation to establish good practice around the handling of information, promote a culture of awareness and improvement and comply with legislation and other mandatory standards.

2. Impact Analyses

2.1 Equality

In accordance with the CCG's commitment to Equality and Diversity, we aim to eliminate discrimination, harassment and victimisation, advance equality of opportunity, and promote good relations between groups. We need to do this for the nine protected characteristics: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

In developing this framework, an equality impact assessment has been considered as a neutral impact as the content of this policy does not have any adverse or detrimental impact on a particular group. This is because the framework is formatted in a way that is easy to read and can be made available on request in other formats and in other languages from the author of this framework. Arrangements can be made for members of staff with disabilities who wish to access information in a different format.

2.2 Bribery Act 2010

The relevance of the Bribery Act 2010 must be considered in respect of every policy.

The CCG follows good NHS business practice as outlined in the Standard of Business Conduct and Conflicts of Interest Policy and has robust controls in place to prevent fraud, bribery and corruption. Due consideration has been given to the Bribery Act 2010 in the development (or review, as appropriate) of this document and no specific risks were identified

Anyone with concerns or reasonably held suspicions about potentially fraudulent activity or practice should refer to the Local Anti-Fraud and Corruption Policy and contact the Local Counter Fraud Specialist through this hyperlink.

3. Information Governance Strategy

The development of a fixed IG Framework will support an IG Strategy that will develop over time with the current version published at Annex A.

4. National Context

~~The NHS Information Governance Assurance Programme (IGAP) was established in February 2008 in response to the Cabinet Office Data Handling review. The Prime Minister commissioned the review following the high-profile data losses in 2007~~. The NHS Information Governance Assurance Programme ~~I~~GAP developed a number of principles to support and strengthen the existing Information Governance agenda. The principles are:

- All NHS organisations should be part of the same Information Governance Assurance Framework (IGAF)
- Information Governance should be as much as possible integrated into the broader governance of an organisation, and regarded as being as important as financial and clinical governance in organisational culture
- The Framework will provide assurance to the several audiences interested in the safe custody and use of special categories of personal information in healthcare. This involves greater transparency in organisational business processes around Information Governance
- Information Governance Assurance Framework ~~GAF~~ to be built on the strong foundations of the existing Information Governance agenda and is the mechanism by which:
    - IG policies and standards are set
    - Regulators can check an organisation's compliance
    - An organisation can be performance managed

5. Aim

The purpose of this local framework is to set out an overall strategy and promote a culture of good practice around the processing of information and use of information systems. That is, to ensure that information is handled to ethical and quality standards in a secure and confidential manner. The organisation requires all employees to comply with the Policies, Procedures and Guidelines, which are in place to implement this framework with the aim of ensuring that NELCCG maintains high standards of IG.

NELCCG will establish, implement and maintain procedures linked to this policy to ensure compliance with the requirements of ~~current Data Protection Legislation and the General Data Protection Regulations (EU) 2016/679 (GDPR)~~ Data Protection Act 2018, Records Management Guidance, Information Security Guidance and other related legislation and guidance, contractual responsibilities and to support the assurance standards of the Data Security and Protection Toolkit. These standards are:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance

This framework supports the CCG in its role as a Commissioner of health and care Services and will assist in the safe sharing of information with its partners and agencies.

6. Data Security and Protection Toolkit (DSPT)

Completion of the DSPT is mandatory for all organisations ~~that have access to NHS patient data and systems. providing NHS services and processing NHS personal data~~. All organisations are required to show compliance with assertions and (mandatory) evidence items. Annual plans will be developed year on year from the DSPT to achieve a satisfactory compliance with all assertions and (mandatory) evidence. As the DSPT is a ~~publically~~ publicly available assessment, the compliance and assurance of partner organisations in completing a DSPT will be used to assess their suitability to share information and to conduct business with.

Social care providers who provide care through the NHS Standard contract need to comply with the DSPT. For social care providers who do not provide care through the NHS Standard

Contract, it is recommended that all social care providers consider complying with the DSPT to help demonstrate compliance of the data security standards and meeting their obligations on data protection and data security.

~~Whilst completion is not mandatory for commissioners of social care it is however considered good practice that the CCG is compliant for the delivery of its commissioning functions of adult social care~~.

7. Roles and Responsibilities

7.1 ~~EMBED Health Consortium~~ N3i Ltd

NELCCG has a contract in place with ~~eMBED Health Consortium~~ N3i to deliver Specialist advice and IG Support ~~a range of IG Services~~ including ~~support to achieve~~advice on compliance with the DSPT.

~~7.2 Governing Body~~

~~The Governing Body is accountable for ensuring that the necessary support and resources are available for effective implementation of this framework. It has the responsibility for the Information Governance Agenda supported by identified senior roles i.e. Caldicott Guardian, SIRO, and IG Lead.~~

~~7.3 Integrated Governance Audit Committee~~

~~The Integrated Governance & Audit Committee (IG&A) support and drive the broader information governance agenda and provide the Governing Body with the assurance that effective information governance best practice mechanisms are in place within the organisation.~~

~~The Information Governnce agenda will be led by the CCG's SIRO supported by CCG staff and staff of eMBED Health Consortium and will report through regular IG Meetings to the IG&A Committee.~~

~~The IG Work Programme, and new or significantly amended strategies and policies are escalated for consideration and approval to the IG&A Committee and the Governing Body.~~

~~7.4 IG Steering Group~~

~~The IG Steering Group will report to the IG&A Committee, through minutes or action notes and will ensure the IG&A is briefed on any significant issues~~.

7.5 Caldicott Guardian

The Caldicott Guardian for NEL CCG is the Clinical Lead, Governance & Quality.

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information sharing. The Guardian plays a key role in ensuring that NHS, Councils with Social Services Responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share and advises on options for lawful and ethical processing of information. The Caldicott Guardian also has a strategic role, which involves representing and championing Information Governance requirements and issues at Board or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

7.6 Senior Information Risk Owner (SIRO)

The SIRO for NELCCG is the Director of Quality & Nursing

The Senior Information Risk Owner (SIRO) is an Executive or Senior Management ~~Board~~ Governing Body Member who will take overall ownership of the Organisation's Information Risk Policy, act as champion for information risk on the ~~Board~~ Governing Body and provide written advice to the Accounting Officer on the content of the Organisation's Annual Governance Statement in regard to information risk.

The SIRO must understand how the strategic business goals of the Organisation and how other organisations business goals may be impacted by information risks, and how those risks may be managed. The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the organisation and advises the Governing Body ~~Board~~ on the effectiveness of information risk management across the organisation.

7.7 Data Protection Officer

Under GDPR public authorities or organisations who carry out large scale processing of sensitive data must appoint a Data Protection Officer. The role of Data Protection Officer is to facilitate the CCG's compliance with GDPR and will:

- Monitor CCG compliance with the ~~GDPR~~data protection responsibilities and obligations
- Provide advice and assistance with regards to the completion of Data Protection Impact Assessments
- Act as a contact point for the Information Commissioners Office (ICO), members of the public and CCG staff on matters relating to GDPR and the protection of personal information
- Assist in implementing essential elements of the data protection legislation~~GDPR~~ such as the principles of data processing, data subjects' rights, Data Protection impact assessments, records of processing activities, security of processing and notification and communication of data breaches

7.8 Information Governance Lead

The Information Governance Lead for NELCCG is the Chief Finance Officer

~~The IG Lead works with eMBED Health Consortium to ensure systems are developed and implemented.~~ The IG Lead is responsible for the co-ordination of the implementation of systems within the CCG. The IG lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG within the CCG. This role includes but is not limited to:-

- developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, eg an overarching ~~high level~~high-level strategy document supported by corporate and/or directorate policies and procedures;

- ensuring that there is top level awareness and support for IG resourcing and implementation of improvements;
- providing direction in formulating, establishing and promoting IG policies;
- establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives;
- ensuring annual assessments and audits of IG policies and arrangements are carried out, documented and reported;
- ensuring that the approach to information handling is communicated to all staff and made available to the public;
- ensuring that appropriate training is made available to staff and completed as necessary to support their duties and for NHS organisations;
- liaising with other committees, working groups and programme boards in order to promote and integrate IG standards;
- monitoring information handling activities to ensure compliance with law and guidance; and providing a focal point for the resolution and/or discussion of IG issues.

7.9 Information Asset Owners and Administrators

Information Asset Owners (IAO) are senior individuals involved in the running of their respective business functions and are directly accountable to the SIRO. IAOs must provide assurance that information risk is being managed effectively in respect of the information assets they are responsible for and that any new changes introduced to their business processes and systems undergo a Data Protection impact assessment were appropriate.

An Information Asset Administrator (IAA) will have delegated responsibility for the operational use of an Asset.

7.10 Managers

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 for information security;
- where to access advice on matters relating to security and confidentiality; and
- the security of their physical environments where information is processed or stored.

7.11 All staff

Information Governance compliance is an obligation for all staff. Staff should note that they are expected to participate in induction training, annual refresher training and awareness raising sessions carried out to inform/update staff on information governance issues. Any breach of confidentiality, inappropriate use of health, business or staff records or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract and must be reported to the SIRO and (in the case of health or social care records), the Caldicott Guardian.

All staff are personally responsible for compliance with the law in relation to the Data Protection Act, the General Data Protection Regulation and the Common Law of Confidentiality.

Staff are responsible for reporting any possible or potential issues whereby a breach of security may occur.

7.12 Third Party Contractors

Contracts with third parties providing services to and on behalf of NELCCG must include appropriate, detailed and explicit requirements regarding confidentiality, data protection and information governance to ensure that Contractors are aware of ~~their~~ IG obligations.

All support services that process information on behalf of the CCG will be required to

- Ensure a suitable contract/SLA and or as a minimum, a confidentiality agreement is in place to form a Controller to Processor relationship where Personal or Personal Sensitive data is managed on behalf of the CCG.
- Ensure that services commissioned meet the requirements of the current Data Protection Act and GDPR when providing services including, but not limited to, fair processing and maintaining a Data Protection notification with the Information Commissioners Office.
- Complete the annual Data Security and Protection Toolkit (if applicable), and at the request of the CCG, undertakes a compliance check/audit in order to provide assurance that they have met expected requirements.
- Ensure that any new processing is within the remit of the contract or seek written confirmation if there is any ambiguity.
- Report any known incidents or risks in relation to the use or management of information owned by the CCG.
- Set out expectations regarding providing information in relation to requests for information made under the Freedom of Information Act.
- Ensure inclusions regarding Exit Plans are addressed following transfer of services or decommission of service e.g. passing on data/deletion/retention of data at the end of the contract.

8. ~~Governance Arrangements~~

The following arrangements have been agreed:

- ~~The CCG Governing Body will receive periodic assurance that management and accountability arrangements are adequate and are informed in a timely manner of future changes in the IG agenda by assurance updates/reports from the IG&A Committee.~~
- ~~The CCG will obtain Information Governance Support through a contract with eMBED Health Consortium.~~
- ~~Responsibility and accountability for Information Governance will be cascaded through the organisation via staff contracts, contracts with third parties, Information Asset Owner arrangements and Line Managers, and newsletters, and IG awareness sessions as and when required.~~

9. Key Principals and Procedures

9.1 Openness and Transparency

- The CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.
- Information will be defined and where appropriate kept confidential underpinning the principals of Caldicott legislation and guidance.
- Information about the organisation will be available to the public in line with the Freedom of Information Act, Environmental Information Regulations and Protection of Freedoms Act unless an exemption applies. The CCG will establish and maintain a Publication Scheme in line with the legislation and guidance from the Information Commissioner.
- There will be clear procedures and arrangements for handling queries from patients, staff and other agencies and the public concerning personal and organisational information.
- Integrity of information will be developed, monitored and maintained to ensure it is appropriate for the purposes intended.
- Legislation, national and local guidelines will be followed
- The CCG will undertake annual assessments and audits (through the Data Security and Protection Toolkit) of its policies, procedures and arrangements for openness.
- Patients will have ready access to information relating to their own health care under Data Protection legislation using the CCG's ~~Access to Records policy.~~subject access request policy
- The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media.

9.2 Legal Compliance

- The CCG regards all identifiable personal information relating to patients as confidential. Compliance with legal and regulatory requirements will be achieved, monitored and maintained.
- The CCG will undertake or commission annual assessments and audits of its compliance with legal requirements as part of the Annual Assessment against the Data Security and Protection Toolkit Assertions and in line with changes and developments in legislation and guidance
- The CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise as set out in the principals of the Human Rights Act and in the public interest.
- The CCG will establish and maintain policies to ensure compliance with the current Data Protection legislation, Freedom of Information Act, Human Rights Act and the common law of confidentiality and associated guidance

- ~~Information Governance training will be mandatory for all staff. This will include awareness and understanding of Caldicott Principles and confidentiality, information security and data protection. Information Governance will be included in induction training for all new staff with completion of refresher training on an annual basis thereafter. The necessity and frequency of any further training will be personal development based~~

- The CCG will work in collaboration with the Local Counter Fraud Specialists and other related agencies to support their work in detecting and investigating fraudulent activity across the NHS.

- The CCG is bound by the provisions of a number of items of legislation affecting the stewardship and control of patient and other information - refer to Annex B

Formatted: List Paragraph, Space Before: 0 pt, No bullets or numbering

Formatted: Font: 11 pt

Formatted: Font: 11 pt

10. Information Security

With the increasing use of electronic data and ways of working which rely on the use of electronic information and communication systems to deliver services there is a need for professional advice and guidance on their use as well as the need to ensure that they are maintained and operated to the required standards in a safe and secure environment. The CCG has a Records Management policy covering all aspects of records management and consistent with the Records Management Code of Practice for Health and Social Care 2016.

Accreditation of Information Systems

The CCG shall ensure that all new information systems, applications and networks include a security policy are appropriately approved prior to implementation.

System specific security policies will be developed for systems under CCG control in order to allow granularity in the security management considerations and requirements of each. This may result in specific responsibilities being assigned and obligations communicated directly to those who use the system.

The CCG shall ensure that all new information systems, applications and networks include a Data Protection Impact Assessment (DPIA) and System Level Security Policy (SLSP) and are approved by the Information Governance Steering Group and/or the CCG IT Service provider before they commence operation.

When planning for, and during procurement of, new systems, it is the responsibility of the Project Manager or Lead to ensure that appropriate system security features are included within the system. As a minimum this will include a password protection feature and audit logs.

Systems and applications must be adequate for their purpose.

Software applications, upgrades and amendments must be developed in a controlled manner, documented and thoroughly tested before implementation.

Unauthorised software must not be introduced onto any system without prior authorisation from the CCG IT Service Provider.

~~10.1 Quality Assurance and Records Management~~

- ~~The CCG will establish and maintain policies and procedures for information quality~~

assurance and the effective management of records.

- The CCG will undertake or commission annual assessments and audits of its information quality and records management arrangements.

- Managers are expected to take ownership of, and seek to improve of, the quality of information within their services.

- Wherever possible, information quality should be assured through policies, procedures, user manual and training.

- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

- The CCG will establish a Records Management policy covering all aspects of records management and consistent with the Records Management Code of Practice for Health and Social Care 2016.

11. Current Data Protection Act and General Data Protection Regulations (EU) 2016/679 Data Protection Act 2018

The current Data Protection Act Legislation and the General Data Protection Regulations (EU) 2016/679 Data Protection Act 2018 is are the most fundamental pieces of legislation that underpins Information Governance. NELCCG are registered with the Information Commissioners Office and will fully comply with all legal requirements. A process will be adopted to promote Data ProtectionPrivacy by Design and ensure that a review of all of new systems is carried out and where requirements such as the need for Data Protection Impact Assessments (DPIA) are highlighted these will be completed.

Current Data Protection Legislation and General Data Protection Regulations (EU) 2016/679 Principles are detailed in Annex B.

12. Caldicott Principles and Requirements

The Caldicott Principles are fundamentals that organisations should follow to protect any information that could identify a patient, such as their name and their records. They also ensure that this information is only used and shared when it is appropriate to do so. These principles determine whether they need to share information that could identify an individual.

NELCCG, complies and acts in accordance with these principles.

The original Caldicott Report on the Review of Patient-Identifiable Information 1997 and the subsequent Report of the Caldicott 2 Review - Information: To share or not to share? and The Information Governance Review 2013. These two reports have identified specific principles that are considered essential practice for the appropriate sharing and security of Patient Information.

Government Response to the Report of the Caldicott 2 Report acknowledges the findings of this and promotes that everyone should understand how to protect and, where appropriate, share information about the people they care for, either directly or indirectly. The Caldicott Principles are detailed at Annex C.

This is further supported by the Everyone Counts: Planning for Patients 2014/15 to 2019/20 by

~~detailing practical applications for information sharing, these are detailed at Annex D.~~

13. Handling Confidential Information

When handling confidential information and especially where an individual can be identified from the information to be processed, the CCG must ensure that it has determined and documented a legal basis for processing that information.

In addition, it must ensure that arrangements are in place to ensure:

- data subjects are appropriately informed of all uses of their information
- the security of that information at all points of its lifecycle.
- objections to the handling of confidential information and where circumstances under which an objection cannot be upheld are recognized and recorded.
- that where objections are received where the proposed uses are not required by law the CCG should ensure they act in accordance with that objection.
- procedures are implemented for recognising and responding to individuals' requests for access to their personal information.
- procedures are in place to promote and support the exercise of all data subject rights?
- appropriate information sharing arrangements are in place for the purposes of direct care.
- appropriate data processing agreements are in place to collect or obtain information for management purposes.

NHS Digital has issued two guidance documents in respect of appropriate information handling and confidentiality of that information:

1. **Code of practice on confidential information**: This code of practice describes good practice for organisations handling confidential information concerning, or connected with, the provision of health services or adult social care.

2. **A guide to confidentiality in health and social care**: A guide for those involved in the direct care of a patient on the appropriate handling of confidential information.

14. Risk Management

The ability to apply good risk management principles to IG is fundamental and all organisations will apply them through organisational policies. Risk assessment are included as part of the Information Asset Owners role. Any information flows from or into identified information assets will be risk assessed and the results reported to the CCG SIRO for risk mitigation, acceptance or transfer.

15. Training and Guidance

In accordance with the requirement to achieve compliance with the DSP Toolkit, all staff must complete an induction session, which will include Information Governance, when they first start employment. In subsequent year's Data Security Awareness training for all staff is mandatory and will include awareness and understanding of Caldicott principles and confidentiality, information security and data protection. E-learning products are provided for the training via the eLearning for Health website and ESR.

There will be specific modules available for Caldicott, SIRO and ~~IG~~ Information Asset

Ownersstaff themselves. Appropriate staff must complete the modules relevant to their roles as detailed in the Training needs analysis. when training becomes available.

Monitoring and Review

This framework will be monitored and reviewed on an annual basis by the IG Steering Group.

The Governing Body will be responsible for the approval of the framework.

16. Awareness and Advice

eMBED Health Consortium will provide advice on any IG related issue. They will work with the NELCCG IG Lead to produce newsletters and staff e-mails to provide information and updates on IG issues.

Responsibility and accountability for IG is cascaded through the CCG and is coordinated by the CCG Corporate Governance Team via the following:

- IG survey
- Data Protection Impact Assessment Proforma;
- Information Asset Owners handbook
- Review of information asset register
- Data Security Awareness Training
- Training Need Analysis
- IG updates in staff newsletters
- IG awareness sessions as and when required
- IG and related policies and procedures

17. Incident Management

17.1 Incident Reporting

Information Governance and Information Technology related incidents, including cyber security incidents (including but not limited to, physical destruction or damage to the organisation's computer systems, loss of systems availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions) must be reported and managed through the CCG's Incident Management and Reporting Policy. ~~Under GDPR, w~~Where a data breach is likely to result in a risk to the rights and freedoms of the individual, incidents must be reported to the Information Commissioners Office within 72 hours.

An information governance incident of sufficient scale or severity to be classified as a Serious Incident Requiring Investigation (SIRI) (via the NHS Digital checklist on the DSP Toolkit) will be:

- Notified immediately to the CCG's SIRO and Caldicott Guardian
- Reported to the Department of Health, Information Commissioners Office and other regulators via STEIS and the Data Security and Protection Toolkit.
- Investigated and reviewed in accordance with the guidance in the NHS Digital checklist
- Reported publicly through the CCGs Annual Report and Governance Statement

17.2 Investigation

~~eMBED Health Consortium~~N3i will support the investigation of all IG issues reported. This may include, but is not limited to, breaches of policy, breaches of confidentiality and issues related to IT Security. The ~~eMBED~~ N3i IG Team will assist with the procedural processes to ensure that investigations of incidents will be carried out in a way that ensures the preservation of evidence and in a manner that enables both legal and disciplinary action to be taken if necessary.

18. Organisational ~~Structure for IG~~ Reporting and Assurance

The Governing Body is accountable for ensuring that the necessary support and resources are available for effective implementation of this framework. It has the responsibility for the Information Governance Agenda supported by identified senior roles i.e. Caldicott Guardian, SIRO, and IG Lead

The CCG Governing Body will receive periodic assurance that management and accountability arrangements are adequate and are informed in a timely manner of future changes in the IG agenda by assurance updates/reports from the IG&A Committee.

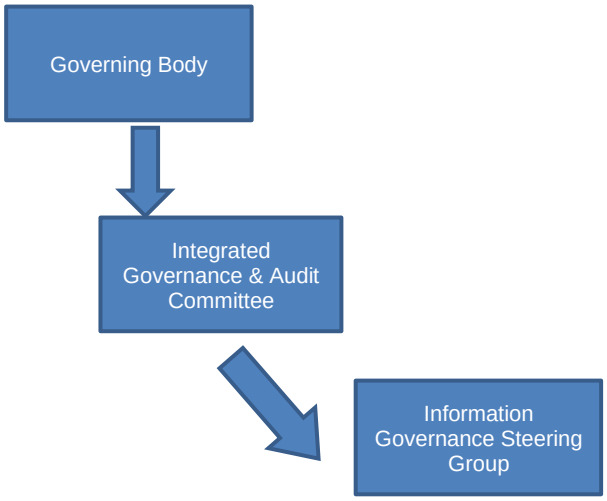
The Integrated Governance & Audit committee (IG&A) support and drive the broader information governance agenda and provide the Governing Body with the assurance that effective information governance best practice mechanisms are in place within the organisation.

The Information Governance Steering Group is accountable to the Governing Body through the Integrated Governance & Audit Committee and supports and drive the broader information governance agenda. The group ~~will~~ reports to the IG&A Committee, through minutes or action notes and will ensure the ~~IG&A is~~committee is briefed on any significant

issues.

The SIRO will ensure that the Integrated Governance & Audit Committee is made aware of any IG matters of concern and will provide an annual IG report to the committee.

~~The Governing Body retains overall responsibility and accountability for all aspects of Information Governance.~~



19. Policies and Procedures

The CCG will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Freedom of Information Act, Human Rights Act and the common law of confidentiality and associated ~~The~~guidance. The Information Governance Framework and Strategy are supported by a range of detailed policies and procedures.

These include but are not limited to:

- All Data Protection & Confidentiality ~~Policy~~ Policies
- ~~Confidentiality: Code of Conduct Policy~~
- Records Management policy
- Safe Haven Policy
- ~~Mobile working policy~~
- ~~Information Security Policy~~
- ~~B~~usiness Continuity ~~and Strategy Policy~~Plan
- ~~Confidentiality Audit Policy~~
- Subject Access Request Policy
- ~~Acceptable Computer Use Policy~~ NELC ICT & Information Security Policy
- Email Policy
- Information Asset Owner ~~AO role and responsibilities/~~Handbook

- ~~Information Security Policy~~
- ~~Information Governance Checklist and~~
- ~~Privacy Impact Assessment~~
- Data Protection Impact Assessment

All of these documents are available on the CCG Intranet site.

20. Reference Material

- ~~Current Data Protection Legislation~~
- ~~General Data Protection Regulations (EU) 2016/679~~
- ~~Human Rights Act 1998 (Specifically Article 8)~~
- ~~NHS Information Governance: Guidance on Legal and Professional Obligations.~~
- ~~Report on the Review of Patient-Identifiable Information 1997 (Caldicott Report)~~
- ~~Report of the Caldicott2 Review – Information: To share or not to share? The Information Governance Review 2013~~
- ~~Government Response to Report of the~~ Caldicott2 Review 2013.
- ~~NHS England: Everyone Counts: Planning for Patients 2014/15 to 2018/19.~~
- ~~NHS Digital: A guide to confidentiality in health and social care: Treating confidential information with respect - September 2013~~
- ~~NHS Digital: A guide to confidentiality in health and social care: references - September 2013~~
- ~~National Information Board and DH: Personalised Health and Care 2020~~
- ~~NHS England: NHS Standard Contract~~
- ~~Information Commissioner: Data Sharing Code of Practice~~
- ~~Information Commissioner: Privacy Impact Assessment Code of Practice~~
- ~~Records Management Code of Practice for Health and Social Care 2016'~~

~~In addition to the above policies and guidance documents the Registration Authority is managed and run by eMBED Health Consortium. Any work in this area will be completed following the Registration Authority Standard available on the eMBED Portal~~.

Formatted: Right: 0 cm, Line spacing: Exactly 14.65 pt

Formatted: Space Before: 0 pt

Annex A – North East Lincolnshire CCG Information Governance Strategy ~~2015 to 2020~~2020 - 2025

1. The IG Strategy of NELCCG will be based upon a vision of a long-term delivery of clear open principles to ensure that:

   1.1. The CCG complies with all statutory requirements

   1.2. The CCG has an information governance strategy that supports the achievement of corporate objectives

   1.3. The CCG can demonstrate an effective framework for managing information governance assurance

   1.4. Staff are aware of their responsibilities and the importance of information governance

   1.5. Information governance becomes a systematic, efficient and effective part of business as usual for the organisation

   1.6. Information governance is integrated into the change control process

   1.7. That there are effective methods for seeking assurance across the organisation and with its key partners

   1.8. That the organisation can demonstrate that the information governance arrangements of organisations it commissions services from across healthcare and commissioning support are adequate

   1.9. The CCG will facilitate and encourage the sharing of information where it is in the interest of the patients and ensure that any sharing remains compliant with information governance requirements.

Annex B - Legal Compliance – relevant legislation

- The current Data Protection legislation
- Access to Health Records Act, 1990
- Computer Misuse Act, 1990;
- Copyright, Designs and Patents Act, 1988 (as amended by the Copyright (Computer Programs) Regulations, 1992;
- Crime and Disorder Act, 1998; and

- The Human Rights Act 1998 - This policy describes the way in which information should be managed, in particular, the way in which personal or sensitive information should be protected.
- In addition to the above, other legislation can impact upon the way in which we should use personal information. This includes:
  - Public Interest Disclosure Act 1998;
  - Audit & Internal Control Act 1987;
  - Public Health (Code of Practice) Act 1984;
  - NHS (VD) Regulations 1974;
  - National Health Service Act 1977;
  - Human Fertilisation & Embryology Act 1990;
  - Abortion Regulations 1991;
  - The Terrorism Act 2000;
  - Road Traffic Act 1988;
  - Regulations under Health & Safety at Work Act 1974
  - Regulation of Investigatory Powers Act 2000
  - Freedom of Information Act 2000
  - The Health and Social Care (Safety and Quality) Act 2015

Much of the legislation mentioned is available in electronic format, via the Internet (www.legislation.hmso.gov.uk). In addition, the CCG is bound by the confidentiality aspects of common law and the Caldicott guidance on protection of patient information.

Formatted: Indent: Left: 0 cm, Hanging: 1.27 cm, Space After: 6 pt, Bulleted + Level: 1 + Aligned at: 1.27 cm + Indent at: 1.9 cm, Widow/Orphan control, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

Annex B - ~~Current Data Protection Legislation~~ Data Protection Act - Principles

~~(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');~~

~~(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');~~

~~(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');~~

~~(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');~~

~~(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');~~

~~(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').~~

~~(g) the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')~~

Annex C - Caldicott Principles

1. Justify the purpose(s)

Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary

Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data

Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis

Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities

Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law

Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

~~Annex D - Everyone Counts: Planning for Patients 2014/15 -2019/20~~

~~This document sets out the NHS England vision with regards to the provision and outcomes of high quality care for all, now and for future generations. One of the six national conditions focuses in on 'Better data sharing between health and social care, based on the NHS number' and that local organisations should 'ensure they have the appropriate Information Governance controls in place for information sharing in line with Caldicott 2, and if not, when they plan for it to be in place.'~~

~~The requirements of the above document are as follows: The CCG should where required~~

1. ~~Confirm that they are using the NHS Number as the primary identifier for health and care services, and if they are not, when they plan to;~~
2. ~~Confirm that they are pursuing open APIs (ie. systems that speak to each other); and~~
3. ~~Ensure they have the appropriate Information Governance controls in place for information sharing in line with Caldicott 2, and if not, when they plan for it to be in place.~~

~~NHS England has already produced guidance that relates to both of these areas. (It is recognised that progress on this issue will require the resolution of some Information Governance issues by DH).~~