South Lincolnshire
Clinical Commissioning Group

Information Governance Management Framework

(Including Policy and Strategy)

.

Reference Number:	IG01	
Version:	Version 1.0	
Approved by:	CCG Senior Management Team	
Date approved:	2nd March 2017	
Name and designation of author/originator:	Information Governance Services, Optum Commissioning Support Services	
Name of responsible Committee:	Senior Management Team	
Date issued for publication:	March 2017	
Review date:	January 2019	
Expiry date:	April 2019	
Target audience:	All staff	
Type of policy (mark appropriate box):	Non-clinical X	Clinical ☐
Mandatory to read?	Non-clinical staff X	Clinical staff X
Which NHSLA Risk Management Standard(s)?	Governance and Competent and capable Workforce	
Which relevant CQC standards (where applicable)?	Consent, Good Governance and Staffing	

Revision History

Version	Revision Date	Summary of Changes
0.1	Feb 2017	New Policy document replacing IG01: IGMF and IG02: Information Governance Policy
1.0	March 2017	Issued as “Final Approved” version

NHS
South Lincolnshire
Clinical Commissioning Group

CONTENTS

Definitions that apply to this Policy

Legal	Established by law
Ethical	Conforming to accepted standards of conduct, in this case respecting the privacy and dignity of the patient and obtaining their consent
Asset Owners	Those responsible for the information assets used within the service
Asset Administrators	Those given delegated authority to safe guard the use and security of the information assets
Statement of Internal Control	The mechanism for providing assurance in relation to appropriately managing and controlling resources
Forensic readiness	Ability to collect credible digital evidence and estimating the cost of an incident response
Privacy Impact Assessment	Assessing the extent to which activities intrude on privacy
Due Regard	Having **due regard** for advancing equality involves: • Removing or minimising disadvantages suffered by people due to their protected characteristics. • Taking steps to meet the needs of people from protected groups where these are different from the needs of other people. Encouraging people from protected groups to participate in public life • Or in other activities where their participation is disproportionately low.

1.1 Summary of Policy

Information plays a key part in the clinical and corporate governance of NHS South Lincolnshire CCG (referred to from herein as "*the* organisation") and the quality in the commissioning of patient services, planning, performance management, assurance, and financial management relies upon accurate and available information.

The Information Governance Assurance Framework (IGAF) is the national framework of standards that brings together all statutory, mandatory, and best practice requirements concerning information management. The standards are set out in the Information Governance Toolkit (IGT) as a roadmap enabling organisations to plan and implement standards of best practice and to measure and report compliance on an annual basis.

Performance against these standards is mandated by and reported to the Department of Health (DH) via the Care Quality Commission (CQC) and forms part of the assurance processes associated with Risk Management standards.

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. The way that an organisation chooses to deliver against these requirements is referred to within the Information Governance Toolkit as the organisation's Information Governance Management Framework (IGMF). The Information Governance Management Framework brings together all the requirements, standards and best practice that apply to the processing of personal information to ensure:

- Compliance with the law;
- Implementation of DH guidelines
- Planned year on year improvement
- IGT requirements

This framework sets out the approach the organisation is taking to provide a robust approach to IG standards.

This document provides a comprehensive view of the overarching framework for the strategic Information Governance agenda within the organisation.

2.0 Introduction

Information is a vital asset and resource, both in terms of commissioning and the efficient management of services and its support. It plays a key part in healthcare governance, service planning and performance management and improvement. It is of paramount importance to ensure that information is managed legally, ethically and efficiently; that appropriate accountability, standards, policies and procedures provide a robust governance framework for information management. This policy is supported and dependent on ensuring appropriate information is given

to members of the public, service users and staff at appropriate service interface's to ensure that the CCG's processes are open and transparent.

Information Governance is a framework that brings together all of the requirements, standards and best practice, that apply to the handling of personal information.

Senior level ownership of information risk is a key factor in successfully raising the profile of information risks and to embedding information risk management into the overall risk management culture of NHS SL CCG. Senior Leadership through the appointment of a Senior Information Risk Officer (SIRO) demonstrates the importance of ensuring information security remains high on the CCG's Governing Body agenda.

3.0 Purpose

To describe a system that ensures SWL CCG meets its responsibility for the legal and ethical management of information assets and resources and ultimate compliance with the Information Governance Toolkit (IGT), NHS and other professional Codes of Conduct relating to confidentiality and consent; and guidance from the Information Commissioner.

The IGT is used as a performance measure and the introduction of partnership working and national systems increase the importance of maintaining a suitable management framework to progress the IG agenda. The IGT is used by the Care Quality Commission (CQC) to determine the quality of the CCG's services.

Information Governance covers **all** staff employed by SWL CCG, private contractors, volunteers and temporary staff. The scope is:

- All information recorded, disclosed and used by the organisation
- All information systems managed by the organisation
- Any individual using information '*owned*' by the organisation
- Any individual requiring access to information '*owned*' by the organisation

4.0 Duties within the Organisation

Senior roles within the organisation supporting the Information Governance agenda are held by the organisation's Senior Information Risk Owner (SIRO), the Caldicott Guardian, and the IG Lead supported by the IG Team provided by Optum Commissioning Support Services under contract.

This framework applies to:

- All staff of the organisation, including temporary staff and contractors / sub- contractors;
- All information used by the organization;
- All information systems managed by or used by the organization;
- Any individual using information 'owned' by the organization;
- Any individual requiring access to information 'owned' by the organisation

4.1 CCG Responsibilities

All clinical information used in the NHS is subject to consent to its recording by the individual to whom the data relates and its subsequent uses, and handling by individuals within the legal and ethical requirements relating to data recording and usage. The organisation will ensure that all staff members are clear about their legal and ethical responsibilities and the CCG will ensure the provision of appropriate education and training.

The CCG will ensure legal and ethical requirements relating to information are met.
The CCG will make arrangements to meet the performance assessed requirements of NHS Digital's IG Toolkit which ultimately feeds into other external assessments, e.g. Care Quality Commission.

To manage its obligations the CCG will issue and support standards, policies and procedures ensuring information is **H**eld, **O**btained, **R**ecorded, **U**sed and **S**hared correctly (HORUS principles).

4.2 Responsibilities of Users

Recorders and users of information must:

- Be aware of their responsibilities
- Comply with policies and procedures issued by the CCG
- Work within the principles outlined in the information governance toolkit, relevant NHS Codes, and guidelines produced by e.g. Information Commissioner.

4.3 Caldicott Guardian

The Caldicott Guardian has a key role in ensuring that the CCG achieves the highest practical standards for handling patient information. This includes representing and championing confidentiality requirements and issues at Governing Body level, and wherever appropriate within the CCG's overall governance framework.

4.4 Senior Information Risk Owner

The SIRO is responsible for ensuring that there is an information risk policy and strategy; to have responsibility for the risk assessment process of information risk; including the annual Statement of Internal Control; to manage threats to security; to ensure that all employees are aware of their responsibilities and to keep the Governing Body informed about all information risk issues.

4.5 Information Asset Owners (IAO)

The SIRO is supported by IAOs who are responsible for running relevant business services. Their role is to understand what information is held, what is added, and what is removed, how

information is moved, who has access and why. As a result they are able to understand and address risks to information assets they "own" and to provide assurance to the SIRO on the security and use of the assets.

4.6 Information Asset Administrators (IAAs)

IAA's are staff who work with an information asset. They have day to day responsibility to ensure that policies and procedures are followed by staff in their services and they have a responsibility to recognise actual or potential security incidents, and consult their IAO on incident management.

4.7 CCG Information Governance Lead

The Information Governance Lead is responsible for co-ordinating on behalf of the SIRO and Caldicott Guardians the above functions and to ensure the smooth development of information governance aspects for the CCG covering the wide breadth of areas. This is done in conjunction with and through the support of the Information Governance team in Optum Commissioning Support Services, under contract.

4.8 The Governing Body Chair

The Governing Body Chair acts as the Information Governance Champion for the organisation, ensuring that communications have both a top down and bottom up approach.

5.0 CCG Information Governance Aims and Objectives

The fundamental aims of Information Governance are:

- To support the commissioning and therefore provision of high quality care by promoting the ethical, legal, effective and appropriate use of information
- To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources.
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards.
- To enable organisations to understand their own performance and manage improvement in a systematic and effective way.
- To hold information securely and confidentially
- To obtain information ethically, legally and efficiently, i.e. in line with the Data Protection Act 1998 and relevant codes of practice including those issued by the Department of Health and Professional regulatory bodies.
- To record information accurately and reliably and with the consent of the individual concerned (staff and/or patient).
- To use information effectively, legally and ethically.
- To disclose information ethically, lawfully and minimally as possible within those two

requirements.

- To commission safe care and maximise respect for public and service user privacy and dignity.

6.0 Legal and Regulatory Framework

There are a number of legal and ethical obligations placed upon the CCG for:

- The use and security of personal identifiable information.
- Appropriate disclosure of information when required.
- Regulatory frameworks for the management of information via NHS Digital's IG Toolkit.
- NHS and professional Codes of Conduct for consent to the recording and use of information.
- Operating procedures and codes of practice adopted by the NHS

7.0 Key Elements of the Information Governance Framework

The principles of this IGAF are based on the following elements:

7.1 National Requirements (i.e. Operating Framework, etc)

The NHS Operating Framework for the NHS in England sets out the key priority areas for systematically improving quality across the NHS.

The IG element details that the legal framework governing the use of personal confidential data in health care is complex. It includes the NHS Act 2006, the Health and Social Care Act 2012, the Health and Social Care (Quality and Safety) Act 2015, the Data Protection Act, and the Human Rights Act. The law allows personal data to be shared between those offering care directly to patients, but it protects patients' confidentiality when data about them are used for other purposes.

These "secondary uses" of data are essential if organisations are to run a safe, efficient, and equitable health service. It also includes the requirement for all NHS organisations to achieve a minimum of level 2 performance against all key requirements in the IG Toolkit as set out by the Department of Health (DoH). The CCG is ambitious and wishing to be high performing in this regard with the ambition to get to Level 3 compliance (where possible) on each IGT requirement over a 2 – 3 year period.

The CCG is responsible for ensuring that all organisations with which data is shared, including independent contractors and the third section, achieve the IGAF requirements. Information security and confidentiality are key priorities in ensuring continued commissioning of quality healthcare and patient centred health services.

7.2 Information Governance Toolkit

The annual information governance assessment is measured via a self-assessment process of compliance against the standards set out in the IG Toolkit and verified by Audit Review. The standards are ordered into the following initiatives:

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

NHS organisations are required to submit online IG performance reports to the Department of Health which can be tracked by monitoring bodies (i.e. CQC, Monitor). Currently CCG's are required to make a final annual self-assessment report on the 31st March each year. This performance assessment is shared with the Care Quality Commission, and the Audit Commission. The results are reported on the DoH website and made available to the general public. The CCG also provides this information in its Annual Report.

7.3 CCG's Information Governance Working Group

The CCG's Information Governance Working Group (CCG IG WG) has day to day responsibility for the Information Governance Agenda, and works alongside other governance groups (i.e. Senior Management Team, Risk and Governance Committee). The group has membership from nominated staff across the 4 Lincolnshire CCG's. The terms of reference for the group are available on request. The terms of reference are reviewed annually to ensure that there are no gaps or weaknesses in the CCG's IG accountability arrangements and that roles and responsibilities and responsibilities are current and in line with national guidelines and requirements.

The ultimate responsibility for Information Governance in the organisation lies with the Governing Body. The Governing Body discharges its functions through to the Senior Management Team as an assurance group to the Governing Body. The CCG Information Governance Working Group, through the Executive Nurse, Quality Lead and Caldicott Guardian provides assurance on information Governance through to the Senior Management Team. The CCG IG WG will through the development and routine reporting of agreed key performance indicators, identify risks, measure progress, oversee any necessary remedial action to be taken and provide report to SMT/Governing Body in line with its work plan and provide its minutes to the SMT.

The CCG IG WG has overall responsibility for overseeing the development and implementation of this framework, which includes the IG policy and IG strategy. This will be subject to periodic review and progress reports with any identified risks highlighted.

8.0 Information Governance – Key Areas

8.1 Asset Register

In order to appropriately scope and prioritise risk management efforts, it is necessary to ensure that a complete and accurate information asset register exists. As part of the identification

process, it is imperative that all instances of information assets be located.

In addition, information assets need to be classified in terms of sensitivity and criticality to the CCG.

It is also essential to ensure that all information assets have an identified owner. Information Asset Owners are senior individuals involved in running the relevant business. Their role is to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of those assets. Identified key risks (those rated medium or high), once assessed by the SIRO, supported by the CCG IG Working Group, will be considered for inclusion on the Risk Register.

This will support promoting accountability for complying with policy compliance and risk management and Privacy Impact Assessment requirements throughout the organisation. The Information Risk and Privacy Impact Assessment Policies set out clear guidance in relation to these issues.

8.2 Audit and Spot Check Compliance

The use of audit and the Spot Check Compliance Checklist is aimed to:

- Help raise the awareness of Data Protection and the legal framework upon which Information Governance is based;
- Show the organisation's commitment to and recognition of the importance of information governance in day to day working practices;
- Provide some self-assessment on our compliance to support the trajectory of level 3 compliance
- Identification of information governance risks to enable practical, pragmatic and operational specific recommendations
- Another vehicle in which to share knowledge

The focus of an audit approach is to determine whether the organisation has implemented policies and procedures to regulate the management and handling of personal information.

8.3 Communication

The CCG has a separate Information Governance Communication Plan. The key areas of communicating are:

- Publication Scheme (FOI)
- Updating of Intranet and Internet Sites relating to Information Governance

- Information Governance monthly update to CCG IG WG to be shared throughout the CCG as appropriate
- Targeted communication in terms of specific projects
- Privacy Notices
- Survey Monkey Questionnaires as a process of testing staff understanding of a particular theme
- Face to Face IG training sessions to support practical application of information governance elements

8.4 Contracts

Optum Commissioning Support Services Information Governance Team work with Optum's contracting team and NHS Arden and Greater East Midlands procurement team, respectively to ensure that contractors and the procurement process meet the required IG standards.

8.5 Corporate Records

The CCG will ensure it is managing Corporate Records effectively in line with the IG Toolkit requirements and the standards that need to be achieved to reach level three (3) compliance. Responsibility for corporate records management is with the CCG Board Secretary, supported appropriately by Optum's IG team.

8.6 Information Rights

The CCG contracts with Optum Commissioning Support Services for the provision of a Freedom of Information Act request and Subject Access Request (under the Data Protection Act) service. Through this responses are made to all requests received by acknowledging, finding the relevant information, co-ordinating into a suitable response, ensuring that necessary exemptions are applied whilst meeting the various legislative requirements in terms of timescales etc. Optum's IG team are also responsible for providing advice and support to the CCG in terms of disclosure decisions and where necessary apply other Laws (i.e. Access to Health Records for deceased patients, Section 29(3) requests for the Police).

8.7 Information Security Management

Information Security and its management deals with all aspects of information, whether spoken, written, printed, electronic or relegated to any other medium, regardless of whether it is being created, viewed, transported, stored or destroyed. This is contrasted with IT security, which is concerned with security of information within the boundaries of the technology domain.

Following good practice there are six basic outcomes of effective information security governance:

- Strategic alignment – aligning information security management to the CCG strategy and in support of its organisational objectives.
- Risk management – executing appropriate measures to mitigate risk and reduce potential impacts on information resources to an acceptable level
- Value delivery – optimizing security investments in support of the CCG business objectives
- Resource optimization – using information security knowledge and infrastructure efficiently and effectively
- Performance measurement – monitoring and reporting on information security processes to ensure that objectives are achieved
- Integration – integrating all relevant assurance factors to ensure that processes operate as intended from end to end.

8.7.1 Cyber Security

The technical threats to IT services are constantly changing with new technologies and services presenting a widening profile over which a malicious attacker could operate. This 'threat landscape' is also magnified by the constant introduction of new vulnerabilities into existing and legacy technologies, especially as the CCG explores the use of technology to find efficiencies in working. This presents a challenging management environment where the balance between the provision of ICT functionality must be tempered by the risk exposure to technical threats and malicious attack

The CCG is also part of the CareCERT programme which provides alert notification of threats both nationally and where any specific threat has been identified.

8.8 Policies

All information governance policies are approved in principle by the CCG IG WG before adoption by the Senior Management Team and ratification by the Governing Body. All policies are made available to staff via the Intranet / Internet site and are communicated in line with the CCG communication policy requirements.

Existing policies are updated and new policies introduced in line with current information governance agenda. These policies provide the organisation's Staff Code of Conduct and must be read in conjunction with the Organisation's Staff Handbook and Staff employment contracts.

Policies outline scope and intent and provide staff with a robust IG framework whilst setting out their responsibilities as employees of the CCG. The CCG is committed to ensuring that all staff and those working with the CCG are familiar with the organisation's objectives and what is expected of staff in order to achieve these objectives. Policies and procedures are one of the key means the CCG uses to communicate these expectations to staff. Staff are informed

through local team meetings, professional meetings and CCG briefings.

8.9 Registration Authority and Staff Identity Service

The Registration Authority Service and Staff Identity Service is provided under contract to the organisation through Optum Commissioning Support Services, Information Governance team.

The IG team are responsible for the registration process by which users of Smartcard- enabled IT applications are authenticated (proven who they say they are beyond reasonable doubt) and authorised (enabled to have particular levels of access to particular patient data).

The Registration Authority is the governance framework within which the CCG can register individuals as users to access the NHS Smartcard enabled system(s) - maintaining the confidentiality and security of patient information at all times.

Having a common and rigorous approach to how users are registered and are given access to the national services, and other services, is an integral part of protecting the confidentiality and security of personal and health care details.

8.10 Risk Assessment and Incident Management Process

Potential losses arising from breaches of IT and information security include physical destruction or damage to the organisation's computer systems, loss of system availability and the theft, disclosure or modification of information due to intentional or accidental unauthorised actions. In addition, healthcare organisations process person identifiable data of particular sensitivity, which needs to be protected from loss or inappropriate disclosure.

Clear guidance has been documented and issued to staff and all should be made aware of the organisation's incident reporting and management procedures (currently via the Datix system hosted by the Federated Clinical Risk and Compliance Team at NHS Lincolnshire West CCG). This process is supported by the CCG IG policies and procedures regarding information risk management. The process for the investigation of Information Governance Serious Incidents (SI's) is in line with the HSCIC Information Governance SUI Checklist published in May 2015. Reference is made in the CCG Incident Reporting Policy.

The CCG IG Lead, with the appropriate support of Optum CSS is responsible for ensuring that adequate arrangements are in place for:

- Reporting IG events or incidents
- Managing IG Risks
- Analysing, investigating and upward reporting of events/incidents and recommendations in collaboration with STEIS and the Information Commissioner's Office reporting requirements.
- IG work plans progress recommendations and learn the lessons Communicating IG

developments and standards to staff.

8.11 Training and Development

Information Governance Training and Development is essential for the development and improvement of staff knowledge and skills relating to IG not only within the IG Team but across the CCG.

IG training must extend beyond basic confidentiality and security awareness in order to develop and follow best practice. Staff must understand the value of information and their responsibility for it, which includes data quality, information security, records management, confidentiality, legal duty, information law and rights of access, and patient's rights in terms of a right of privacy and choice.

To ensure that different learning styles are catered for, training is available through face to face sessions and via NHS Digital's IG e learning module.
Information Governance training is a mandatory requirement for all staff and is included on induction and in line with the requirements of NHS Digital.

The organisation also utilises the following additional methods to ensure staff are trained in Information Governance:

- Articles in CCG staff communications
- Regular IG Campaigns
- Survey Monkey Questionnaires
- Policies, Procedures and Guidelines – staff have clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures. IG awareness and mandatory training procedures are in place and all staff received training appropriate to their role.
- Confidentiality – staff are provided with clear guidance on keeping information secure and on respecting confidentiality
- Consent – is appropriately sought before personal information is used in ways that do not directly contribute to the delivery of care services and objections to the use of such information are appropriately respected
- Fair processing – individuals are informed about the proposed use of personal information.

The governance group responsible for monitoring training is the CCG IG Working Group.

9.0 Management of the Information Governance Framework

The organisation will be responsible for implementing the Information Governance Policy and Framework.

The CCG IG WG will monitor the policy and the Executive Nurse will report to the SMT/Governing Body as appropriate.

10.0 References

10.1 Legal Framework

The organisation is bound by the provisions of a number of items of legislation and regulation affecting the stewardship and control of information. The main relevant legislation regulations are:

- Data Protection Act 1998
- Human Rights Act 1998
- Access to Health Records Act 1990
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Copyright (Computer Programs) Regulations 1992
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- Health and Social Care Act
- Regulation of Investigatory Powers Act 2000 (and Lawful Business Practice Regulations)
- Public Interest Disclosure Act 1998
- Public Records Act 1958
- Regulations under the Health and Safety at Work Act 1974
- Re-use of Public Sector Information Regulations 2005

This list is not exhaustive

10.2 Regulatory Framework

In relation to many of the above the NHS has set out and mandated a number of elements of regulation that constitute “Information Governance” through a national programme. This area is developing at a fast changing pace and the focus within this section will need significant periodical review.

Regulatory Elements are:

- The Information Governance Toolkit which requires CCG’s to assess their progress against set criteria
- Caldicott Reports and Recommendations
- Standards for Information Security Management

- Information Quality Assurance
- NHS Confidentiality: Code of Practice (2003)
- NHS Guidance on Consent to Treatment
- Care Quality Commission Regulations
- Information Commissioner's Office

10.3 Ethical Framework

The right to expect privacy ethically entitles individuals to exercise of control over the content, uses of and disclosures of information about them as an individual. Respect for that privacy by staff is essential for maintaining trust in, and integrity of any services provided by the CCG.

Three official bodies provide basic principles that underpin ethical frameworks and which form part of staff working practices in implementing this policy. These are:

A. Department of Health Code on Confidentiality which includes the following important principles:

   Staff should:
   - Protect – look after patient's information
   - Inform – ensure patients are aware of how their information is used; there should be no surprises
   - Provide Choice – allow patients to decide whether their information can be disclosed and used in particular ways
   - Improve practice – by always looking for better ways to protect, inform and provide choice

   So that the Public/patient will:
   - Understand the reasons for recording and processing information
   - Give their consent for the disclosure and use of their personal information
   - Gain trust in the way the NHS handles information
   - Understand their rights to access information held about them

B. Caldicott principles, applying to the disclosure of patient-identifiable information are:

   - Justify the purpose(s) of every proposed use or transfer
   - Don't use it unless it is absolutely necessary, and
   - Use the minimum necessary.
   - Access to it should be on a strict need to know basis
   - Everyone with access to it should be aware of their responsibilities; and
   - Understand and comply with the law.
   - The duty to share information can be as important as the duty to protect patient confidentiality

C. The Office of the Information Commissioner has specific responsibilities under the Data Protection Act 1998. This Act provides a framework to ensure that personal information is handled properly. The Act works in two ways:

1. It states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:
   - Fairly and lawfully processed
   - Processed for limited purposes
   - Adequate, relevant and not excessive
   - Accurate and up to date
   - Not kept for longer than is necessary
   - Processed in line with individual rights
   - Secure
   - Not transferred to other countries without adequate protection

2. The Act provides individuals with important rights, including the right to find out what personal information is held on computer and most paper records.

Additionally, all staff should be familiar with their own professional codes relating to ethical aspects of information governance (i.e. respect for patient privacy and dignity).

11.0 Information Governance Management Strategy

This strategy sets out the approach taken within the CCG to provide a robust Information Governance (IG) Framework for the current and future management of information.

Information Governance currently encompasses the following initiatives or work areas:

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

Others may be included as the scope of the Information Governance agenda widens.

Information Governance has the following fundamental aims:

- To support the commissioning of high quality care by promoting the effective and appropriate use of information
- To encourage staff to work closely together, preventing duplication of

effort and enabling more efficient use of resources
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards

To enable organisations to understand their own performance and manage improvements in a systematic and effective way.

11.1 Purpose of the Strategy

The purpose of this strategy is to set out the approach that the CCG will take to provide a robust Information Governance Framework for the future management of information assets.

This strategy has been developed taking into consideration:

- CCG self-assessment against national Information Governance requirements including the Information Governance Toolkit, NHS Operating Framework and CQC Registration.
- Relevant legislative framework
- Guidelines for Caldicott Guardians
- NHS Digital's priority areas for Information Governance including compliance with the NHS Care Record Guarantee
- External audit expectations and recommendations

There are two key components underpinning this strategy:

- A focus on the risks associated with information assets;
- An annual action plan arising from a baseline assessment against requirements set out in the NHS Information Governance Toolkit.

11.2 Responsibilities for delivering this strategy

- The Governing Body is responsible for ensuring that sufficient resources are made available to support the requirements of this strategy.
- The Senior Management Team on behalf of the Governing Body will be responsible for the overseeing of the delivery, evaluation and monitoring of outcomes of this strategy.
- The CCG IG WG will be responsible for the operational delivery and monitoring the implementation of the strategy and subsequent action plans reporting to the SMT through the Executive Nurse.

11.3 Wider Implications of Information Governance

This strategy cannot be seen in isolation as information plays a key part in Corporate Governance; Strategic Risk; Clinical Governance; service commissioning, planning and redesign; service delivery and performance management. The continual implementation of this strategy will

undoubtedly reduce the level of risk.

The focus on the risks associated with information assets will be captured on the Information Asset Register. This will include the identification of Information Assets and Information Asset Owners, information governance risk assessments, control measures, and where necessary the completion of Privacy Impact Assessments and the agreement of Information Sharing Protocols and Agreements.

Inbound and outbound data flows will be 'mapped' assessed and revised to mitigate risks of breaches to confidentiality and data security.

11.4 Associated Information Governance Policies/Strategies

- Information Security Policy
- Freedom of Information Policy
- Information Lifecycle and Records Management Policy and Strategy
- Data Protection, Caldicott and Confidentiality Policy
- Access to Personal Records Policy
- Information Sharing Policy

This is not an exhaustive list and all IG related policies and procedures are available on the CCG website

11.5 Information Governance Action Plan

The CCG Information Governance work plan is the framework developed to establish the overall direction of information governance and the baseline principles and objectives for a robust information handling culture that permeates throughout the organisation. It set out a programme of development to achieve and inform everyone's approach as to how they perform their daily tasks around information and its security regardless of seniority. An Action Plan aligned to the IG principles supports the delivery of the Information Governance Toolkit standards

Fundamental to the success of delivering the Information Governance Strategy is developing an Information Governance culture within the organisation. Awareness and training will be provided to all staff that utilise information in their day-to-day work to promote this culture. To deliver this the CCG will utilize NHS Digitals e learning packages and face to face training.

12.0 Dissemination

Copies of this Policy will be made available to all staff via the intranet. All staff will be notified of a new or reviewed Policy via the communication arrangements detailed in the

communications plan.
This document will be included in the CCG Publication Scheme in compliance with the Freedom of Information Act 2000.

13.0 Monitoring and Audit

- The organisation will monitor this policy and related strategies, policies and guidance through the CCG IG WG
- As assessment of compliance with requirements, within the Information Governance Toolkit (IGT) will be undertaken each year.
- The CCG IG WG will ensure implementation of the Information Governance Action Plan.
- Annual reports and proposed action/development plans will be presented to the Governing Body / SMT for approval prior to submission to the IGT.
- The organisation will ensure that the support infrastructure for the SIRO is in place, and is kept under regular review.

Ref	Minimum Requirements	Evidence for Self-assessment	Process for Monitoring	Responsible Individual / Group	Frequency of monitoring
	All staff have all completed Information Governance Mandatory Training in the last 12 months	Section 8.11	Information Governance Training compliance	CCG IG WG	Bi-Monthly
	Information Assets have a designated owner	Section 8.1	Review of Information Asset Register	CCG IG WG	Annually
	Managers undertake IG Spot checks	Section 8.2	IG Highlight Report	Records & Information Governance Group	Quarterly

	Information Governance SIRIs managed in line with HSCIC standards	Section 8.10	SI Reports	CCG IG WG	Quarterly

14.0 Links to Standards/Performance Indicators

This policy links directly to work required under the annual Information Governance Toolkit return.

Standards/Key Performance Indicators

Target/Standards	Key Performance Indicator
Meet Level 2 in each of the Information Governance Toolkit standards	Overall Information Governance assessment

15.0 Review of Policy

This policy and associated strategies will be reviewed every 2 years unless there are changes to the standards within the Information Governance Toolkit, any changes to legislation that may occur, and/or guidance from the Department of Health and/or NHS Executive.

15.1 Archiving

The CCG Governing Body Secretary is responsible for ensuring that superseded versions of policies and procedures are retained in accordance with the Records Management: Code of Practice for Health and Social Care 2016.

Appendix 1

The NHS Constitution

The NHS will provide a universal service for all based on clinical need, not ability to pay. The NHS will provide a comprehensive range of services

Shape its services around the needs and preferences of individual patients, their families and their carers	✓
Respond to different needs of different sectors of the population	✓
Work continuously to improve quality services and to minimise errors	✓
Support and value its staff	✓
Work together with others to ensure a seamless service for patients	✓
Help keep people healthy and work to reduce health inequalities	☐
Respect the confidentiality of individual patients and provide open access to information about services, treatment and performance	✓

Appendix 2

Equality Statement

NHS South Lincolnshire CCG (SL CCG) aims to design and implement policy documents that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

It takes into account the provisions of the Equality Act 2010 and promotes equal opportunities for all.

This document has been assessed to ensure that no one receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

In carrying out its functions, NHS SL CCG must have due regard to the different needs of different protected equality groups in their area.

This applies to all the activities for which NHS SL is responsible, including policy development and review.

Due Regard

The CCG's commitment to equality means that this policy has been screened in relation to paying due regard to the Public Sector Equality Duty as set out in the Equality Act 2010 to eliminate unlawful discrimination, harassment, victimisation; advance equality of opportunity and foster good relations.

A due regard review found the activity outlined in the document to be equality neutral because the document sets out the framework within which the handling and management of information is expected to be fulfil legal and statutory requirements.