Cambridgeshire and Peterborough
Clinical Commissioning Group

Cambridgeshire and Peterborough Clinical Commissioning Group (CCG)

INFORMATION GOVERNANCE POLICY 2017 - 2019

Approval Process

Lead Author:	Cambridgeshire and Peterborough CCG Information Governance Manager
Reviewed by:	Cambridgeshire and Peterborough CCG IG, BI & IM&T Group
Approved by:	Cambridgeshire and Peterborough CCG IG, BI & IM&T Group
Ratified by:	Clinical Executive Committee
Date ratified:	May 2017
Version:	3.0
Review date:	May 2019 (or earlier if significant change to local or national requirements)
Valid on:	April 2017

Document Control Sheet

Development and Consultation:	Policy developed in consultation with the IG, BI and IM&T Steering Group and endorsed by the Clinical Executive Committee.
Dissemination	This policy will be promoted to all staff within the CCG and held on the CCG's website.
Implementation	The Director of Corporate Affairs is responsible for monitoring the application of the policy by ensuring that:- • The policy is brought to the attention of all employees and building users • Managers are aware of their responsibilities for ensuring that staff under their control implement the policy • Staff are informed and consulted as appropriate • Appropriate training and guidance is provided to staff • Corporate business processes support the implementation of the policy.
Training	Training will be undertaken as part of the Trust's induction process.
Audit	Implementation of the Policy will be monitored in line with Information Governance Toolkit requirements.
Review	This policy will be reviewed two yearly, or earlier if there are changes in procedures or legislation.
Links with other Documents	The Policy should be read in conjunction with: see IG Framework (Appendix 3)
Equality and Diversity	The Corporate Services Support Manager with responsibility for E&D has carried out an Equality & Diversity Impact Assessment and concluded the policy is compliant with the CCG Equality and Diversity Policy. No negative impacts were found.

Revisions

Version	Page/ Para No	Description of change	Date approved
1		Discussed by Information Governance & IM&T Steering Group	April 2013
1.1		IG Framework reviewed and updated	June 2013
1.2	IG Framework	Attached revised version	Nov 2013
1.3	Contents	Revised wording	Nov 2013
2.0		Revised wording and ratification by CMET	July 2015
3.0		Reporting structure changes and general bi-annual review	April 2017

Information Governance Policy

Table of Contents

Information Governance Policy

1. Purpose

Information is a vital asset, both in terms of the clinical management of individual patients and the efficient management of services and resources. It plays a key part in Clinical Governance, service planning and performance management.

It is therefore of paramount importance to ensure that information is effectively managed and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

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 the Clinical Commissioning Group (CCG). Senior leadership through the appointment of a Senior Information Risk Owner (SIRO) demonstrates the importance of ensuring information security remains high on the Governing Body agenda.

This policy gives assurance to the CCG and to individuals that personal information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care.

The CCG will establish and maintain policies and procedures to ensure compliance with requirements contained in the latest version of the NHS Digital Information Governance Toolkit.

This policy, and its supporting standards and instructions, are fully endorsed by the Governing Body through the production of these documents and their minuted approval.

2. Scope

This policy covers all aspects of information within the organisation, including but not limited to:
Patient/client/service user information

- Personnel information
- Organisational information

This policy covers all aspects of handling information, including but not limited to:

- Structured record systems – paper and electronic
- Transmission of information –email, post, telephone and in exceptional circumstances, fax.

This policy covers all information systems purchased, developed and managed by, or on behalf of the organisation, and any individual directly employed or otherwise by the organisation.

3. Principles

The CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information.

The CCG fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and commercially sensitive information.

The CCG also recognises the need to share information with other health organisations and other agencies in a controlled and legal manner consistent with the interests of the patient and, in some circumstances, the public interest.

The CCG believes that accurate, timely and relevant information is essential to support the delivery of the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision making processes.

There are 4 key interlinked strands to the information governance policy:

- Openness and transparency
- Legal compliance
- Information security
- Quality assurance

3.1 Openness & 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 principles of Caldicott and the regulations outlined in the Data Protection Act and looking ahead to the implementation of the General Data Protection Regulation (GDPR). Non-confidential information on the CCG and services will be available to the public through a variety of means, in line with the CCG's code of openness and in compliance with the Freedom of Information Act, Freedom of Information Policy, Code of Conduct for Confidentiality, Data Protection Act and Access to Records Policy.

- Patients will have access to information relating to their own health care, options for treatment and their rights as patients. There will be clear procedures and arrangements for handling queries from patients and the public.

- The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media. See Appendix 1 for associated policies.

- Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.

- Availability of information for operational purposes will be maintained within set parameters relating to its importance via appropriate procedures and computer system resilience.

- The CCG regards all identifiable personal information relating to patients as confidential. Compliance with legal and regulatory framework will be achieved, monitored and maintained.

- The CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise.

- The CCG will establish and maintain policies and procedures to ensure compliance with the Data Protection Act (and the General Data Protection Regulation GDPR when it comes into force), Human Rights Act, the common law duty of confidentiality and the Freedom of Information Act.

- Information Governance training including awareness and understanding of legal and statutory requirements including Caldicott principles and confidentiality, information security and data protection, will be mandatory for all staff on an annual basis. Information governance will be included in induction training for all new staff. The necessity and frequency of any further training will be assessed at appraisal and determined as part of the NHS Cambridgeshire organisation development plan.

3.2 Legal Compliance

- The CCG regards all identifiable personal information relating to patients as confidential.
- The CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise
- The CCG will undertake or commission annual assessments and audits of its compliance with legal requirements through the IG Toolkit.
- The CCG will establish and maintain policies to ensure compliance with the Data Protection Act (and GDPR when it comes into force), Human Rights Act and the Common Law Duty of Confidentiality.
- The CCG will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act and Protection of Children Act)
- The CCG has a comprehensive range of policies supporting the information governance agenda; reference must be made to these alongside this policy. Legal and professional guidance should also be considered where appropriate (Appendix 1).

3.3 Information Security

- The CCG will establish and maintain policies for the effective and secure management of its information assets and resources
- The CCG will undertake or commission annual assessments and audits of its information and IT security arrangements through the IG Toolkit framework.
- The CCG will promote effective confidentiality and security practice to its staff through policies, procedures and training
- The CCG will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security
- All planned major information systems within the Organisation will be assessed via the Privacy Impact Assessment process before these systems become live to ensure appropriate levels of privacy and security are in place prior to launch.

3.4 Information Quality Assurance

- 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 in line with the IG Toolkit requirements
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services
- Wherever possible, information quality should be assured at the point of collection
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The CCG will promote information quality and effective records management through policies, procedures/user manuals and training.

4. Responsibilities

It is the role of the CCG Governing Body to define the CCG's policy in respect of Information Governance, taking into account legal and NHS statutory requirements. The Governing Body is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

The Chief Officer is the CCG's Accountable Officer and has overall accountability and responsibility for Information Governance and is required to provide assurance, through the Annual Governance Statement that all risks to the CCG, including those relating to information, are effectively managed and mitigated.

The Senior Information Risk Officer (SIRO) is an Executive Director of the CCG Governing Body. The SIRO is expected to understand how the strategic business goals of the CCG may be impacted by information risks. The SIRO will act as an advocate for information risk on the Governing Body and in internal discussions, and will provide written advice to the Accounting Officer for inclusion in the content of their Annual Governance Statement in regard to information risk.

The SIRO will provide an essential role in ensuring that identified information security threats are followed up and incidents managed. They will also ensure that the Governing Body and the Accountable Officer are kept up to date on all information risk issues. The role will be supported by the CCG's Corporate Services Manager (responsible for Information Governance, Risk and Records Management), the CCG's Head of ICT Service Development, and the CCG's Caldicott Guardian, although ownership of the risk assessment process will remain with the SIRO.

The IG, BI and IM&T Group is responsible for overseeing day to day Information Governance issues, developing and maintaining policies, standards, procedures and guidance, coordinating and raising awareness of Information Governance in the CCG.

All Managers within the CCG are responsible for ensuring that the policy and supporting standards and guidelines are promoted and built into local processes to ensure on-going compliance.

All staff, whether permanent, temporary or contractors are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis.

5. Training/Awareness

Information governance will be a part of induction training. All new staff will receive awareness training and information on information governance, which will include Caldicott and confidentiality, data protection, information security and freedom of information. The NHS Digital online IG Training Tool modules will be utilised and uptake monitored.

Information Governance training, including awareness and understanding of Caldicott principles and confidentiality, information security and data protection, will be mandatory for all staff. The frequency of any further information governance training will be determined as part of the CCG's organisation development plan and appraisal process.

The Governing Body member assigned to the SIRO role will undertake the strategic information risk management training at least annually.

6. Monitoring/Audit

- The CCG will monitor this policy and related strategies, policies and guidance through the Information Governance and IM&T Group.
- As assessment of compliance with requirements, within the Information Governance Toolkit (IGT) will be undertaken each year. The CCG will identify staff to undertake Administrator, Reviewer and User roles as described in the IGT.
- The Information Governance and IM&T Group will ensure implementation of the Information Governance Action Plan.
- Annual reports and proposed action/development plans will be presented to the CCG's Clinical and Management Executive Team for approval prior to submission to the IGT.
- It is assumed that both Internal and External Audit will review this and associated procedures.
- The CCG will ensure that the support infrastructure for the SIRO is in place, and is kept under regular review.

7. Information Governance Management

Information Governance management across the organisation will be co-ordinated by the IG, BI and IM&T Group. The structure and Terms of Reference of this Steering Group are shown in Appendix 2.

The responsibilities of the IG, BI and IM&T Group will include, but not be limited to:

- Recommending for approval policies and procedures, to the appropriate CCG Clinical Executive Committee (CEC).

- Recommending for approval to the CCG CEC the annual submission of compliance with requirements in the IGT and related action plan.
- Co-ordinating and monitoring the Information Governance strategy across the organisation.
- The Information Governance and IM&T Steering group will provide exception reports to the Governing Body via the CEC and individual items of action may be included within the Corporate Assurance Framework (CAF) for regular monitoring.

The IG, BI and IM&T Group will endorse Information Governance Strategy for the CCG and utilise joint and collaborative working provided by Serco, BCF Data Sharing Board and the East of England Information Governance Forum

8. Review

This policy and associated strategy will be reviewed in April 2019 or earlier if appropriate, to take into account any national changes to legislation or statutory requirements that may be required, and/or guidance from the Department of Health or other regulatory body.

Appendix 1

Legal Acts

- Data Protection Act 1998
- Human Rights Act 1998
- Freedom of Information Act 2000
- Access to Health Records Act 1990 (where not superseded by the Data Protection Act 1998)
- Computer Misuse Act
- Copyright, designs and patents Act 1988 (as amended by the copyright computer programmes regulations 1992)
- Crime and Disorder Act 1998
- Electronic Communications Act 2000
- Regulations of Investigatory Powers Act 2000 (RIPA)
- Mental Capacity Act 2005
- Health and Social Care Act 2012

Supporting Documents

- Information Security Management: NHS Code of Practice April 2007
- UK Strategy for Information Assurance:
- Protecting our information systems CSIA Cabinet Office 2004
- Lord Chancellor's code of practice on the management of records under section 46 of the Freedom of information act 2000 - November 2002
- Cabinet Office Report – Data Handling 2008

Appendix 2

Information Governance (IG) Business Intelligence (BI) and Information Management and Technology (IM&T) Steering Group

Terms of Reference

1. Purpose

The key strategic aim is to ensure Information Governance and IM&T is at the heart of the CCG and to ensure that all business and commissioned services are compliant with national standards, legislation and statutory duties.

To act as the project board for selected CCG IG and IM&T projects and to agree IM&T investments in line with national, area and local priorities.

Set the Information Governance Strategy and related policies and procedures, providing assurance to the Governing Body.

2. Objectives

- To ensure consistent and high standards of record keeping and information handling, in accordance with statutory and legal requirements.
- To support the CCG's corporate objective to transform services by improving the quality, outcome, effectiveness and efficiency of patient care and ensuring appropriate records management, data quality, confidentiality, information sharing and security measures are in place.
- To complete and submit an IG Toolkit self-assessment on behalf of the CCG, ensuring the necessary evidence is in place to support scores.
- To review, monitor and action relevant internal audits
- To review and approve Information Sharing Agreements, Privacy Impact Assessments that support new Business Case Approval Process.
- To manage and report breaches of confidentiality and security, and any other IG related incidents. Where necessary undertake or recommend remedial action and cascade learning from these events where appropriate.
- To agree the IG element of mandatory corporate training programme with HR for them to monitor.
- To develop and advise staff, general practice and our providers of best practice in relation to information governance.
- To promote and develop multi-agency information sharing to both patients and staff.
- Maintain strong working relationships with other partner organisations and develop same with newly created NHS organisations.

The Steering Group has delegated responsibility for the approval of policy / procedure. Endorsement by CEC will be sought through an exception report after each meeting for onward reporting to the Governing Body requesting ratification.

3. Frequency, Structure and Administration

Meetings of the Steering Group will be held quarterly. The Chair of the meeting may request additional meetings if necessary.

The Steering Group shall be supported administratively by the Corporate Services Team, whose duties in this respect will include:

- Preparation of the agenda and collation of papers
- Taking the minutes
- Keeping a record of matters arising and action log to be carried forward.

4. Membership

The core membership of the Committee is set out below:

Director of Corporate Affairs (Chair and SIRO)
Associate Director of Corporate Affairs and CCG Secretary (Corporate Governance, FOI Lead and Deputy SIRO and Deputy Chair)
Chief Nurse (Caldicott Guardian)
Deputy Chief Nurse (Deputy Caldicott Guardian)
Corporate Services Manager (Data Protection and IG Lead and Privacy Officer)
Corporate Services Support Manager (Information Governance SME)
Associate Director of Business Intelligence (Data Quality Lead)
Senior Information Manager
Senior ICT Service Development Manager
Strategic Clinical Services IM&T Consultant
Primary Care IT Manager
Head of PMO
GP Clinical Lead for IG, BI and IM&T *(to Provide Clinical Leadership when appointed)*

The Steering Group can invite people whose attendance is relevant to matters to be discussed. All other attendance will be at specific invitation of the Group, including attendance as an observer.

The principle of arranging a 'deputy' to attend the Steering Group meetings on behalf of members who are unable to attend will apply. Attendance will be monitored and reported six monthly.

5. Quorum

A quorum shall be the chair (or nominated deputy) and the SIRO (or their deputy) and the Caldicott Guardian (or their deputy). If these members are not available then the meeting can take place but decisions must be deferred.

6. Reporting Arrangements

The IG, BI and IM&T Steering Group will advise and assure the Governing Body of key issues through regular exception reporting to the Clinical Executive Committee (CEC). An annual report including FOI will be prepared for the Governing Body. Highlight reports for specific purposes will be prepared as required.

APPROVED BY:
IG, BI and IM&T Group
February 2017

REVIEW DATE
April 2018. The terms of reference will be reviewed on an annual basis or before if required.

Information Governance Management Framework

Heading	Requirements
Scope	The Information Governance Framework applies to: • All staff working for and on behalf of the CCG; • All types of information held or processed by the CCG (paper and electronic); • Organisations or staff holding or processing data on behalf of the CCG; • All Information Technology application systems within the CCG.
Senior Roles	Accountable Officer – Chief Officer
	Information Governance Lead – Information Governance Manager
	SIRO – Director of Corporate Affairs
	Caldicott Guardian – Director of Quality: Chief Nurse
	IT Security – Senior ICT Service Development Manager
	FOI Lead - CCG Secretary / Associate Director of Corporate Affairs
	Privacy Officer and Data Protection Lead – Information Governance Manager
	Data Quality Lead - Associate Director of Business Intelligence
	Risk Lead – CCG Secretary / Associate Director of Corporate Affairs

Key Policies	Date Ratified	Review Date
IG Strategy	July 2017	April 2019
IG Policy	July 2017	April 2019
Records Management and Lifecycle Policy	July 2015	April 2017
Code of Conduct for Confidentiality	July 2017	July 2019
Information Security Staff Policy	January 2016	January 2018
Removable Media Policy	July 2017	July 2019
Data Quality Policy	July 2017	July 2019
Information Governance Forensic Readiness Policy	April 2017	April 2019

Key Policies (Cont'd)	Date Ratified	Review Date
Destruction and Disposal of Unwanted Information and Equipment	November 2016	October 2018
Risk Management Policy	September 2015	September 2017
Freedom of Information Act Policy & Publication Scheme	July 2015	July 2017
Data Protection and Access to Records Policy	July 2015	April 2017
Cambridgeshire Information Sharing Framework	January 2017	January 2019
Registration Authority Policy and Procedure (NEL CSU)	October 2016	October 2018
Safe Haven Policy	July 2017	July 2019
Controlled Environment for Finance (CEfF)	July 2017	July 2019
Policies are available to staff and public via the CCG extranet and website, staff are notified of updates or new policies through articles published in the staff bulletin.		

Key Governance Bodies	Information Governance, Business Intelligence and Information Management and Technology (IG, BI & IM&T) Steering Group (Quarterly) Clinical and Executive Committee (CEC) See Appendix 1 – Governance Structure
Resources	Information Governance Manager Information Governance Support Manager Senior ICT Service Development Manager CCG Secretary – Freedom of Information Lead, Risk and Business Continuity Lead Data Quality Lead - Associate Director of Business Intelligence Serco SLA identifies areas where specialist advice and support is provided -signed data processing agreement in place Information Governance and Legal Manager – support provided by Serco Information Technology Infrastructure – Serco Information Technology Security Manager – Serco Registration Authority – Head of RA, NEL CSU Information Management and Technology budget identifies resources for IT security e.g. encryption and is reported to IG. BI & IM&T Steering Group
Governance Framework	Information Asset Owners – named Directors to conduct annual review and risk assessments. Critical information assets to be identified and regularly reviewed as part of the business continuity plans. Staff contracts include Information Governance responsibilities. Information Governance component embedded in contracts. Confidentiality agreement to be signed by all temps, volunteers etc. Records Management leads for each base identified. The CCG's Project Management System includes Information Governance component and requirement to complete privacy impact assessment.
Training & Guidance	IG Training Tool mandatory modules agreed for all staff. Training figures are reported quarterly to the IG, BI & IM&T Steering Group Guidance for line managers on individual training needs available.

	Corporate Induction Training: The induction pack includes information governance related guidance - reviewed January 2016. Staff Bulletin: Information Governance messages are a regular feature in the staff newsletter. These are based on the learning from incidents and also any new guidance requiring promotion to staff. Information Governance policies are available via the staff extranet and the public website. Staff are informed via email or staff bulletin of recently reviewed and revised policies or procedures. Confidentiality Awareness Campaign disseminates key messages via email to staff as appropriate.	
Risk and Incident Management	Each Directorate will be responsible for developing and maintaining a Directorate Risk Register which will be part of the overall Service Performance Framework Risk Register. Directorates are required to nominate a Risk Co-ordinator who will undertake Datix training. The CCG will use the CCG Assurance Framework and Risk Register (CAF), Service Performance Framework Risk Register, Programme Area and LCG Risk Registers to prioritise and manage risks. Incident management and reporting is included in the Integrated Risk Management Policy and available to staff via the Extranet. The Datix reporting system is used for reporting, investigation and management of IG incidents and near misses. All incidents reported on Datix will be reviewed by the IG Manager using the CCG assessment checklist to identify SI levels and reporting procedures. Relevant leads are identified for management/review of IG related incidents. SI reporting is managed by the Risk Manager. IG risks and incident reporting are standing items on the IG, BI & IM&T steering group agenda. Shared learning is disseminated via all staff email or staff bulletin as appropriate.	
Document Background	The IG Management Framework was adopted from the Cambridgeshire and Peterborough Cluster PCT and reviewed April 2013. The Clinical Management Executive Team (CMET now known as CEC) agreed the review April 2013.	
Revisions for this Version	Annual review of IG Management Framework undertaken: • Amendment to job roles as applicable. • Policy review dates confirmed and updated where required.	 January 2017 January 2017
Approval/Sign off	Approved by Information Governance, BI & IM&T Steering Group Endorsed by Clinical & Executive Committee (CEC)	February 2017 March 2017

High Level CCG Governance Structure