Derby and Derbyshire
Clinical Commissioning Group

INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK

Document History

Document Reference:	IG01
Document Purpose:	The document compliments all other Information Governance policies and sets out the management arrangements for information governance for Derby and Derbyshire CCG
Approved	8th November 2018
Approving Committee:	Derby and Derbyshire CGG Governance Committee
Version Number:	1.0
Status:	
Next Revision Due:	November 2019
Developed by:	Derby and Derbyshire CCG's Corporate Delivery Team
Policy Sponsor:	Director of Corporate Delivery
Target Audience:	All Staff within the CCG whether operating directly or providing services to other organisations under a service level agreement or joint agreement and to none executive directors, contracted third parties (including agency staff), locums, students, volunteers, trainees, visiting professionals or researchers, secondees and other staff on temporary placements within the organisation.
Associated Documents:	All Information Governance Policies and the Data Security & Protection Toolkit
Shared with Public	Yes/No (delete as appropriate)

Revision History

Version	Revision date	Summary of Changes
1.0	August 2013	Revised in line with NHS England Policies and updated to reflect version 11 of the Information Governance Toolkit
1.1	August 2014	Revised in line to reflect Version 12 of the Information Governance Toolkit
FINAL 1.2	August 2014	Approved at IG Product Group
FINAL 1.3	September 2014	Amended – not circulated
FINAL 1.4	October 2014	Appendix 3 – training matrix amended – circulated
Draft 1.5	June 2015	Revised to reflect Version 13 of the Information Governance Toolkit. . Reference to GEM CSU changed to Arden & GEM CSU, contact details and web links updated.
Draft 1.6	July 2015	Amended in line with comments from CCG IG Leads
Draft 1.7	June 2016	Annual review
Final 1.8	June 2016	Annual review
Draft 1.9	June 2017	Annual review
Draft 1.10	November 2017	Reviewed by IG Working group
Final 1.11	November 2017	Approved at IGC
Draft 1.12	October 2018	Annual review
Draft 1.13	October 2018	Reviewed by IGWG
FINAL 1.14	November 2018	Approved by Governance Committee

Policy Dissemination information

Reference Number	Title	Available from
IG01	Information Governance Management Framework	

Contents

Information Governance Management Framework

1.0 Introduction

This framework applies to Derby and Derbyshire Clinical Commissioning Group (CCG), subsequently referred to in this document as the CCG. It includes:

Robust Information Governance requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. The way the CCG will deliver this is documented within this Information Governance Management Framework. The Framework will be recommended by the Information Governance Assurance Group (IGAG) for approval by the Derby and Derbyshire CCG Governance Committee.

This document sets out the CCG's approach to embedding robust information governance throughout the CCG.

This framework is a standalone document and provides a summary/overview of how the CCG is addressing the IG agenda and reflects the capacity and capability of the CCG.

2.0 Purpose and Scope

The purpose of this policy is to establish employee responsibility and the rules of conduct for all members of staff regarding the CCG's Information Governance Framework. This policy applies to all staff within the CCG whether operating directly or providing services to other organisations under a service level agreement or joint agreement. and to non-executive directors, contracted third parties (including agency staff), locums, students, volunteers, trainees, visiting professionals or researchers, secondees and other staff on temporary placements within the organisation.

3.0 Policy Statement

NHS Digital mandates that the Data Security & Protection Toolkit (DSPT) is completed by all organisations that commission or provide services within and to the NHS.

The DSPT requires that 'There is a data security and protection policy or policies that follow relevant guidance.' and there are 'policies in place that explain the organisation's plan or principles for data protection, data quality, records management, data security, registration authority and network security and refer to the organisation's procedures for implementing the policies'.

An Information Governance Management Framework (IGMF) is required to be in place to ensure that the Information Governance agenda is owned and implemented in a structured manner.

4. 0 Senior Information Governance Management Details

4.1 Organisational Roles & Accountability

- The CCG will appoint an Information Governance (IG) Lead, Senior Information Risk Owner (SIRO), Data Protection Officer (DPO) and Caldicott Guardian. These designated roles will be reported in the CCG's DSPT return.

- The roles of the Senior Information Risk Owner, a Caldicott Guardian and Data Protection Officer will be undertaken by senior members of the organisations management team and will be members of the Governing Body.

- The DPO will be an independent position and will report directly to the Accountable Officer who will oversee the strategic direction and context of the work of this role.

- The Information Governance Lead is a senior representative in the organisation who leads and co-ordinates the information governance works programme and is line managed by a member of the senior management team.

- The Accountable Officer has overall accountability and responsibility for Information Governance and is required to provide assurance through the Statements on Internal Control that all risks to the CCG, including those relating to information, are effectively managed and mitigated.

- The Records Lead is an individual/s with clear responsibility for the management of the records of an organisation from the time they are created up to their eventual disposal. This may include naming, version control, storing, tracking, securing and destruction (or in some cases, archival preservation) of records

- An Information Asset Owner is a senior individual 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

- Information Asset Administrators are usually operational members of staff who understand and are familiar with information risks in their area or department. Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date

4.2 The CCG Information Governance Lead will:

- Develop and maintain comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, e.g. an overarching high level strategy document supported by corporate and/or directorate policies and procedures

- Ensure that there is senior management awareness and support for IG resourcing and implementation of improvements

- Provide direction in formulating, establishing and promoting IG policies

- Establish working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives

- Ensure that assessment and improvement plans are prepared for approval by the senior level of management in a timely manner and in line with national reporting requirements

- Ensure 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 in line with the DSPT requirements and as detailed in the CCG's training needs analysis

- Liaise with other committees, working groups and programme boards in order to promote and integrate IG standards

- Monitor information handling activities to ensure compliance with law and guidance

- Provide a focal point for the resolution and/or discussion of IG issues.

- Undertake annual training required by the role as identified in the CCG Training Needs Analysis.

4.3 The SIRO will:

- Take ownership of the organisation's information risk policy and information risk management strategy. All key information assets will be identified and their details included in an Information Asset Register.

- Take ownership of the risk assessment process for information and cyber security risks, including review of an annual information risk assessment to support and inform the Annual Governance Statement.

- Ensure that Information Asset owners will be identified for each key information asset.

- Ensure that all systems information assets have an assigned information asset owner.

- Ensure that all staff assigned responsibility for co-ordinating and implementing information risk management will be appropriately trained to carry out their role.

- Ensure that Information Asset Owners carry out risk reviews of the assets for which they are accountable, the frequency of review depending upon the importance of the asset and the nature of the risk environment but at least annually.

- Lead and implement the information governance risk assessment and advise the Governance Committee on the effectiveness of risk management across the organisation.

- Undertake annual training required by the role as identified in the CCG Training Needs analysis.

- To be added to and maintain registration on the National Register of SIROs.

4.4 The Data Protection Officer:

- Provide support, advice and assurance of compliance of Data Protection Legislation across the CCG.

- Maintain expert knowledge of data protection law and practices and how they apply to the business of the organisation

- Be the first point of contact within the organisation for all data protection matters.

- Support programmes of work from inception to ensure that data protection is addressed by default and in the design of new systems and information processes.

- Ensure that any supporting team are deployed appropriately and that they are appropriately trained and maintain their expertise.

- Be available to be contacted directly by data subjects – the contact details of the Data Protection Officer will be published in the organisation's Privacy Notice.

- Ensure that appropriate confidentiality is maintained in the performance of his or her tasks.

- Support programmes and initiatives that involve the development of new or innovative information processes on the need for Data Protection Impact Assessment.

- Support and advise programmes and initiatives in conducting data protection impact assessments, and to assure the proposed mitigations.

- Provide advice to programmes on when a Data Protection Impact Assessment is required.

- Be the first point of contact for the Information Commissioner's Office (ICO).

- Cooperate with the ICO in any matters relating to data protection compliance including provision of evidence of compliance, and in relation to breach management.

- Consult with the Information Commissioner where proposed processing poses a high risk in the absence of proposed mitigations.

- Develop or advise senior management on the development and establishment of policies, procedures and other measures to ensure compliance with the GDPR, including but not limited to:

  - Records of processing activities
  - Data protection by design and default
  - Data Protection Impact Assessment (DPIA)
  - Fair processing

4.5 The Caldicott Guardian will:

- Be added to and maintain registration on the National Register of Caldicott Guardians.
- Identify the support necessary to ensure work related to confidentiality and data protection is appropriately carried out.
- Provide a plan for the Caldicott Function of the CCG.
- Ensure all staff assigned responsibility for co-ordinating and implementing the confidentiality and data protection work programme have been appropriately trained to carry out their role.
- Identify the work necessary to provide Confidentiality and Data Protection Assurance.
- Be a senior person responsible for protecting the confidentiality of patient and service user information and enabling appropriate information sharing.
- Undertake annual training required by the role as identified in the CCG Training Needs Analysis.

4.6 The Information Asset Owner will:

- Be a Director of the CCG.
- Identify and document the scope and importance of all Information Assets they own. This will include identifying all information necessary in order to respond to incidents or recover from a disaster affecting the Information Asset.
- Take ownership of their local asset control, risk assessment and management processes for the information assets they own. This includes the identification, review and prioritisation of perceived risks and oversight of actions agreed to mitigate those risks.
- Provide support to the organisation's SIRO and the appropriate risk management group to maintain their awareness of the risks to all Information Assets that are owned by the organisation and for the organisation's overall risk reporting requirements and procedures.
- Ensure that staff and relevant others are aware of and comply with expected IG working practices for the effective use of owned Information Assets. This includes records of the information disclosed from an asset where this is permitted.
- Provide a focal point for the resolution and/or discussion of risk issues affecting their Information Assets.
- Ensure that the organisation's requirements for information incident identification, reporting, management and response apply to the Information Assets they own. This

includes the mechanisms to identify and minimise the severity of an incident and the points at which assistance or escalation may be required.

- Foster an effective IG culture for staff and others who access or use their Information Assets to ensure individual responsibilities are understood, and that good working practices are adopted in accordance with the organisation's policy.

- Ensure there is good understanding of the hardware and software composition of their assigned assets to ensure their continuing operational effectiveness. This includes establishing and maintaining asset records that will help predict when asset configuration changes may be necessary.

- Undertake annual training required by the role as identified in the CCG Training Needs Analysis

4.7 Information Asset Administrators will:

- Be a Deputy or Head of Service of the CCG.

- Ensure that policies and procedures are followed when using an information asset.

- Recognise actual or potential security incidents.

- Consult their IAO on incident management.

- Assist the IAO to ensure that information asset registers are accurate and up to date, for example by reporting when an information asset they use is no longer required.

- Undertake annual training required by the role as identified in the CCG training needs analysis.

4.8 The Programme Management Office will:

- Ensure that all projects are assessed for privacy risks to individuals in the collection, use and disclosure of personal information.

- Ensure that appropriate Data Protection Impact Assessments are carried out in line with the Project Management Office Governance arrangements.

5.0 Key Policies

The CCG will provide the following policies (or equivalent) to set out scope and intent in terms of embedding Information Governance processes throughout the organisation:

- An Overarching Information Governance Policy

- A Confidentiality and Data Protection Policy

- An Information Security Policy
- A Freedom of Information Policy
- An Information Lifecycle Management Policy (Records Management and Information Quality)

In particular the CCG will implement policies as required to support confidentiality, security and records management processes in addition to this Information Governance Management Framework

6.0 Governance Arrangements

The following governance arrangements have been agreed:

- The Governance Committee 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 IG updates within the corporate report.
- The Governance Committee will approve the Information Governance Management Framework and the Information Governance Committee Terms of Reference.
- The Information Governance Assurance Group will have responsibility for the Information Governance Agenda supported by identified senior roles i.e. Caldicott Guardian, SIRO, IG Lead and Data Protection Officer.
- The Information Governance Assurance Group will be responsible for approving all protocols, strategies and procedures across the IG agenda.
- The Governance Committee will be responsible for approving all policies across the IG agenda.
- The Information Governance Assurance Group will provide regular assurance reports to the Governance Committee.
- Responsibility and accountability for Information Governance will be cascaded through the organisation via staff contracts, contracts with third parties, Information Asset Owner arrangements and departmental leads.
- Key information governance messages will be developed by the CCG's Corporate Delivery Team for dissemination across the CCG.

For further detail about the Information Governance Assurance Group please the Terms of Reference appendix 1.

7.0 Resources

Key staff involved in the Information Governance Agenda, below those at Executive Team level, is the Derbyshire CCG's Corporate Delivery Team, which comprises of an Information Governance Manager and an Information Governance Support Officer.

8.0 Training Guidance

Staff need clear guidelines on expected working practices and on the consequences of failing to follow policies and procedures.

The approach to ensuring that all staff receive training appropriate to their roles will be detailed and provided by the CCG's Corporate Delivery Team. The Corporate Delivery Team will assist the CCG in achieving 95% take up of mandatory information governance training, known as 'Data Security Awareness Level 1' and advise/manage staff to undertake further specialist information governance training as required.

Mandatory annual Information Governance Training should be completed by all third party contractors.
Training will be made available via:

- The Electronic Staff Record (ESR) and
- The NHS Digital online training portal https://nhsdigital.e-lfh.org.uk/

9.0 Incident Management

Clear guidance on incident management procedures will be documented and staff will be made aware of their existence, where to find them and how to implement them by the Corporate Delivery Team,

All incidents will be discussed at the CCG Information Governance Committee (or equivalent) on a monthly basis.

10.0 Equality & Diversity Impact Assessment

The CCG's aim is to design and implement policy documents that meet the diverse needs of the services, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.

This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.

In carrying out its functions, the CCG must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which the organisation is responsible, including policy development, review and implementation.

11.0 Monitoring and Compliance

The IGMF will be reviewed at least annually in line with the Data Security and Protection Toolkit or amended as required to reflect changes in organisational ownership.

12.0 Further Information or Guidance

Contact the Corporate Delivery Team - DDCCG.IGteam@nhs.net

13.0 References

NHS Code of Confidentiality:
https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

The. Data Security & Protection Toolkit
https://www.dsptoolkit.nhs.uk

Guide to the Notification of Data Security & Protection Incidents
https://www.dsptoolkit.nhs.uk/Help/29

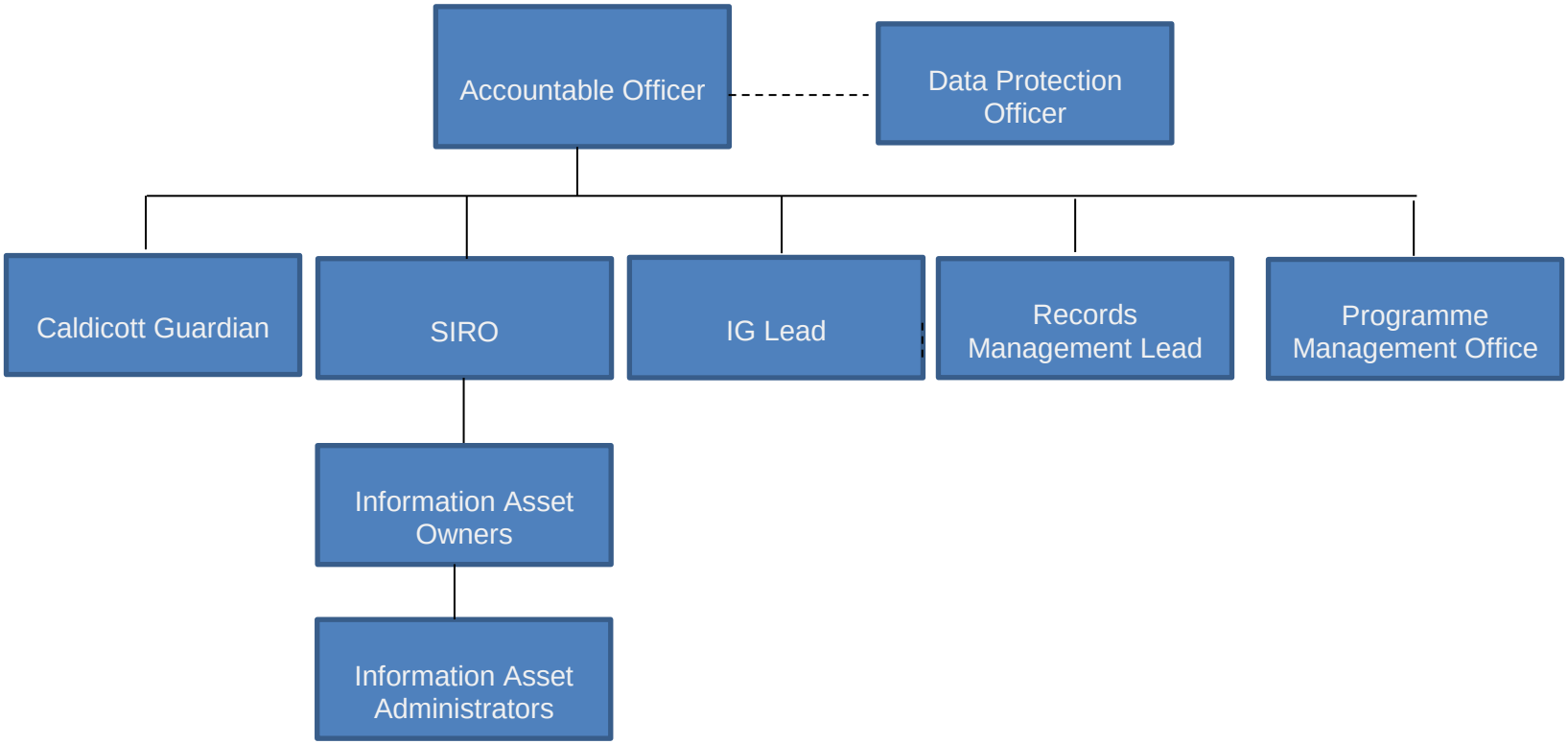
NHS Information Risk Management
https://digital.nhs.uk/article/1201/Information-security-management-NHS-code-of-practice

The Caldicott Review: Information Governance in the Health and Social Care System
https://www.gov.uk/government/publications/the-information-governance-review

Appendix 1 Terms of Reference for Information Governance Committee

To be added once agreed

Appendix 2 Information Governance Operational Structure



Derby and Derbyshire
Clinical Commissioning Group

Appendix 3 Committee Reporting Structure

CCG Information Governance Working Group

Terms of Reference

Will be added once agreed.

Appendix 4- Training Needs Analysis

To be added once approved.

Appendix 5 Information Governance Related Policies, Procedures & Guidance

Name of Policy	Policy Approval Date	Approving Body/Individual
Corporate Information Security Policy		
Confidentiality & Data Protection Policy		
Data Protection Policy		
Data Quality Policy		
Email Policy		
Freedom of Information (FOI) Policy		
Incident Reporting Policy		
Information Governance Management Framework (IGMF)		
Information Governance Policy		
Information Lifecycle Policy (including information quality)		
Information Risk Policy		
Information Security Policy		
IT Acceptable Use Policy		
Network Security Policy		
Records Management Policy		

Name of Procedure	Procedure Approval Date	Approving Body/Individual
Confidentiality Audit Process		
Electronic Remote Working Guidance (see IG Briefing Pack/Handbook		
Incident Reporting Procedure		
Mobile Working Procedure		
Privacy Impact Assessment (PIA) Procedure		
Safe Haven Procedure		
Subject Access Request (SAR) Procedure		
Derbyshire Wide Protocol for IG Incidents		

Local Guidance	Approval Date	Approving Body/Individual
Fair Processing Notice		
Privacy Notice		
Staff Code of Conduct		

Dissemination Process

All the above policies and procedural documentation will be disseminated to staff by the CCGs via the staff intranets.

Appendix 5 Data Security & Protection Toolkit – Small Organisation

Requirements List