NHS
Derby and Derbyshire
Clinical Commissioning Group

Information Governance Policy

Document History

Document Reference:	IG02
Document Purpose:	An Information Governance Policy is a statement of the organisation's approach and intentions to fulfilling statutory and organisational responsibilities. It will enable management and staff to make correct decisions, work effectively and comply with relevant legislation and the organisations aims and objectives
Date Approved:	10th January 2019
Approving Committee:	Derby and Derbyshire CCG Governance Committee
Version Number:	1.0
Status:	
Next Revision Due:	January 2020
Developed by:	Derby and Derbyshire Clinical Commissioning Group
Policy Sponsor:	Executive Director Corporate Strategy & Delivery
Target Audience:	The procedure applies to all permanent, temporary staff and secondees of the CCG
Associated Documents:	All Information Governance Policies and the Data Security and Protection Toolkit

Revision History

Version	Revision date	Summary of Changes
1	July 2013	Amended in line with Caldicott Review and CCG Information Governance Toolkit version 11
1.1	July 2014	Review for CCG comments and in line with version 12 of the IG Toolkit
1.2	August 2014	Review at IG Product Group and approval as FINAL.
2.0	Sept 2014	Reviewed at IGC
2.1	July 2016	Draft for review
2.2	July 2016	Final
2.3	November 2017	Draft – annual review – updated legislation – EU GDPR Regulation 2016
3.0	November 2017	Final – approved at IGC
3.1	November 2018	Draft for annual review
3.2	November 2018	Further changes made
4.0	January 2019	Final - Approved at Derby and Derbyshire Governance Committee

Policy Distribution and Implementation

Reference Number	Title	Available from
IG02	Information Governance Policy	*Local arrangements*

Contents Number **Page**

1 Introduction

1.1 This policy applies to the Derby and Derbyshire Clinical Commissioning Group, subsequently referred to in this document as the CCG.

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.

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

1.3 The Information Governance (IG) framework for health and social care is formed by those elements of law and policy from which applicable information governance standards are derived, and the activities and roles which individually and collectively ensure that the set standards are clearly defined and met.

2 Policy Statement

2.1 An Information Governance Policy is a statement of an organisation's approach and intentions to fulfilling its statutory and organisational responsibilities. It will enable management and staff to make correct decisions, work effectively and comply with relevant legislation and the organisation's aims and objectives.

2.2 This document sets out the high level principles across the CCG for confidentiality, integrity and availability of information (information governance) to promote and build a level of consistency across the community on these principles.

Information Governance is defined as:

"the structures, policies and practice of the DH, the NHS and its suppliers to ensure the confidentiality and security of all records, and especially patient records and to enable the ethical use of them for the benefit of individual patients and the public good". ('Information Governance in the Department of Health and the NHS', 2006)

2.3 Failure by any employee of the CCG to adhere to corporate policy and its associated procedures and guidelines may be viewed as a serious matter and may result in disciplinary action in line with the CCG's HR disciplinary policy.

3 Scope

3.1 It is the responsibility of the CCG's Executive Directors, Functional Directors, Assistant Directors, Heads of Service and Senior Managers to ensure that the Information Governance Policy is brought to the attention of all staff and that staff have appropriate training on information security and confidentiality on induction and annually thereafter.

3.2 The Information Governance Policy is supported by a range of corporate policies covering the key areas of Information Governance including:

- Confidentiality and Data Protection

- Information security and risk
- Information lifecycle management including records management and information quality
- Corporate governance including requirements under the Freedom of Information Act 2000.

The Information Governance Management Framework details the arrangements for compliance with the legal and national regulatory framework.

3.3 This policy covers all aspects of processing activities that relate to (but is not limited to):

- Patient/client/service user information
- Staff and personnel information
- Organisational, business and operational information
- Research, audit and reporting information

3.4 This policy covers all aspects of handling the way the organisation holds, obtains, records, uses and shares information.

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

4 Organisational responsibility under the Policy

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

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

4.3 The CCG will sustain a robust Information Governance Framework by:

- Demonstrating compliance with the key IG standards through achievement of at least level 'Standards met' within the NHS Digital Data Security and Protection Toolkit and ensuring plans are in place to progress beyond this minimum where it has been achieved.
- Mandating all staff to complete basic IG training (delivered via the Data Security Awareness level1 module) annually appropriate to their role through ESR or other method approved by the Department of Health;
- Continuing to report on the management of the information risks in statements of internal controls and to include details of data loss and confidentiality breach incidents in annual reports;

4.4 The CCG aims to ensure organisations contracted to deliver services also achieve a compliant information governance standard (Data Security and Protection Toolkit compliance). This includes commissioned services delivering both clinical and non-clinical services.

5 Governance

5.1 The CCG's Corporate Delivery team will be responsible for delivering robust IG support which provides a full range of expert advice, guidance, training and support in data protection and confidentiality, information risk management, security, data quality, information management.

5.2 Members of the Corporate Delivery Team will be members of the Information Governance Working Group (IGWG), which will be responsible for the operational delivery of the IG agenda.

5.3 The IGWG will report to the Information Governance Assurance Group (IGAG) which will be responsible for recommending policies and approving procedures[1].

5.4 The IGAG will report to the CCG's Governance Committee which will approve IG Policies.

6 Information Governance Strategy/Improvement Plan

6.1 The CCG has an associated Information Governance Management Framework (IGMF) which details the way that the CCG will deliver against the national and legal information governance requirements. This document provides a summary/overview and sets out an overarching framework for the strategic Information Governance agenda at the CCG and is supported by an Information Governance improvement plan, which is monitored by the Information Governance Working Group or equivalent.

7 Roles and Responsibilities

Overall accountability across the organisations lies with the Accountable Officers who have overall responsibility for establishing and maintaining an effective information governance assurance framework for meeting all statutory requirements and adhering to guidance issued in respect of procedural documents. All staff must adhere to the CCG's policies and procedures relating to the processing of personal information. All staff members are responsible for maintaining compliance with the Data Protection Principles and the General Data Protection Regulation (GDPR) and for reporting non-compliance through the CCG incident reporting process.

7.1 Senior Information Risk Owner (SIRO)

The SIRO will:

- take overall ownership of the organisation's information and cyber security risk policy;
- oversee the role of Information Asset Owner;
- sign off the annual toolkit submission;
- act as champion for information risk on the Board and provide written advice to the Chief Executive Officer on the content of the organisation's statement of internal control in regard to information risk;

[1] As an interim measure until 31st March 2019 the IGWG will report to the CCGs Governance Committees in Common which will approve IG policies and procedures.

- understand how the strategic business goals of the CCG may be impacted by information risks, and how those risks may be managed;
- implement and lead the NHS information governance risk assessment and management processes within the CCG;
- advise the Board on the effectiveness of information risk management across the CCG; and
- undertake training as necessary to ensure they remain effective in their role as SIRO.

  The SIRO will be supported in this role by the CCG's Corporate Delivery Team

7.2 Data Protection Officer (DPO)

The Data Protection Officer will:

- provide support, advice and assurance of compliance across the organisation;
- 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;
- manage the data protection compliance team if applicable;
- 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, which 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 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; and

- 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

7.3 Caldicott Guardian

The Caldicott Guardian acts as the ‘conscience’ of an organisation, actively supporting work to facilitate and enable information sharing, advising on options for lawful and ethical processing of information as required.
The Guardian will:

- ensure that the CCG satisfies the highest practical standards for handling patient identifiable information;
- facilitate and enable information sharing and advise on options for lawful and ethical processing of information;
- represent and champion information governance requirements and issues at Board level;
- ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff; and
- oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside the CCG;
- undertake necessary training as set out in the CCG Training needs analysis; and
- the Caldicott Guardian will be supported in this role by the CCG’s Corporate Delivery Team.

7.4 Information Asset Owners

Information Asset Owners (IAOs) will:

- lead and foster a culture that values, protects and uses information for the benefit of patients;
- oversee the role of Information Asset Administrator;
- sign off the Data Flow Mapping and Asset Registers;
- know what information comprises or is associated with the asset, and understands the nature and justification of information flows to and from the asset;
- know who has access to the asset, whether system or information, and why, and ensures access is monitored and compliant with policy;
- understand and address risks to the asset, and providing assurance to the SIRO;

- Undertake necessary training as set out in the CCGs Training needs analysis; and
- Further information can be found in the Information Governance Management Framework at 4.6.

7.5 Information Asset Administrators

Information Asset Administrators will:

- be accountable to the IAOs;
- support the IAOs in providing assurance that information risk is being managed effectively for their assigned information assets;
- ensure all staff complete information governance training as set out in the CCG Training needs analysis;
- on an annual basis, be responsible for local assessment of data collections to establish an information asset register (IAR) and Data Flow Map (DFM); and
- audit staff compliance with Information handling requirements.

7.6 Line Managers

Line managers will take responsibility for ensuring that the information governance policy is implemented within their group or directorate.

7.7 Staff

It is the responsibility of each employee to:

- adhere to the policy;
- complete annual Data Security and Protection training;
- Complete any role specific training such as Records Management for example; and
- report any information incidents through the incident recording mechanism.

All staff must make sure that the organisation's information systems are used and operated appropriately and as set out in the standard operating procedures of the organisation.

8 Use of Information

The CCG recognises that as a Clinical Commissioning Group it does not have legal rights to process personal confidential data for commissioning purposes and will use anonymised, pseudonymised and aggregated data for that purpose.

8.1 The CCG will:

- proactively use information within the organisations and with partner agencies, both for the care of service users and for service management as determined by law, statute and best practice;

- put in place effective arrangements to ensure the confidentiality, security and quality of personal confidential information and other sensitive information; and
- ensure information within the organisations is of the highest quality in terms of completeness, accuracy, relevance, accessibility and timeliness.

9 Confidentiality

9.1 All members of staff working within the CCG are bound by the Common Law Duty of Confidentiality, in addition to their contract of employment, code of professional practice or other applicable ethical standards and as such, can be held personally liable for any breaches of confidentiality. If service user confidentiality is breached, this may lead to disciplinary action, a personal fine, and/or employees can be held personally responsible for a civil action.

9.2 The CCG will establish and maintain policies to ensure compliance with the Freedom of Information Act (2000). A Publication Scheme will be maintained in line with the Information Commissioner's Office (ICO) model Publication Scheme and this is available for all service users on each CCG Internet site. This will be maintained and updated frequently in line with the guidance.

9.3 Patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients. This information will inform patients of the use of their information, which agencies their information will be shared with and the circumstances where explicit consent will be sought.

9.4 The CCG will, where there is a defined purpose (or set of), which are beneficial and justifiable, sign up to information sharing protocols with partner organisations, provided these protocols are set out within the boundaries of applicable legislation and regulation and do not compromise the organisation or the confidentiality of the personal/sensitive data that it holds.

10 Legal Compliance

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

10.2 The CCG will establish and maintain policies to ensure compliance with Data Protection Legislation which includes the Data Protection Act 2018, EU General Data Protection Regulations 2016, the Human Rights Act and the Common Law Duty of Confidentiality.

10.3 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, Protection of Children Act).

11 Information Security

11.1 The CCG will promote effective confidentiality and security practice to its staff through policies, procedures and training. Contractual arrangements with third parties and suppliers will include agreement on the classification of confidentiality, and how this will be applied. This will ensure the CCG maintains the security of organisational information processing facilities and information assets,

11.2 CCG staff will be trained in the use of systems and procedures, to ensure the quality and appropriate handling of information, in order to minimise risks to the organisation from poor information governance.

11.3 Guidance from the Department of Health (DH) states specifically that **no** patient/person information should be held on any mobile devices unless the device is encrypted to the approved standard. This includes data held on USB memory sticks, CD-ROM, DVD, mobile phones and tablets. Safe Haven Procedures will be implemented for the secure transfer of any person identifiable information.

12 Information Quality Assurance

12.1 The CCG will establish and maintain policies and procedures for information quality assurance and the effective management of records and will promote information quality and effective records management through policies, procedures, user manuals and training.

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

13 Equality and Diversity

The CCG aims 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.

13.2 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.

13.3 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.

14 Due Regard

14.1 This policy has been reviewed in relation to having due regard to the Public Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

15 Monitoring compliance and effectiveness, auditing arrangements

15.1 Compliance with the Information Governance Assurance Framework will be assessed by the annual completion of the Data Security and Protection Toolkit. Formal reports will be provided to the CCG's Governance Committee (on delegated authority) throughout the year. The toolkit will be signed off by the CCG's SIRO prior to submission.

15.2 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. As part of the training and awareness programme, employees and third party contractors will also be made aware of definitions of incidents/weaknesses and the process for dealing with them.

16 Review and revision arrangements

16.1 This policy will be reviewed as per the review data on the policy front sheet; however it will be reviewed particularly where it is affected by major internal or external changes such as:

- Legislation
- Practice change or change in system/technology
- Changing methodology
- Reorganisation

17 Training Requirements

17.1 Users will be trained in the use of systems and procedures to ensure the quality and appropriate handling of confidential information, in order to minimise risks to the organisation from poor information governance.

17.2 All staff will receive mandatory induction training covering all aspects of Information Governance and annual refresher updates through ESR or the e-learning for Healthcare website. Awareness raising of the key information governance principles will be implemented through regular team briefings, team meetings and awareness raising sessions.

17.3 A staff Code of Conduct for Information Security and Confidentiality will be updated annually and be available to all staff via the Intranet and in hard copy where applicable. This gives staff the key points regarding confidentiality and information security and best practice guidance.

17.4 Staff with key roles (e.g. SIRO/Caldicott Guardian/Information Asset Owner/DPO) will undertake annual training relevant to their role.

18 References

NHS Information Governance: Guidance on Legal and Professional Obligations
https://www.gov.uk/government/publications/nhs-information-governance-legal-and-professional-obligations

Handbook to the NHS Constitution
https://www.gov.uk/government/publications/the-nhs-constitution-for-england/the-nhs-constitution-for-england

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

Data Security and Protection Toolkit
https://dsptoolkit.nhs.uk

NHS Care Record Guarantee
http://systems.hscic.gov.uk/rasmartcards/documents/crg.pdf

Information Security Management: NHS Code of Practice
http://systems.hscic.gov.uk/infogov/codes/securitycode.pdf

Records Management Code of Practice for Health & Social Care 2016
https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga

Caldicott Guardian Manual 2017
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf

NHS Digital Guide to the Notification of Data Security & Protection Incidents. Sept 2018.
https://www.dsptoolkit.nhs.uk/Help/29

NHS Information Risk Management
http://systems.hscic.gov.uk/infogov/security/risk/inforiskmgtgpg.pdf

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

General Data Protection Regulations 2016
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The Data Protection Act 2018
https://ico.org.uk/for-organisations/data-protection-act-2018/

Your Data: Better Security, Better Choice, Better Care
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/627493/Your_data_better_security_better_choice_better_care_government_response.pdf