NHS
Leeds
Clinical Commissioning Group

INFORMATION GOVERNANCE POLICY AND MANAGEMENT FRAMEWORK

Version:	1.3
Ratified by:	Audit Committee
Date ratified:	18 November 2020
Name & Title of originator/author:	Karen Rowe, Information Governance Manager
Name of responsible committee/individual:	Information Governance Committee
Date issued:	November 2020
Review date:	November 2021
Target audience:	All Staff

Executive Summary

This aim of this policy is to ensure that all staff understand their responsibilities with regard to any information which they come into contact with in the course of their work and to provide assurance to the Governing Body that such information is dealt with legally, securely, efficiently and effectively.

The policy outlines the responsibilities of all staff in regard to Information Governance and identifies the CCG's obligations in respect of legal compliance and information security. In addition, the annual IG work plan for raising staff awareness of their responsibilities is included as an appendix to this policy.

The CCG will establish, implement and maintain procedures linked to this policy to ensure compliance with the General Data Protection Regulation (GDPR) (EU) 2016/679 and Data Protection Act 2018 (DPA), Freedom of Information Act 2000 (FOI) and other related legislation and guidance, contractual responsibilities and to support the assurance standards of the Data Security and Protection Toolkit (DSPT).

This policy supports the CCG in its role as a commissioner of health services and will assist in the safe sharing of information with its partner agencies.

Equality Statement

This policy applies to all employees, Governing Body members and members of Leeds Clinical Commissioning Group's Partnership irrespective of age, race, colour, religion, disability, nationality, ethnic origin, gender, sexual orientation or marital status, domestic circumstances, social and employment status, HIV status, gender reassignment, political affiliation or trade union membership.

A full Equality Impact Assessment is not considered to be necessary as this policy will not have a detrimental impact on a particular group.

Contents

1 Introduction

NHS Leeds Clinical Commissioning Group (CCG) recognises the importance of reliable information, both in terms of the clinical management of individual patients and the efficient management of services and resources. The CCG also recognises the duty of confidentiality owed to patients, families, staff and business partners with regard to all the ways in which it processes, stores, shares and disposes of information.

This overarching Information Governance Policy and Management Framework sets out how the CCG will meet their information governance obligations and outlines the underlying operational policies and procedures which will enable the CCG to fulfil their information governance responsibilities.

The policy provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of confidential, business sensitive and personal information

2 Scope

This policy must be followed by all staff who work for or on behalf of the CCG including those on temporary or honorary contracts, secondments, volunteers, pool staff, Board members, students and Leeds City Council staff working on behalf of the CCG. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

This policy and framework covers all aspects of information within the organisation, including (but not limited to):

- Patient/Client/Service User information
- Personnel/Staff information
- Organisational information
- Structured and unstructured record systems - paper and electronic
- Photographic images, digital, text or video recordings including CCTV
- All information systems purchased, developed and managed by/or on behalf of the organisation
- CCG information held on paper, floppy disc, CD, USB/Memory sticks, computers, laptops, tablets, mobile phones and cameras

The processing of all types of information, including (but not limited to):

- Transferring of information – e-mail, post, telephone, MS Teams and removable media such as laptops and memory sticks, etc.
- Sharing of information for clinical, operational or legal reasons
- The storage and retention of information
- The destruction of information

The CCG recognises the changes introduced to information management as a result of the Health and Social Care Act 2012 and the Health and Social Care (Safety and Quality) Act 2015 and will work with national bodies and partners to ensure the continuing safe use of information to support services and clinical care.

Failure to adhere to this policy may result in disciplinary action and/or referral to the appropriate regulatory bodies including the police and professional bodies.

3 Roles and Accountability

3.1 The Governing Body

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

3.2 Audit Committee

The Information Governance agenda will be led by the SIRO supported by the information governance team and will report through the Information Governance / Business Intelligence/Information Technology (IG/BI/IT) Committee to the Audit Committee.

The Data Protection Officer provides the Audit Committee with an independent view of the organisations compliance with the GDPR.

The Information Governance work programme, and new or significantly amended strategies and policies are escalated to the IG/BI/IT Committee for their consideration and onward approval by the Audit Committee.

3.3 Information Governance Committee

The IG/BI/IT Committee meets on a bi-monthly basis and consists of the SIRO, Caldicott Guardian, Information Governance Managers, Data Protection Officer, Records Manager, and appropriate representation. The IG/BI/IT Committee will:

- report to the Audit Committee
- support the SIRO and Caldicott Guardian in their roles
- monitor information governance performance annually using the Data Security and Protection Toolkit.
- be responsible for overseeing operational information governance issues
- develop and maintain policies, standards, procedures and guidance
- co-ordinate and monitor the implementation of the information governance policy and management framework across the CCG
- provide direction in formulating, establishing and promoting IG policies
- ensure that the approach to information handling is communicated to all staff and made available to the public

- ensure that appropriate training is made available to staff and completed as necessary to support their duties
- monitor information handling activities to ensure compliance with the law and guidance

3.4 Senior Information Risk Owner (SIRO)

The SIRO is responsible for ensuring that organisational information risks are properly identified, managed and that appropriate assurance mechanisms exist. The SIRO will:

- 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 CCG's information governance risk assessment and management processes within the organisation
- providing a focal point for the resolution and/or discussion of IG issues
- own the CCG's Information Security Policy
- undertake training as necessary to ensure they remain effective in their role as SIRO

3.5 Caldicott Guardian

The Caldicott Guardian oversees the arrangements for the use and sharing of patient information and will:

- act as the 'conscience' of the CCG
- represent and champion Information Governance requirements and issues at a senior management level
- facilitate and enable information sharing and advise on options for lawful and ethical processing of information
- ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff
- oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS
- undertake training as necessary to ensure they remain effective in this role

3.6 Data Protection Officer

Article 38 of the GDPR provides that the controller and the processor shall ensure that the DPO is 'involved, properly and in a timely manner, in all issues which relate to the protection of personal data'. Article 39(1)(b) entrusts DPOs with the duty to monitor compliance with the GDPR. Recital 97 further specifies that DPO 'should assist the controller or the processor to monitor internal compliance with this Regulation'.

As part of these duties to monitor compliance, DPOs may, in particular:

- Collect information to identify processing activities
- Analyse and check the compliance of processing activities
- Inform, advise and issue recommendations to the controller or
- processor

3.7 Cyber Assurance and Compliance Manager

Responsibilities of the Cyber Assurance and Compliance Manager include:

- Acting as a central point of contact on IT security within the organisation and for external organisations that has entered into an agreement for the provision of IT services by the CCG.
- Implementing an effective framework for the management of security.
- Assisting in the formulation of Information Security Policy and related policies.
- Advise on the content and implementation of the Information Security Programme.
- Co-ordinate IT security activities particularly those related to shared information systems or IT infrastructures.
- Liaise with external organisations on IT security matters, including representing the organisation on cross-community committees.
- Advising users of information systems, applications and Networks of their responsibilities.
- Creating, maintaining, giving guidance on and overseeing the implementation of IT Security.
- Ensuring that risks to IT systems are reduced to an acceptable level by applying security countermeasures identified following an assessment of the risk.
- Ensure breaches of policy and recommended actions are reported in line with organisation's procedures.

3.8 Information Asset Owners and Administrators

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

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

3.9 Head of Corporate Governance and Risk

The Head of Corporate Governance and Risk will:

- Maintain and publish the organisations Publications Scheme

3.10 Managers

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

3.11 Employees

Information Governance compliance is an obligation for all staff. Staff should note that there is confidentiality clause in their contract and that they are required to participate in induction training, annual refresher training and awareness raising sessions carried out to inform/update staff on information governance issues. Any breach of confidentiality, inappropriate use of health, business or staff records or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract.

All employees are personally responsible for compliance with the law in relation to the General Data Protection Regulation (EU) 2016/679, Data Protection Act 2018 and the Common Law Duty of Confidentiality.

3.12 Third Party Contractors

Contracts with third parties providing services to the CCG must include appropriate, detailed and explicit requirements regarding confidentiality and information governance to ensure that contractors are aware of their IG obligations. Further guidance is available from the CCG's Provider Contract and Commissioning Information Governance Assurance document.

3.13 Clinical Services

All clinical services commissioned by or on behalf of the CCG will be required to:

- Have a suitable contract in place that defines the Data Controller / Processor relationship regarding the information required to effectively monitor commissioned services
- Provide sufficient guarantees that they are meeting the requirements of the General Data Protection Regulation and Data Protection Act when providing services including, but not limited to, Privacy notice ,completion of the annual Data Security and Protection Toolkit as required and undertake an independent audit if requested, to be disclosed to the CCG in order to provide further assurance they have met expected requirements
- Ensure privacy notices make individuals aware of the CCG's role in Commissioning and the personal and special category data it may receive to undertake the role.
- Ensure that where any IG incidents occur that they are reported to the CCG via routes determined within the contract and in accordance with data protection legislation
- Set out expectations regarding providing information in relation to requests for information made under the Freedom of Information Act

- Ensure inclusions regarding exit plans are addressed following transfer of services or decommission of service e.g. passing on data/deletion/ retention of data at end of the contract

3.14 Support services

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

- Ensure a suitable contract/SLA and or as a minimum a confidentiality agreement is in place to form a Data Controller to Data Processor relationship where Personal or Special Categories of Personal Data is managed on behalf of the CCG
- Provide sufficient guarantees that they are meeting the requirements of the General Data Protection Regulation and Data Protection Act when providing services including, but not limited to, Privacy notice ,completion of the annual Data Security and Protection Toolkit as required and undertake an independent audit if requested, to be disclosed to the CCG in order to provide further assurance they have met expected requirements.
- Ensure that any new processing is within the remit of the contract or seek written confirmation if there is any ambiguity
- Report any known incidents or risks in relation to the use or management of information owned by the CCG and in accordance with Data Protection legislation
- Set out expectations regarding providing information in relation to requests for information made under the Freedom of Information Act
- Ensure inclusions regarding Exit Plans are addressed following transfer of services or decommission of service e.g. passing on data/deletion/retention of data at end of the contract

4 Governance Arrangements

The following governance arrangements have been agreed:

- 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.

5 Key Principles and Procedures

5.1 Legal compliance

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

- The CCG regards all identifiable personal information relating to patients and staff as confidential except where national policy on accountability and openness requires otherwise as set out in the principles of the Human Rights Act and in the public interest

- Data Protection Impact Assessments will be completed where defined in the respective procedure.
- Information about the organisation will be available to the public in line with the Freedom of Information Act, Environmental Information Regulations and Protection of Freedoms Act unless an exemption applies. The CCG will establish and maintain a Publication Scheme in line with legislation and guidance from the Information Commissioner.
- There will be clear procedures and arrangements for handling queries from patients, staff, other agencies and the public concerning personal and organisational information.
- The CCG will undertake or commission annual assessments and audits of its compliance with legal requirements as part of the annual review and submission of the DSPT and in line with changes and developments in legislation and guidance.
- Integrity of information will be developed, monitored and maintained to ensure that it is appropriate for the purposes intended.
- The CCG will establish and maintain policies to ensure compliance with the Data Protection legislation, Freedom of Information Act, Human Rights Act and the common law of confidentiality and associated guidance.
- The CCG will undertake annual assessments and audits (through the DSPT) of its policies, procedures and arrangements for openness.
- Patients will have ready access to information relating to their own health care under the General Data Protection Regulation and Data Protection Act 2018.
- The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media
- The CCG will work with partner NHS bodies and other agencies to establish Information Sharing Protocols to inform the controlled and appropriate sharing of patient information with other agencies.
- Information Governance training is mandatory for all staff. This will include awareness and understanding of Caldicott principles and confidentiality, information security and data protection. Information Governance will be included in induction training for all new staff with completion of refresher training on an annual basis thereafter. The necessity and frequency of any further training will be Personal Development Review (PDR) based.
- The CCG will work in collaboration with the Local Counter Fraud Specialists and other related agencies to support their work in detecting and investigating fraudulent activity across the NHS.

5.2 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 as part of the annual review and

submission of the DSPT and in line with changes and developments in legislation and guidance.

- The CCG will promote effective confidentiality and information 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.
- The CCG will appoint a Senior Information Risk Owner and assign responsibility to Information Asset Owners to manage information risk.
- The CCG will use pseudonymisation and anonymisation of personal data where appropriate to further restrict access to confidential information.
- All new projects, processes and systems (including software and hardware) which are introduced must meet confidentiality and data protection requirements. To enable the organisation to address the privacy concerns a Data Protection Impact Assessment will be carried out.

5.3 Clinical Information Assurance, Quality Assurance and Records Management

- The CCG will establish and maintain policies and procedures for information quality assurance and the effective management of records
- The CCG will undertake or commission annual assessments and audits of its information quality and records management arrangements
- Managers are expected to take ownership of, and seek to improve of, the quality of information within their services
- Wherever possible, information quality should be assured at the point of collection
- The CCG will promote data quality through policies, procedures, user manual and training.
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The CCG will establish a Records Management and Information Lifecycle Policy covering all aspects of records management and consistent with the Records Management Code of Practice for Health and Social Care 2016.

6 Training

The CCG includes Information Governance as part of its mandatory annual training for all staff.

- All staff are required to complete the Data Security Awareness Level 1 training module via Electronic Staff Record portal, attend face to face workshops or virtual training sessions via MS Teams.
- New staff must review the IG Handbook and sign the Information Governance Declaration before being provided with any access to CCG information assets.

- The CCG has identified other recommended training for staff members whose role has information governance responsibilities and requires further role specific training. Ad hoc training may be completed where an incident investigation requires this. Specific training needs are detailed within the IG Training Strategy.

7 Incident Management

Information Governance and IT related incidents, including cyber security incidents, must be reported and managed through the CCG's Incident Management Policy and Serious Incident Policy. All incidents will be reviewed by the IG team and where necessary escalated to the DPO, SIRO and or the Caldicott Guardian

8 Monitoring Compliance and Effectiveness

An assessment of compliance with the requirements in the DSPT will be undertaken each year. Annual assessments and proposed action/development plans will be presented to the CCG's Senior Information Risk Owner. The requirements are grouped into the following initiatives:

1. Personal Confidential Data
2. Staff Responsibilities
3. Training
4. Managing Data Access
5. Process Reviews
6. Responding to Incidents
7. Continuity Planning
8. Unsupported Systems
9. IT Protection
10. Accountable Suppliers

9 Associated Documentation

The CCG will maintain the following key policies and procedures to support effective Information Governance:

- Individual Rights including Subject Access Request (Access to Health Records) Policy
- Confidentiality and Data Protection Policy
- Freedom of Information Act and Environmental Regulations Policy
- Information Governance Policy and Management Framework
- Information Security Policy
- Records Management and Information Lifecycle Policy
- Acceptable Use Policy

Supplementary to the key policies listed above, the CCG will also maintain the following policies and guidelines:

- Confidentiality Code of Conduct
- Email Policy
- Internet and Social Media Policy
- Data Protection Impact Assessment Procedure

- Network Security Policy

10 Implementation and Dissemination

All the Information Governance policies and procedures will be made available in electronic format and will be located on the CCG website. Any updates/new policies/procedures are approved by the Audit Committee following consideration at the IG/BI/IT Committee and are communicated to staff via the staff E-bulletin and staff briefings.

Every new member of staff will be directed to the policy pages on the internet as part of the induction process.

11 Review

This policy will be reviewed every year or in line with changes to relevant legislation or national guidance.

APPENDIX 1: DOCUMENTED ACTION PLAN FOR RAISING STAFF AWARENESS

The Data Security and Protection Toolkit requires organisations providing health and social care services to have a documented action to promote staff awareness of information governance standards, inform staff of their responsibilities and the consequences of misconduct and advise staff their compliance with IG requirements will be checked and monitored

There are 10 standards that need to be met within the DSPT.

The DSPT assertions below identify the requirements that are required to meet some of the assertions and will be incorporated into the CCG's Information Governance work programme.

Key messages to be communicated to staff and made available throughout the organisations	**Examples of suitable evidence**	**Delivery Method**
IG Policies have been communicated to appropriate staff and made available throughout the organisation	Selection of Policies – Information Governance Policy; Confidentiality and Data Protection Policy; Information Security Policy; Records Management Policy; Freedom of Information Policy	All policies available on the Internet/extranet
Information Governance Awareness and Mandatory Training for all staff. Additional training for staff in key roles	Training Needs Analysis to cover mandatory IG Training/additional training for key staff groups/Induction Programme for New Starters/Training materials/documented training programme/Training Records/Test of Comprehension/Reports evidencing numbers of staff trained	E-Learning Tool/ Face to Face / MS Teams

Key messages to be communicated to staff and made available throughout the organisations	Examples of suitable evidence	Delivery Method
All staff members with the potential to access confidentiality personal information have been informed that monitoring and auditing of access is being carried out, of the need for compliance with confidentiality and security procedures and the sanctions for failure to comply.	Confidentiality clause in staff contract; Information Governance policies; Data Security Awareness training; acceptable use banner	Internet/team meetings, staff briefing materials, IG compliance spot checks undertaken, CCG Website
All staff members that are likely to introduce new information processes or information assets are effectively informed about the requirement to obtain approval from the SIRO / Data Protection Officer / IG team at the proposal stage of the new process or information asset.	Data Protection Impact Assessment procedure	CCG Website/team meetings, staff briefing materials
Employees are informed of the nature and source of any information stored about them, how it will be used, who it will be disclosed to; and their data protection rights regarding access and sharing of the personal information	The CCG's Website to provide information on how personal information about patients or other service users is stored, used and shared and informs individuals about their rights in relation to that information	Privacy notice on website Confidentiality and Data Protection policy on internet
All staff assigned responsibility for Information Security have been appropriately trained to carry out their role	Information Governance Management Framework Policy	Training attendance lists/existing qualifications
Staff members have been informed of the incident reporting procedures and in particular of their own responsibilities for reporting incidents and near-misses	Documented incident management and report procedures and training on how to report an incident on Datix	CCG Website

Key messages to be communicated to staff and made available throughout the organisations	Examples of suitable evidence	Delivery Method
The SIRO and all other staff assigned responsibility for coordinating and implementing information risk management have been appropriately trained to carry out their role	TNA/training attendance lists/training materials/existing qualifications or training evaluation records	E-learning module certificate, face to face sessions
All relevant staff are made aware of business continuity plans and any implications for their role - all staff are aware of their roles and responsibilities	Business Continuity Plan in place to respond to threats to data security	Business Continuity policy on Internet/team meeting notes, staff briefing materials