

Information Governance Strategy

Version:	1.1
Ratified by:	Quality and Performance Committee
Date ratified:	1th January 2018
Name & Title of originator/author:	John Robinson, Senior Information Governance Specialist (eMBED Health Consortium)
Name of responsible committee/individual:	Information Governance Committee
Date issued:	22nd January 2018
Review date:	January 2019
Target audience:	All staff

Equality Statement

This policy applies to all employees, Governing Body members and members of the Leeds Clinical Commissioning Groups 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.....	4
2	The Scope of the Strategy	4
3	Aims and objectives	5
4	Purpose.....	5
5	Information Governance Toolkit	5
6	Roles and Responsibilities	5
6.1	Caldicott Guardian (Medical Director)	5
6.2	Senior Information Risk Owner (Director of Finance).....	5
6.3	Information Governance and Freedom of Information support to the SIRO and Caldicott Guardian	6
6.4	Head of Corporate Governance	7
6.5	Governance performance and Risk Committee	7
6.6	Information Governance Committee	7
6.7	Information Asset Owners	7
7	Strategic Objectives 2017/18	7
7.1	All staff must understand and apply best practice and the principles of information governance to manage all information to support the business activities of the CCG	7
7.2	The CCG will undertake regular reviews and audits of how information is used through	8
7.3	The CCG will ensure that clear advice and guidance is made available through CCG website, to patients, families and carers about how their personal information is used	8
7.4	The CCG will achieve the specified performance level of compliance for all key IG requirements and demonstrate year on year improvement	8
8	Legal Compliance	9
9	Information Security	9
10	Information Risk	10
11	Confidentiality	10
12	Information Sharing	11
13	Data Protection	11

14 Freedom of Information 11

15 Review of Information Governance (structure, resources, expertise and accountability – covering Information security, Information Risk, Records Management and Information / Data Quality) 11

Appendix 1 Information Governance Policies and Procedures 12

1 Introduction

Information Governance has the following fundamental aims:

- To support the provision of high quality care and research by promoting the effective and appropriate use of information
- To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources
- To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities to consistently high standards
- To enable organisations to understand their own performance and manage improvement in a systematic and effective way

Leeds CCGs Partnership has a statutory responsibility to patients and the public to ensure that the services it provides have effective processes, policies and people in place to deliver its objectives in relation to holding and using confidential and personal information. As a commissioner it will need to be assured that the services the organisation commissions from other organisations also comply with the Care Quality Commission in relation to information governance.

Information Governance provides a framework to bring together all the legal rules, guidance and best practice that apply to the handling of information, allowing:

- implementation of advice and guidance
- compliance with the law
- year on year improvement plans

Information Governance is about setting a high standard for the handling of information and giving organisations the tools to achieve that standard. The ultimate aim is to demonstrate that an organisation can be trusted to maintain the confidentiality and security of personal information, by helping individuals to practice good information governance and to be consistent in the way they handle personal and corporate information.

2 The Scope of the Strategy

There are two key components underpinning this strategy which are:

1. The organisation's Information Governance Policy and Management Framework
2. A development plan arising from a baseline assessment against the standards set out in the Information Governance Toolkit

The ultimate responsibility for Information Governance in the organisation lies with the organisation's Governing Body. The Information Governance Committee will have delegated authority from The Governing Body, via the Quality and Performance Committee, to discharge its functions in this respect.

The Information Governance Committee has overall responsibility for overseeing the development and implementation of this strategy, the Information Governance Policy and Management Framework.

A key function of the Information Governance Committee will be to monitor and review untoward occurrences and incidents relating to Information Governance and ensure that effective remedial and preventative action is taken.

3 Aims and objectives

The CCGs aims to achieve a standard of excellence in information governance by ensuring information is dealt with legally, securely, efficiently and effectively in the course of CCGs business.

All information processing will be undertaken in accordance with relevant legislation and best practice. The CCGs will set policies and procedures to ensure that appropriate standards are defined, implemented and maintained.

4 Purpose

The purpose of this strategy is to describe the management arrangements that will deliver Information Governance assurance within the Leeds CCGs.

5 Information Governance Toolkit

The Information Governance Toolkit (IGT) is an online tool that enables organisations to measure their performance against the information governance requirements and compliance with the toolkit provides assurance that organisations have established good practice around the handling of information, are actively promoting a culture of awareness and improvement to comply with legislation and other mandatory standards.

Completion of the Information Governance Toolkit (IGT) is mandatory for all organisations providing NHS services (handling patient identifiable information) and/or using NHS Mail and the N3 network. All organisations are required to score on all requirements at least level 2 and be at a satisfactory level. Development plans will be developed year on year from the IGT to achieve a satisfactory level in all requirements and to explore scope for improvements. As the IGT is a publically available assessment the scores of partner organisations will be used to assess their suitability to share information and to conduct business with and/or commission services from.

6 Roles and Responsibilities

6.1 Caldicott Guardian

The Caldicott Guardian will be responsible for:

- The protection and confidentiality of patient-identifiable information, both within the organisation and when sharing it with other organisations
- Agreeing levels of access to the organisations patient information systems

6.2 Senior Information Risk Owner (Chief Finance Officer)

The Senior Information Risk Owner (SIRO) has organisational responsibility for all aspects of risks associated with information governance, including those relating to confidentiality

and data protection. These duties include:

- Take ownership of the organisations Information Security Policy and risk assessment process
- Act as advocate for information risk for the Governing Body and provide written advice to the accountable officer (if this is not the SIRO) on the content of the Annual Governance Statement in regard to information risk
- Understand how the strategic business goals of the organisation may be impacted by information risks
- Oversee the development of an Information Security Policy, and a strategy for implementing the policy within the existing Information Governance Framework.
- Take ownership of risk assessment processes for information risk, including the review of the annual information risk assessment to support and inform the Annual Governance Statement
- Ensure that identified information security threats are followed up and incidents managed
- Review and agree action in respect of identified information risks
- Ensure that the organisation's approach to information risk is effective in terms of resources, commitment and execution and that this is communicated to all staff
- Provide a focal point for the resolution and/or discussion of information risk issues
- Ensure The Governing Body is adequately briefed on information risk issues
- Be required to undertake and pass strategic information risk management training at least annually
- Ensuring that sufficient resources are provided to support Information Governance
- Defining the organisations policy in respect of Information Governance and records management, taking into account legal and NHS requirements

6.3 Information Governance and Freedom of Information support to the SIRO and Caldicott Guardian

The CCG has commissioned eMBED to provide an advisory and supportive Information Governance and a Freedom of Information service.

The Freedom of Information service specification includes:

- Provision of management, advice and responses to Freedom of Information (FOI) and Environmental Information Requests (EIR) to the Clinical Commissioning Group (CCG) so that the client is compliant with relevant national legislation, codes of practice and guidance from the Information Commissioner

The Information Governance service specification includes:

- An IT security service which provides advice and assurance for all areas of IT and Cyber Security.
- IG Consultancy and Support:
- Provision of advice and support on IG related issues, which includes existing operational processes and new business initiatives.
- Provision of advice and guidance around IG legislation
- IG policy support for the production and maintenance of local CCG IG policies and procedures

- IG Training support
- IG incident management and investigations

6.4 Head of Corporate Governance

The Head of Corporate Governance will:

- Monitor all requests for information under the Freedom of Information Act by members of the public, and support the FOI team to coordinate responses
- Maintain and publish the organisations Publications Scheme
- Manage Subject Access Requests and requests for information

6.5 Quality and Performance Committee

The Information Governance agenda will be led by the SIRO supported by staff of eMBED Health Consortium and will report through IG Committee to the Quality and Performance Committee.

The IG work programme, and new or significantly amended strategies and policies are escalated to the IG Committee for their consideration and onward approval by the Quality and Performance Committee.

6.6 Information Governance Committee

The IG Committee reports to the above Quality and Performance Committee and meets on at least a quarterly basis. Membership consists of the SIRO, Caldicott Guardians, eMBED Health Consortium Senior IG Specialist, and appropriate representation. The Terms of Reference for the IG Committee are included as an Appendix to the Information Governance Policy and Management Framework.

6.7 Information Asset Owners

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.

7 Strategic Objectives

The CCG will establish a robust information governance process conforming to the standards and the objectives in the Information Governance Policy and Management Framework. It is the responsibility of all organisations to comply with relevant legislation.

- 7.1 The CCGs will feel assured that they are making necessary plans and preparations for the General Data Protection Regulation based upon guidance from the Information

7.2 All staff must understand and apply best practice and the principles of information governance to manage all information to support the business activities of the CCG

- All staff involved in the administration of information governance must receive senior management backing, training and encouragement to be aware of developments in information governance and any relevant information handling issues that will affect them.
- Delivery of mandated information governance training for all staff.
- All staff signing confidentiality clauses within all staff contracts
- Publication of IG policies, procedures and guidance on the CCG's internet
- Agreement and sign up by staff to key IG and IT Policies
- Utilising the IG Training Strategy to develop training programmes to ensure that staff are aware of their responsibilities, including induction and contractual arrangements. This will extend to non-contract staff.

7.3 The CCG will undertake regular reviews and audits of how information is used through

- Mapping of data flows and register of information assets.
- Review of reported information incidents
- Data quality checks
- Ad-hoc IG s compliance checks with best practice

7.4 The CCG will ensure that clear advice and guidance is made available through CCG website, to patients, families and carers about how their personal information is used

Information will be made available explaining how information is recorded and shared and how any concerns may be raised, in the form of the Privacy Notice. Information will also be provided on Subject Access requests (SAR) under the Data Protection Act 1998.

7.5 The CCG will achieve the specified performance level of compliance for all key IG requirements and demonstrate year on year improvement

- The CCG's IG performance is measured through the self assessed annual IG Toolkit (Data Security Protection Toolkit from April 2018) submissions and reported to the IG Committee. Performance will also be measured and monitored through a programme of internal audit.
- The CCG's IG Toolkit performance is monitored by the IG Committee and reported to the Audit Committee. The IG Committee will receive IG exception reports and the IG Toolkit submission report.
- The IG Committee will monitor progress against action plans
- The CCG will complete the self assessment against the IG Toolkit requirements on an annual basis, in form of an IG Toolkit Development Plan.

8 Legal Compliance

The organisation is required to comply with a number of UK legislation related to information, including:

- Access to Health Records Act 1990
- Anti-Terrorism Crime and Security Act 2001
- Care Act 2014
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Criminal Justice Act 2003
- Data Protection Act 1998
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- General Data Protection Regulation (EU) 2016/679
- Health and Social Care Act (Safety and Quality) 2015
- Health and Social Care Act 2012
- Human Rights Act 1998
- NHS Act 2006
- Privacy and Electronic Communications Regulations 2003
- Regulation of Investigatory Powers Act 2000

In order to maintain compliance with the relevant legislation, the Governing Body via the Quality and Performance Committee will ensure that:

- The CCG establishes and maintains appropriate Information Governance policies, standards, and guidelines
- The CCG undertakes or commissions regular assessments and audits of its compliance with legal requirements
- Non-confidential information about the CCG and its services will be available to the public on the organisations website, and through a variety of other media
- Staff have access to their employment records
- The CCG has clear procedures and arrangements for handling queries from patients and the public.

9 Information Security

Information security is characterised as the preservation of:

- Confidentiality – ensuring that access to the information is limited to those with the appropriate authority to see it
- Integrity – ensuring that information is complete, accurate, and reliable, and that its authenticity is guaranteed
- Availability – ensuring that the information is available to authorised users when and where required
- Accountability – ensuring that audit trail processes track all viewing, creating, amending, and deleting of the information

In order to maintain required levels of information security, the organisation will:

- Establish and maintain policies for the effective and secure management of its information assets and resources, including an Information Security Policy.
- Promote effective confidentiality and security practice to its staff through policies, procedures and training
- Monitor and investigate all reported instances of actual or potential breaches of confidentiality and information security
- Undertake or commission regular assessments and audits of its information security arrangements.

Cyber and Data Security

In recognition of the rising risk of cyber attacks across all sectors, Department of Health has commissioned NHS Digital to develop the Care Computer Emergency Response Team ([CARECert](#)). CARECert will provide advice and guidance to support health and social care organisations to respond effectively and safely to cyber security threats.

In July 2017 the Department of Health report, [Your Data: Better Security, Better Choice, Better Care](#) was published as the Government response to the National Data Guardian for Health and Care's Review of Data Security, Consent and Opt – Outs and the Care Quality Commission.

The report outlines the National Data Guardian's 10 Security Standards set in 3 leadership obligations.

10 Information Risk

The organisation has put a supporting structure in place to support the information risk agenda as follows:

- The Senior Information Risk Owner (SIRO), supported by the Information Governance Committee,
- Information Asset owners (IAOs) have been designated as senior Heads of Department of the organisation, and have been tasked with nominating their Information Asset Assistants (IAA)
- All IAO's and IAA's will have undertaken the e-learning modules relating to Information Risk.
- The organisation has an Information Security Policy.
- Items that are discussed at the monthly Information Governance Committee are assessed as to whether or not they need to be flagged up to the organisation's risk register
- Risk management is a standing item on the Information Governance Committee's agenda.

11 Confidentiality

The organisation will maintain a duty of confidence to its patients and staff, treating all person-identifiable information as confidential. Patients will be made aware of whom their information may be shared with, and under what circumstances, in order to provide them with high quality care. They will be informed of their rights to object to the disclosure of

their information.

12 Information Sharing

The organisation has signed up to the [Inter-Agency Information Sharing Protocol](#), and will comply with it when sharing confidential information with any other organization.

13 Data Protection

The organisation will ensure compliance with the General Data Protection Regulation (EU) 2016/679 and Data Protection Act by:

- Until April 18 annual notification to the Information Commissioner of the organisations' data processing activities
- Complying with the data protection principles – See appendix 1
- The Senior Information Risk Owner will be responsible for the day-to-day management of the CCG's obligations.

14 Freedom of Information

The organisation will ensure compliance with the Freedom of Information Act 2000 by:

- Maintaining a publication scheme on the CCG's website, containing a range of business information about the organisation
- Managing all requests for information and coordinating the responses in accordance with the requirements of the Freedom of Information Act.

15 Review of Information Governance (structure, resources, expertise and accountability – covering Information security, Information Risk, Records Management and Information / Data Quality)

The Governing Body, via the Quality and Performance Committee, is required to annually review the Information Governance management and accountability arrangements to ensure adequacy. This involves identifying any gaps or weaknesses and approving measures to strengthen them. The Quality and Performance Committee is also required to review access to expertise across the Confidentiality and Data Protection agenda, Information Security agenda, and Information Quality and Records Management agenda.

The implementation of the IG Strategy, Policy and Management Framework and IG Toolkit Development Plan will ensure that information is more effectively managed within the organisation.

The IG Committee will formally review this strategy every year to include any significant changes to mandatory requirements, national guidance or as a result of significant information governance breaches or incidents in order to ensure that all types of information are more effectively managed within the CCG.

Appendix 1 Information Governance Policies and Procedures

The strategy should be read in-conjunction with the following documents:

- Information Governance Policy and Management Framework
- Confidentiality and Data Protection Policy
- Records Management and Information Lifecycle Policy
- Freedom of Information Act and Environmental Information Regulations Policy
- Information Security Policy
- Network Security Policy
- Internet and Social Media Policy
- Email Policy
- Subject Access Request (Access to Health Records) Procedure
- Privacy Impact Assessment Procedure
- Safe Transfer Guidelines and Procedure
- Incident Management Policy
- Serious Incident Policy

Appendix 1

Data Protection Principles

Schedule 1 to the Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
 - (a) at least one of the conditions in Schedule 2 is met, and
 - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.