CCGs working together

Airedale, Wharfedale and Craven CCG
Bradford City CCG
Bradford Districts CCG

Information Governance Strategy and Strategic Vision

Policy approved by: Audit and Governance Committees

Date: 9th October 2017

Next Review Date: October 2018

Version: 3.0

Review and Amendment Log / Control Sheet

Responsible Officer:	Associate director of corporate affairs
Clinical Lead:	
Author:	Senior IG specialist, eMBED
Date Approved:	9th October 2017
Committee:	Audit and Governance Committees
Version:	3.0
Review Date:	October 2018

Version History

Version no.	Date	Author	Description	Circulation
1.0	29 August 2014	IG specialist, YHCS	Initial Draft	
1.1	07October 2014	IG specialist, YHCS	Approved	
2.0	14 October 2016	Senior IG specialist, eMBED	Approved	
2.1	17 August 2017	Senior IG specialist, eMBED	Review and update	Head of Governance (initial drafts), A&G Comms (final)
3.0	October 2017	Senior IG specialist, eMBED	Approved by Audit and Governance Committees 9th October 2017	

Contents **Page Number**

1. Introduction

The CCGs have a statutory responsibility to patients and the public to ensure that the services they provide have effective processes, policies and people in place to deliver their objectives in relation to holding and using confidential and personal information. As commissioners they will need to be assured that the services the organisation commissions from other organisations also have effective processes in place 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 central 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. Scope

There are two key components underpinning this strategy which are:

1. The organisations' information governance policy and management framework; and
2. An annual action 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 organisations governing bodies. The audit and governance committee will have delegated authority from the Governing Bodies, to discharge its functions in this respect. The audit and governance committee will be accountable to the organisations governing Bodies.

The audit and governance committee has overall responsibility for overseeing the development and implementation of this strategy, the information governance policy and management framework, and the information governance toolkit action plan.

A key function of the audit and 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 aim to achieve a standard of excellence in information governance by ensuring information is dealt with legally, securely, efficiently and effectively in the course of CCG 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. Information Governance Toolkit

The information governance toolkit (IGT) is an online tool that enables organisations to measure their performance against information governance requirements. 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 connected to N3, using NHS Mail and providing NHS services. All organisations are required to score on all requirements at level 2 or 3 to be at a satisfactory level. Annual plans will be developed year on year from the IGT to achieve a satisfactory level in all requirements. 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.

5. Roles and Responsibilities

5.1 Chief Officer

The chief officer will be responsible for:

- Defining the organisations policy in respect of information governance and records management, taking into account legal and NHS requirements
- Ensuring that sufficient resources are provided to support information governance

5.2 Caldicott Guardian: Director of Quality

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

5.3 Senior Information Risk Owner: Deputy Chief Officer and Chief Finance Officer

The senior information risk owner (SIRO) will:

- Take ownership of the organisations information risk policy and risk assessment process
- Act as advocate for information risk on the board 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 risk 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 organisations' 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 Board is adequately briefed on information risk issues
- Be required to undertake and pass strategic information risk management training at least annually

5.4 Associate Director of Corporate Affairs

The associate director of corporate affairs, supported by the head of governance, will:

- Work with eMBED Health Consortium IT department to ensure information security
- Act as information security lead for the NPfIT Care Records Service
- Ensure compliance with all relevant legislation, national guidelines and standards
- Write and promote all Information Governance policies and standard
- Liaise with information governance officers and caldicott guardians from local Trusts, organisations, and the police on information governance matters
- Oversee the management of all the organisations' records
- Be responsible for records storage, archiving, and security
- Ensure health records standards comply with national guidelines
- Support the work of the caldicott guardian and advise on patient confidentiality issues
- Be responsible for notifying the information commissioner annually of the organisations' data processing activities
- Advise on all matters related to the Data Protection Act, the General Data Protection Regulation (hereafter known as GDPR) which will in force as of the 25th May 2018 and related legislation (e.g. subject access requests)
- Report progress against national standards to the audit and governance committee
- Ensure that the organisation has robust mechanisms for responding and managing freedom of information requests
- Take responsibility for maintaining record systems whilst complying with the Data Protection Act, GDPR and organisational policies of confidentiality
- Provide support to all projects that require registration to national systems ensuring that project timescales are met
- Provide support for other information governance areas
- Manage all requests for information under the Freedom of Information Act by members of the public, and coordinates the responses
- Provide support to internal meetings in relation to IT, in terms of security and confidentiality
- Maintain and publish the organisations publications scheme
- Manage subject access requests and requests for information
- Take responsibility for maintaining record systems whilst complying with the data protection act, GDPR and organisational policies of confidentiality
- Provide support to all projects that require registration to national systems ensuring that project timescales are met
- Provide support for other information governance areas
- Provide support to internal meetings in relation to IT, in terms of security and confidentiality

5.5 Audit and Governance committees

The organisations have estabished audit and governance committees, which report to the respective governing body and will be responsible for:

- Approving information governance and records management policies, procedures and guidance

- Approving the Information Governance Annual Work Programme and monitoring its implementation.
- Reviewing performance monitoring results

5.6 Data Protection Officer (DPO)

Article 37(5) of the GDPR allows the role of DPO to be assigned to either a member of staff or to an external contractor, designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill the tasks referred to in Article 39. These are:

- to inform and advise the origianisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- To monitor compliance with the GDPR and other data protection laws, including assigning responsibilities, managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- To cooperate with the supervisory authority (the ICO in the UK);
- To act as the contact point for the supervisory authority and for individuals whose data is processed (employees, patients etc) .

Under GDPR, the role of DPO is protected and the organisation must ensure that:

- The DPO reports to the highest management level of the organisation – ie Governing Body level.
- The DPO operates independently and is not dismissed or penalised for performing their task.
- Adequate resources are provided to enable DPOs to meet their GDPR obligations.

6. Strategic Objectives 2017/18

The CCGs will establish a robust information governance process conforming to the IG toolkit standards and the objectives in the organisations information governance policy and management framework. An outline of the high level IG organisational objectives that the CCGs seek to achieve is as follows:

- Establishing, implementing and maintaining policies for the effective management of information
- Ensuring there is provision of sufficient training, instruction, supervision and information to enable all employees to operate within information governance requirements.
- Delivery of mandated information governance induction and update training for all staff.
- All staff signing confidentiality clauses within all staff contracts
- Agreement and sign up by staff to key IG and IT policies
- Minimise the risks arising from information handling processes and the subsequent damage or stress to an individual through the mapping of data flows, review of reported information incidents, data quality checks and ad-hoc IG spot checks on compliance with best practice
- Minimising the risk of personal data breaches
- Minimising inappropriate uses of personal data
- Ensure that clear advice and guidance is made available through the CCGs' websites, to patients, families and carers about how their personal information is used
- Ensure information is made available explaining how information is recorded and shared and how any concerns may be raised

- Ensure information is provided on subject access requests (SAR) under the Data Protection Act and GDPR
- Ensuring that contracts, service level agreements and information sharing agreements between the CCG and other organisations are managed and developed in accordance with information governance principles
- Prepare for the forthcoming GDPR which will bring significant changes to how data can be used, non-compliance brings the risk of potential high level fines and/or prosecution

7. Legal Compliance

The organisations are required to comply with a number of UK legislations related to information, including:

- Access to Health Records Act 1990
- Anti-Terrorism Crime and Security Act 2001
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Criminal Justice Act 2003
- Data Protection Act
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000
- Health and Social Care Act 2012
- Care Act 2014
- Health and Social Care Act (Safety and Quality) 2015
- General Data Protection Regulation (from 25th May 2018)

In order to maintain compliance with the relevant legislation, the governing bodies, via the audit and governance committee will ensure that:

- The CCGs establish and maintain appropriate information governance policies, standards, and guidelines
- The CCGs undertake or commission regular assessments and audits of its compliance with legal requirements
- Non-confidential information about the CCGs 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 CCGs have clear procedures and arrangements for handling queries from patients and the public

8. 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 organisations will:

- Establish and maintain policies for the effective and secure management of its information assets and resources
- 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 and IT security arrangements.

9. Information Risk

The organisations have put a supporting structure in place to support the information risk agenda.

- The deputy chief officer and chief finance officer is the designated senior information risk owner (SIRO)
- The associate director of corporate affairs is the information risk lead
- Information asset owners (IAOs) have been have been tasked with nominating their information asset administrators (IAA)

All IAO's and IAA's will have undertaken the e-learning modules relating to information governance that includes risk.

Items that are discussed at the audit and governance committees 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 joint audit and governance committee's agenda.

10. Data Protection

The CCGs will ensure compliance with the Data Protection Act and the GDPR by:

- Annual notification to the information commissioner of the organisations' data processing activities (after 25th May 2018 this will no longer apply).
- Complying with the Data Protection Act principles and GDPR legislation.
- The associate director of corporate affairs will be responsible for the day-to-day management of the CCGs obligations under the Data Protection Act and GDPR.

11. Monitoring

The CCGs IG performance is measured through:

- The CCGs IG Toolkit performance is monitored by the eMBED IG team and reported to the audit and governance committee.
- The eMBED IG team will monitor progress against action plans
- The CCGs will complete the self assessment toolkit on an annual basis
- An internal audit of the IG toolkit assessment will take place in quarter 4 as part of the CCGs internal audit programme

12. Review

The implementation of the IG strategy, framework and toolkit action plan will ensure that information is more effectively managed within the organisation.

The eMBED IG team will formally review this strategy annually 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 CCGs.

Appendix 1

Information Governance Policies and Procedures

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

- Information Governance Strategy
- Information Governance Policy and Management Framework
- Records Management and Information Lifecycle Policy
- Freedom of Information Act and Environmental Information Regulations Policy
- Information Security Policy
- Network Security Policy
- Integrated Risk Management FrameworkIncident Reporting Policy
- Business Continuity Policy
- Disciplinary Policy
- Anti-Fraud, Bribery and Corruption Policy Raising Concerns Policy
- Internet and Social Media Policy

And their associated procedures (including but not limited to):

- Access to Records Procedure
- Information Sharing Protocol
- Freedom of Information Procedures
- Internet and Social Media Policies
- Privacy Impact processes
- Remote access and home working procedures
- Safe Transfer Guidelines and Procedure
- Incident Management, Investigation and Reporting