Information Governance Framework and Strategy

2017

Important: This document can only be considered valid when viewed on the CCG's website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

Name of Policy:	Information Governance Framework and Strategy
Date Issued:	March 2017
Date to be reviewed:	Annually in line with IG Toolkit Requirements

Policy Title:	Information Governance Framework and Strategy	
Supersedes: (Please List)	Information Governance Framework and Strategy v1.1 Information Governance Framework and Strategy v1.2	
Description of Amendment(s):	Annual review as required by IG Toolkit TOR of Information Governance Group Updated Addition of Sustainability & Bribery Act Sections Organisational IG Structure defined Incident Reporting section updated and flow chart added Reformatting under headings and numbered sections	
This policy will impact on:	All Staff	
Financial Implications:	No change	
Policy Area:	Data Protection	
Version No:	1.4	
Issued By:	eMBED IG Team	
Author:	eMBED IG Team	
Document Reference:	N/A	
Effective Date:	March 2016	
Review Date:	February 2018	
Impact Assessment Date:	Complete	
APPROVAL RECORD	Integrated Audit & Governance Committee	07 March 2017
Consultation:	Relevant Internal Staff	March 2017

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Website
1.0	Barry Jackson	First draft for comments	NR	N/A
1.1	Barry Jackson	Approved version	N/A	N/A
1.2	Helen Sanderson	Amendments to reflect HSCIC Guidance and Caldicott 2	N/A	N/A
1.3	Kathleen Allen	IGG TOR Updated Policy formatting updated Addition of Sustainability Section Addition of Bribery Act Organisational IG Structure detailed More Guidance on Incident Reporting including flow chart	N/A	09 March 2017

CONTENTS

1. Introduction and Purpose

The purpose of this framework is to describe the management arrangements that will deliver Information Governance (IG) assurance within Hull Clinical Commissioning Group (afterwards referred to as HULLCCG). Information Governance is a framework that enables the organisation to establish good practice around the handling of information, promote a culture of awareness and improvement and comply with legislation and other mandatory standards.

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. Impact Analyses

2.1 Equality

This Policy forms part of the CCG's commitment to create a positive culture of respect for all staff and service users. The intention is to identify, remove or minimise discriminatory practice in relation to the protected characteristics (race, disability, gender, sexual orientation, age, religious or other belief, marriage and civil partnership, gender reassignment and pregnancy and maternity), as well as to promote positive practice and value the diversity of all individuals and communities.

As part of its development this Policy and its impact on equality has been analysed and no detriment identified.

2.2 Sustainability

A sustainability Impact Assessment has been completed and details are available alongside this Framework on the CCG's website. No impact on sustainability has been identified.

2.3 Bribery Act 2010

Under the Bribery Act 2010, it is a criminal offence to:

- Bribe another person by offering, promising or giving a financial or other advantage to induce them to perform improperly a relevant function or activity, or as a reward for already having done so; and
- Be bribed by another person by requesting, agreeing to receive or accepting a financial or other advantage with the intention that a relevant function or activity would then be performed improperly, or as a reward for having already done so.

These offences can be committed directly or by and through a third person and, in many cases, it does not matter whether the person knows or believes that the performance of the function or activity is improper. It is therefore, extremely important that staff adhere to this

and other related policies and documentation (as detailed on the CCG's website) when considering whether to offer or accept gifts and hospitality and/or other incentives

3. Information Governance Strategy

The development of a fixed IG Framework will support an IG Strategy that will develop over time with the current version published at Annex A.

4. National Context

The NHS Information Governance Assurance Programme (IGAP) was established in February 2008 in response to the Cabinet Office Data Handling review. The Prime Minister commissioned the review following the high-profile data losses in 2007. IGAP developed a number of principles to support and strengthen the existing Information Governance agenda. The principles are:

- All NHS organisations should be part of the same Information Governance Assurance Framework (IGAF)
- Information Governance should be as much as possible integrated into the broader governance of an organisation, and regarded as being as important as financial and clinical governance in organisational culture
- The Framework will provide assurance to the several audiences interested in the safe custody and use of sensitive personal information in healthcare. This involves greater transparency in organisational business processes around Information Governance
- IGAF to be built on the strong foundations of the existing Information Governance agenda and is the mechanism by which:
    - IG policies and standards are set
    - Regulators can check an organisation's compliance
    - An organisation can be performance managed

5. Aim

The purpose of this local framework is to set out an overall strategy and promote a culture of good practice around the processing of information and use of information systems. That is, to ensure that information is handled to ethical and quality standards in a secure and confidential manner. The organisation requires all employees to comply with the Policies, Procedures and Guidelines which are in place to implement this framework with the aim of ensuring that HULLCCG maintains high standards of IG.

6. Information Governance Toolkit (IGT)

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 IGT is mandatory for all organisations connected to N3 the proprietary NHS computer network, for organisations 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.

7. Roles and Responsibilities

7.1 EMBED Health Consortium

HULLCCG has a contract in place with eMBED Health Consortium to deliver a range of IG Services including support to achieve compliance with the IGT at Level 2.

7.2 Caldicott Guardian

The Caldicott Guardian for HULLCCG is the Director of Quality and Clinical Governance/Executive Nurse

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. The Guardian plays a key role in ensuring that NHS, Councils with Social Services Responsibilities and partner organisations satisfy the highest practical standards for handling patient identifiable information.

Acting as the 'conscience' of an organisation, the Guardian actively supports work to enable information sharing where it is appropriate to share, and advises on options for lawful and ethical processing of information. The Caldicott Guardian also has a strategic role, which involves representing and championing Information Governance requirements and issues at Board or management team level and, where appropriate, at a range of levels within the organisation's overall governance framework.

7.3 Senior Information Risk Owner (SIRO)

The SIRO for HULLCCG is the Chief Finance Officer.

The Senior Information Risk Owner (SIRO) is an Executive Director or Senior Management Board Member who will take overall ownership of the Organisation’s Information Risk Policy, act as champion for information risk on the Board and provide written advice to the Accounting Officer on the content of the Organisation’s Annual Governance Statement in regard to information risk.

The SIRO must understand how the strategic business goals of the Organisation and how other organisations’ business goals may be impacted by information risks, and how those risks may be managed. The SIRO implements and leads the Information Governance (IG) risk assessment and management processes within the Organisation and advises the Board on the effectiveness of information risk management across the Organisation.

7.4 Information Governance Lead

The Information Governance Lead for HULLCCG is Chief Finance Officer
The IG Lead works with eMBED IG Team to ensure systems are developed and implemented. The IG Lead is responsible for the co-ordination of the implementation within the CCG. The IG lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG within the CCG. This role includes but is not limited to:-

- developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities, e.g. an overarching high level strategy document supported by corporate and/or directorate policies and procedures;
- ensuring that there is top level awareness and support for IG resourcing and implementation of improvements;
- providing direction in formulating, establishing and promoting IG policies;
- establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives;
- ensuring annual assessments and audits of IG policies and arrangements are carried out, documented and reported;
- ensuring that the approach to information handling is communicated to all staff and made available to the public;
- ensuring that appropriate training is made available to staff and completed as necessary to support their duties and for NHS organisations;
- liaising with other committees, working groups and programme boards in order to promote and integrate IG standards;
- monitoring information handling activities to ensure compliance with law and guidance; and
- providing a focal point for the resolution and/or discussion of IG issues.

7.5 Managers

Managers are responsible for ensuring that their staff, both permanent and temporary, are aware of:

- all information security policies and guidance and their responsibility to comply with them;
- their personal responsibilities for information security;
- where to access advice on matters relating to security and confidentiality; and
- the security of their physical environments where information is processed or stored.

7.6 All staff

Individual employees have a responsibility to ensure they are aware of all information security policies and guidance and comply with them. Staff must be aware of their personal responsibility for the security and confidentiality of information which they use. Staff are responsible for reporting any possible or potential issues whereby a breach of security may occur.

8. Information Security

With the increasing use of electronic data and ways of working which rely on the use of electronic information and communication systems to deliver services there is a need for professional advice and guidance on their use as well as the need to ensure that they are maintained and operated to the required standards in a safe and secure environment.

9. Data Protection Act (DPA)

The Data Protection Act is the most fundamental piece of legislation that underpins Information Governance. HULLCCG are registered with the Information Commissioners Office and will fully comply with all legal requirements of the Act. A process will be adopted to ensure that a review of all of new systems is carried out and where requirements such as the need for Privacy Impact Assessments (PIA) are highlighted these will be completed.

The Data Protection Principles are detailed at Annex B.

10. Caldicott Principles and Requirements

The original Caldicott Report on the Review of Patient-Identifiable Information 1997 and the subsequent Report of the Caldicott2 Review - Information: To share or not to share? The Information Governance Review 2013. These two reports have identified specific principles that are considered essential practice for the appropriate sharing and security of Patient Information.

Government Response to the Report of the Caldicott 2 Report acknowledges the findings of this and promotes that everyone should understand how to protect and, where appropriate, share information about the people they care for, either directly or indirectly. The Caldicott Principles are detailed at Annex C.

This is further supported by the Everyone Counts: Planning for Patients 2014/15 to 2018/19 by detailing practical applications for information sharing, these are detailed at Annex D.

11. Handling Confidential Information

When handling confidential information and especially where an individual can be identified from the information to be processed, the CCG must ensure that it has determined and documented a legal basis for processing that information.
In addition it must ensure that arrangements are in place to ensure:

- Ensuring data subjects are appropriately informed of all uses of their information
- The security of that information at all points of its lifecycle.
- Recognising and recording objections to the handling of confidential information and where circumstances under which an objection cannot be upheld.
- Ensuring that where objections are received where the proposed uses are not required by law the CCG should ensure they act in accordance with that objection.
- Implement procedures for recognising and responding to individuals requests for access to their personal information.

- Ensure appropriate information sharing arrangements are in place for the purposes of direct care.
- Ensure appropriate data processing agreements are in place to collect or obtain information for management purposes.

The HSCIC issued two guidance documents in respect of appropriate information handling and confidentiality of that information:

1. **Code of practice on confidential information**: This code of practice describes good practice for organisations handling confidential information concerning, or connected with, the provision of health services or adult social care.
2. **A guide to confidentiality in health and social care**: A for those involved in the direct care of a patient on the appropriate handling of confidential information.

12. Risk Management

The ability to apply good risk management principles to IG is fundamental and all organisations will apply them through organisational policies. eMBED IG Team will be responsible for completion of the risk assessments for any IG related issue, and have a specific remit to risk assess new technologies and recommend controls where necessary.

Risk assessment will also be included as part of the Information Asset Owners role. Any information flows from or into identified information assets will be risk assessed and the results reported to the CCG SIRO for risk mitigation, acceptance or transfer.

13. Training and Guidance

In accordance with the requirement to achieve Level 2 on the IG Toolkit all staff must complete an Induction session when they first start employment which will include Information Governance. In subsequent years all staff are required to complete further Information Governance training including any training specific to their role and responsibilities.

A new online Training Module will be available nationally early in 2017 following which staff will be advised of the mandatory and advisory IG training which they should complete.

An Information Governance Handbook and an Information Asset Owners Handbook are available for all staff to ensure that they are fully aware of their responsibilities.

Staff awareness of IG will also be assessed by questions in the Annual Staff survey in order to provide assurance that the training is effective.

14.Awareness and Advice

The eMBED IG Team will provide advice on any IG related issue. They will work with the HULLCCG IG Lead to produce newsletters and staff e-mails to provide information and updates on IG issues.

15. Incident Management

15.1 Incident Reporting

Incidents must be reported and managed through the CCG's Incident Policy. The eMBED IG Team will have an active involvement in all IG related incidents and IG related service desk calls to ensure compliance with IG principles. Significant issues will be subject to full investigation and reporting action via the IGT where appropriate. Incidents relating to personal information will be highlighted to the Caldicott Guardian whilst those of a more technical nature and/or where serious risks are involved will be reported to the SIRO. Please see Incident Reporting Flow Chart attached at Annex F

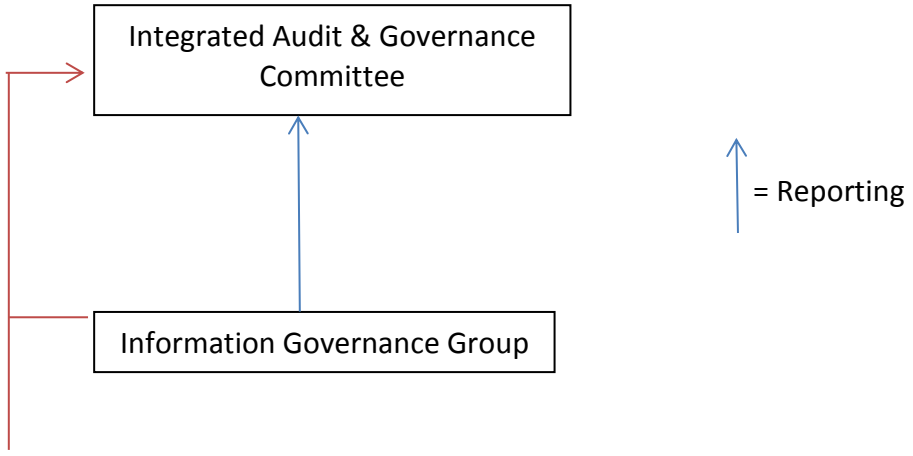
15.2 Investigation

The eMBED IG Team will support the investigation of all IG issues reported. This may include, but is not limited to, breaches of policy, breaches of confidentiality and issues related to IT Security. The eMBED IG Team will assist with the procedural processes to ensure that investigations of incidents will be carried out in a way that ensures the preservation of evidence and in a manner that enables both legal and disciplinary action to be taken if necessary.

16. Organisational Structure for IG Reporting and Assurance

The Information Governance Group has been established to support and drive the broader information governance agenda and provide the Integrated Audit and Governance Committee and the Governing Body with the assurance that effective information governance best practice mechanisms are in place within the organisation.

The Group will meet formally or informally at least every three months and be attended by the SIRO, Caldicott Guardian, Associate Director of Corporate Affairs and a representative of the eMBED provided IG service. Other staff may be invited to attend where the subject topics require their input or advice See Annex E for the Terms of Reference for this group. The Information Governance Group will report to the Integrated Audit and Governance Committee (IAGC) through minutes or action notes and will ensure the SIRO and/or Caldicott Guardian briefed on any significant issues. The Governing Body retains overall responsibility and accountability for all aspects of Information Governance.



17. Policies and Procedures

The Information Governance Framework and Strategy are supported by a range of detailed policies and procedures. These include but are not limited to:

Data Protection & Confidentiality Policy
Confidentiality: Code of Conduct Policy
Records Management policy
Safe Haven Policy
Mobile working policy
Information Security Policy
Bussiness Continuity and Strategy Policy
Confidentiality Audit Policy
Subject Access Request Policy
Acceptable Computer Use Policy
Email Policy
IAO role and responsibilities/Handbook
Information Governance Checklist and Privacy Impact Assessment

These documents are available on the CCG Internet page;

18. Reference Material.

- Data Protection Act 1998
- Human Rights Act 1998 (Specifically Article 8)
- NHS Information Governance: Guidance on Legal and Professional Obligations.
- Report on the Review of Patient-Identifiable Information 1997 (Caldicott Report)
- Report of the Caldicott2 Review - Information: To share or not to share? The Information Governance Review 2013
- Government Response to Report of the Caldicott2 Review 2013.
- NHS England: Everyone Counts: Planning for Patients 2014/15 to 2018/19.
- HSCIC: A guide to confidentiality in health and social care: Treating confidential information with respect - September 2013
- HSCIC: A guide to confidentiality in health and social care: references - September 2013
- National Information Board and DH: Personalised Health and Care 2020
- NHS England: NHS Standard Contract
- Information Commissioner: Data Sharing Code of Practice
- Information Commissioner: Privacy Impact Assessment Code of Practice

Annex A

HULL CCG INFORMATION GOVERNANCE STRATEGY 2015 to 17

1. The IG Strategy of HULLCCG will be based upon a vision of a long term delivery of clear open principles to ensure that:

   1.1. The CCG complies with all statutory requirements

   1.2. The CCG has an information governance strategy that supports the achievement of corporate objectives

   1.3. The CCG can demonstrate an effective framework for managing information governance assurance

   1.4. Staff are aware of their responsibilities and the importance of information governance

   1.5. Information governance becomes a systematic, efficient and effective part of business as usual for the organisation

   1.6. Information governance is integrated into the change control process

   1.7. That there are effective methods for seeking assurance across the organisation and with its key partners

   1.8. That the organisation can demonstrate that the information governance arrangements of organisations it commissions services from across healthcare and commissioning support are adequat

Data Protection Act 1998 - Principles

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.

Annex C

Caldicott Principles

1. Justify the purpose(s)
Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. Don't use personal confidential data unless it is absolutely necessary
Personal confidential data items should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. Use the minimum necessary personal confidential data
Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data is transferred or accessible as is necessary for a given function to be carried out.

4. Access to personal confidential data should be on a strict need-to-know basis
Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. Everyone with access to personal confidential data should be aware of their responsibilities
Action should be taken to ensure that those handling personal confidential data — both clinical and non-clinical staff — are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. Comply with the law
Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. The duty to share information can be as important as the duty to protect patient confidentiality
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Annex D

Everyone Counts: Planning for Patients 2014/15 -2018/19

This document sets out the NHS England vision with regards to the provision and outcomes of high quality care for all, now and for future generations. One of the six national conditions focuses in on 'Better data sharing between health and social care, based on the NHS number' and that local organisations should 'ensure they have the appropriate Information Governance controls in place for information sharing in line with Caldicott 2, and if not, when they plan for it to be in place.'

The requirements of the above document are as follows:

The CCG should where required

1. Confirm that they are using the NHS Number as the primary identifier for health and care services, and if they are not, when they plan to;
2. Confirm that they are pursuing open APIs (ie. systems that speak to each other); and
3. Ensure they have the appropriate Information Governance controls in place for information sharing in line with Caldicott 2, and if not, when they plan for it to be in place.

NHS England has already produced guidance that relates to both of these areas. (It is recognised that progress on this issue will require the resolution of some Information Governance issues by DH).

ANNEX E

INFORMATION GOVERNANCE GROUP TERMS OF REFERENCE

1 AIM

The Information Governance Group has been established to support and drive the broader information governance agenda and provide the Board with the assurance that effective information governance best practice mechanisms are in place within the organisation.

2 MEMBERSHIP

- CCG Chief Finance Officer (Senior Information Risk Officer) CHAIR
- CCG Director of Quality & Clinical Governance/Executive Nurse(Caldicott Guardian)
- CCG Associate Director of Corporate Affairs
- eMBED Information Governance Manager or other eMBED representative

3 ATTENDANCE

All members of this group are required to attend this meeting as a high priority. If they are unable to attend a meeting they should send apologies and, where possible, a named deputy should attend in their absence for continuity purposes. The Information Governance agenda leads provide brief progress reports on their specific areas of work and bring pieces of work to the group for discussion and approval.

4 FREQUENCY

Meetings will occur every three months with additional informal meetings as required.

5 AUTHORITY

The Group is authorised to investigate any activity within its terms of reference. It is authorised to seek any information it requires from any employee and all employees are directed to co-operate with any request made by the Group. The Group are also authorised to implement any activity which is in line with the terms of reference, as part of the IG work programme, which shall be signed off by the Integrated Audit & Governance Committee.

6 DUTIES

- To ensure that an appropriate comprehensive information governance framework and systems are in place throughout the organisation in line with national standards.
- To inform the review of the Organisation's management and accountability arrangements for Information Governance.
- To develop an IG Framework and associated strategy and/or maintain the status of the Framework.
- To develop and oversee the Information Governance & Information Security Assurance Workplans and the Information Governance Toolkit Improvement Plan
- To ensure that the organisations information assets are reviewed at least annually and that risk assessments are completed for all data flows and these are approved by the SIRO annually
- To prepare the annual Information Governance assessment for sign off by the Integrated Audit and Governance Committee.
- To ensure that the Organisation's approach to information handling is communicated to all staff and made available to the public including the publication of Fair Processing Notices
- To coordinate the activities of staff given data protection, confidentiality, security, information quality, records management and Freedom of Information responsibilities.
- To offer support, advice and guidance to the Caldicott Function and Data Protection programme within the Organisation.
- To monitor the Organisation's information handling activities to ensure compliance with law and guidance
- To ensure that training made available by the Organisation is taken up by staff as necessary to support their role.
- Provide a focal point for the resolution and/or discussion of Information Governance issues.
- To ensure that the IAGC and the Governing Body are advised about changes to legislation and guidance which will affect the organisation in the coming year

7 REPORTING

The Information Governance Group will report and be responsible to the Integrated Audit and Governance Committee. The IGG will provide assurance to the CCG Governing Body regarding Information Governance.

8 REVIEW DATE

- These terms of reference will be reviewed annually along with the Information Governance Framework and Strategy.

Information Governance Incident Reporting Flow Chart Annex F