NHS
Scarborough and Ryedale
Clinical Commissioning Group

Information Governance Framework and Strategy Scarborough and Ryedale CCG November 2017

Authorship:	Information Governance Manager			
Committee Approved:	Audit and Governance Committee			
Approved date:	November 2017			
Review Date:	November 2020			
	Relevant	Screening	Full / Completed	Outcome
Equality Impact Assessment	No	No	No	Not applicable
Sustainability Impact Assessment	No		No	Not applicable
Privacy Impact Assessment	No	No	No	Not applicable
Bribery Checklist	No		No	Not applicable
Target Audience:	All CCG Staff			
Policy Reference No:	XXX			
Version Number:	V.3.2			

Publication/Distribution	Website	Email Staff	Others (i.e. SBC)
	Yes	Yes	No

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 Intranet
0.1	IG Manager	First draft for comments	NR	
1.0	IG Manager	Approved version	Quality and Clinical Governance Committee Feb 2014	
1.1	IG Manager	Updated to include social media	NR	
1.2	IG Manager	Amendments based on feedback	Audit Committee Feb 2015	
1.2	IG Officer	Scheduled review completed and no amendments required. Next review set at Sept 2017	Audit and Governance Committee November 2015	
2.0	IG Officer	Amendments to reflect Caldicott 2	Audit and Governance Committee March 201`6	
3.0	IG Officer	Updated for Changes in Relationship to Embed Updates to reflect General Data Protection Requirement Update the Job titles of those holding the key IG Roles within the CCG Update the Terms of Reference membership and additional responsibilities	Audit and Governance Committee November 2017	November 2017

Approval Record

Applicable Y/N	Committee / Group	Consultation / Ratification	Date taken to group	Date last Approved
	Governing Body	Ratification		
	Council of Clinical Representatives	Ratification		
	SMT	Ratification		
	Remuneration Committee	Ratification		
Yes	Audit and Governance Committee	Ratification	November 2017	November 2017
	Finance and Contracting Committee	Ratification		
	Business Committee	Ratification		
	Communications and Engagement Committee	Ratification		
Yes	Quality and Performance Committee	Ratification	February 2017	February 2017
	Primary Care Co-Commissioning Committee	Ratification		
	Other	Ratification		
	All Employees	Consultation		
	Public	Consultation		
	Yorkshire and Humber Social Partnership Forum	Consultation		

1 Introduction and Purpose

The purpose of this framework is to describe the management arrangements that will deliver Information Governance (IG) assurance within Scarborough and Ryedale CCG (SR CCG). 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.

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.

1.1 Information Governance Strategy

The development of a fixed IG Framework will support an IG Strategy that will develop over time with to be in compliance with current legislation and the current information governance toolkit. The current strategy is detailed at Annex A being put in place to support SR CCG.

1.2 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

2 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 SR CCG maintains high standards of IG.

2.1 Information Governance Toolkit (IGT)

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.

3 Roles and Responsibilities

3.1 Embed Health Consortium

SR CCG has in place a service level agreement (SLA) agreement with Embed Health Consortium to deliver a range of IG services including delivery of the IG Toolkit at Level Two.

3.2 Data Protection Officer

From May 2018 the General Data Protection Requirement (GDPR) makes it a mandatory requirement for all public bodies to appoint a Data Protection Officer who will be the cornerstone of accountability for Data Protection, facilitate compliance, inform the data controller and the

organisation of their obligations, promote a data protection culture and monitor compliance with GDPR. This role must be

- easily accessible – contact details to be available to data subjects and the Information commissioner's office (ICO)
- have integrity and high professional ethics
- be involved properly and in a timely manner in all issues relating to protection of personal data
- be consulted when a data breach or incident occurs
- be able to perform duties and tasks in an independent manner, must not be instructed, must be autonomous
- There should be no unfair termination of contract

3.3 Caldicott Guardian

The Caldicott Guardian for SR CCG is the CCG Executive Nurse.

The Caldicott Guardian is a senior person responsible for protecting the confidentiality of patient and service-user information and enabling appropriate and secure 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.

3.4 Senior Information Risk Owner (SIRO)

The SIRO for SR CCG is the Associate Director of Corporate Affairs.

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.

3.5 Information Governance Lead

The Information Governance Lead is the Chief Finance Officer.

The IG Lead works with the 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.

3.6 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.

3.7 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.

4 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.

5 Data Protection Act 1998 (DPA) and General Data Protection Regulation 2016 (GDPR)

The Data Protection Act and General Data Protection Regulation are the most fundamental pieces of legislation that underpin Information Governance. SR CCG are registered with the Information Commissioners Office and will fully comply with all legal requirements of the Act.

Under the General Data Protection Regulation it is a legal requirement to implement a process to ensure 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.

Where personal identifiable information is to be collected and processed a legal basis for doing so must be identified and documented in a data flow map of how that information is collected and used.

The Data Protection and General Data Protection Regulation Principles are detailed at Annex C.

6 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 D.

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 E.

7 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 information 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 has 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.

8 Risk Management

The ability to apply good risk management principles to IG is fundamental and all organisations will apply them through organisational policies. The 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 in to identified information assets will be risk assessed and the results reported to the CCG SIRO for risk mitigation, acceptance or transfer.

9 Third Party Contracts

The CCG will ensure that contracts with third parties providing services to and on behalf of the CCG include appropriate, detailed and explicit requirements regarding confidentiality and data protection to ensure that Contractors are aware of their IG obligations.

10 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 as set out in the on line IG Training Tool (IGTT).

Within the IGTT there are specific modules available for Caldicott, SIRO and IG staff themselves. Appropriate staff must complete the modules relevant to their roles.

The way in which all staff will access this training is through the IG Training Tool:

https://www.igtt.hscic.gov.uk/igte/index.cfm

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

11 Awareness and Advice

The Embed IG Team will provide advice on any IG related issue. They will be responsible for the production of newsletters and all staff e-mails to provide information to staff on IG issues.

12 Incident Management

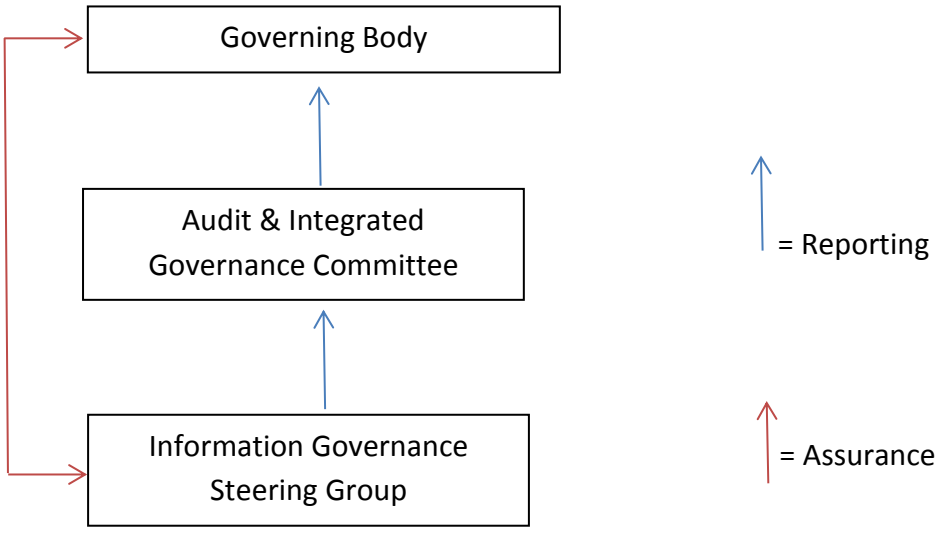
Incidents must be reported and managed through the CCG's Incident Policy. The Embed IG Team will have an active involvement in all IG related incidents and IG related service desk calls to ensure compliance with IG principles. Significant issues will be subject to full investigation and reporting action. Incidents relating to personal information will be highlighted to the Caldicott Guardian whilst those of a more technical nature will be reported to the SIRO.

13 Investigation

The Embed IG Team will be responsible for 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 IG Team will assist the CCG to maintain 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. All incidents must be reported within 24 Hours of being identified

14 Organisational Structures

As described in the SR CCG IG Strategy:



15 CCG Information Governance Steering Group

The Information Governance Steering Group will be established to support and drive the broader information governance agenda and provide the Governing Body with the assurance that effective information governance best practice mechanisms are in place within the organisation. The Group will meet every three months and be attended by the SIRO, Caldicott Guardian, Corporate Governance & Organisational Development Lead and a representative of the Embed Health Consortium providing the IG service. the Terms of Reference for this group are available on the CCG website at:

http://www.scarboroughryedaleccg.nhs.uk/publications/

16 APPENDIX ONE – CCG INFORMATION GOVERNANCE STRATEGY 2017-2020

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

- The CCG complies with all legal and statutory requirements
- The CCG has an information governance strategy that supports the achievement of corporate objectives this will be achieved through the development of an annual Information Governance Work programme
- The CCG can demonstrate an effective framework for managing information governance assurance and this is monitored by the CCG Audit and Integrated Governance Committee
- Staff are aware of their responsibilities and the importance of information governance
- information governance becomes a systematic, efficient and effective part of business as usual for the organisation
- Information governance is integrated into the change control process
- That there are effective methods for seeking assurance across the organisation and with its key partners
- That the organisation can demonstrate that the information governance arrangements of organisations it commissions services from across healthcare and commissioning support are adequate

17 APPENDIX TWO - SUPPORTING POLICIES AND GUIDANCE

- Data Protection & Confidentiality Policy
- Confidentiality: Code of Conduct Policy
- Records Management policy
- Safe Haven Policy
- Mobile working policy
- Information Security Policy
- Confidentiality Audit Policy
- Subject Access Request Policy
- Acceptable Computer Use Policy
- Email Policy
- IAO role and responsibilities
- Privacy Impact Assessment
- Information Governance Steering Group Terms of Reference

All of these documents are available on the CCG Internet site.

18 APPENDIX THREE – DATA PROTECTION PRINCIPLES

(Applicable until 25 May 2018, after which they will be replaced will GDPR Principles detailed below)

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.

18.1 Principles of Lawfulness of Processing Personal Identifiable Information

(Valid from 25 May 2018)

The GDPR requires that data controllers ensure personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

19 APPENDIX FOUR - DEFINITIONS

Data Controller: A natural or legal person, public authority, agency or other body alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor: A natural or legal person, public authority, agency or other body which processes data on behalf of the controller.

Processing: Any operation or set of operations which is performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by any means, alignment or combination, restriction, and destruction.

Personal Data: This means data which relating to an identified or identifiable natural person (data subject). This identifiable natural person is one who can be identified directly or indirectly by reference to:

- those data, or
- those data and any other information which is in the possession of, or is likely to come into the possession of, the data controller.

Identifiers can include name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological genetic, mental, economic, cultural or social identify of that natural person.

It also includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual

Sensitive Data: This means personal data consisting of information as to the:

- Concerning health, sex life or sexual orientation
- Racial or ethnic origins
- Trade union membership
- Political opinions
- Religious or philosophical beliefs
- Genetic data
- Biometric data

Anonymisation: This is where personal identifiers are removed from the data subjects information. However, even where such obvious identifiers are missing, rare diseases, drug treatments or statistical analyses which may have very small numbers within a small population may allow

individuals to be identified. A combination of items increases the chances of patient identification. Information may be used more freely if the data subject of that information is not identifiable in any way.

When anonymised data will serve the purpose, health professionals must anonymise data and whilst it is not necessary to seek consent, general information about when anonymised data will be used should be made available to patients.

Pseudonymisation: The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that the additional information is held separately and is subject to technical and organisational measures to ensure that personal data are not attributed to an identified or identifiable natural person.

Personal Data Breach: A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, or access to, personal data transmitted, stored or otherwise processed.