Hambleton, Richmondshire and Whitby
Clinical Commissioning Group

Information Governance Framework and Strategy

Hambleton, Richmondshire and Whitby CCG

Author Chris Wallace, Information Governance Manager

Date: August 2015

Approved By: Senior Management Team

Review Date: April 2017

Version: 2.1

Information Governance Framework HRW CCG

Introduction and Purpose

The purpose of this framework is to describe the management arrangements that will deliver Information Governance (IG) assurance within Hambleton, Richmondshire and Whitby CCG (HRWCCG). 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.

Information Governance Strategy

The development of a fixed IG Framework will support an IG Strategy that will develop over time with an initial 2013/14 version published at Annex A being put in place to support the first years of the existence of HRW CCG.

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

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 HRW maintains high standards of IG.

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.

North Yorkshire & Humber Commissioning Support Unit (NYHCSU)

HRW CCG has in place a service level agreement (SLA) agreement with NYHCSU to deliver a range of IG services including delivery of the IG Toolkit at Level 2.

Caldicott Guardian

The Caldicott Guardian for HRW CCG is the Clinical GP Board Member.

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.

Senior Information Risk Owner (SIRO)

The SIRO for HRW CCG is the Chief Operating & 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.

Information Governance Lead
The Information Governance Lead is the Chief Operating & Chief Finance Officer.

The IG Lead works with the CSU 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.

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.

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.

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.

Data Protection Act (DPA)

The Data Protection Act is the most fundamental piece of legislation that underpins Information Governance. HRW CCG 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 C.

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.

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.

Risk Management

The ability to apply good risk management principles to IG is fundamental and all organisations will apply them through organisational policies. The NYHCSU 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.

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.

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.

Awareness and Advice

The NYHCSU 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.

Incident Management

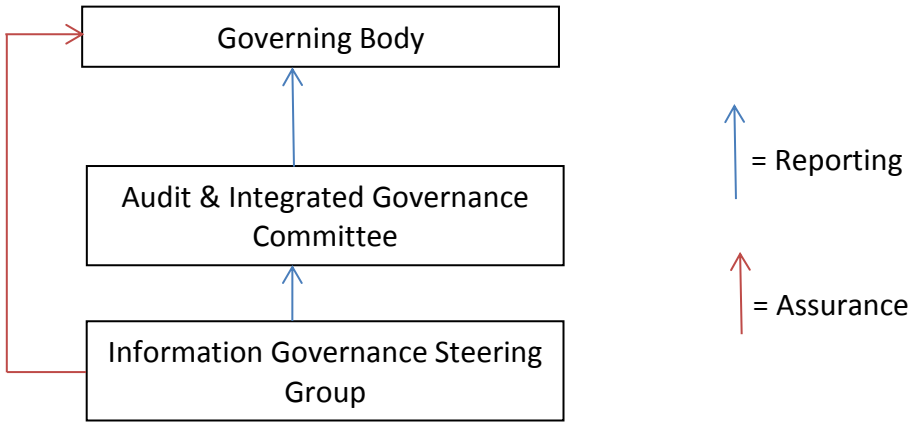
Incidents must be reported and managed through the CCG's Incident Policy. The NYHCSU IG Team will have an active involvement in all IG related incidents and IG related service desk calls to ensure compliance with IG principles. Significant issues will be subject to full investigation and reporting action. 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.

Investigation

The NYHCSU 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 Information Governance & Security Manager is a police trained investigator and the IG Team will 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.

Organisational Structures

As described in the HRW CCG IG Strategy:



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 CSU provided IG service. See Annex B for the Terms of Reference for this group.

ANNEX A

HRW CCG INFORMATION GOVERNANCE STRATEGY 2015-2017

1. The IG Strategy of HRW CCG 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 adequate

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
Bussiness Continuity and Strategy Policy
Confidentiality Audit Policy
Subject Access Request Policy
Acceptable Computer Use Policy
Email Policy
IAO role and responsibilities
Information Governance Checklist and Privacy Impact Assessment

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

Hambleton, Richmondshire and Whitby Clinical Commissioning Group

Information Governance Steering Group

Terms of Reference

Author(s)	IG Officer
Version	0.3
Version Date	August 2014
Implementation/approval Date	Aug 2014
Date Due for Review	Aug 2016
Review Body	Senior Management Team

Version	Author	Date	Amendment
0.1	NYH CSU IG Officer	May 2014	First Draft
0.2	Debbie Newton	29 May 14	Changes to core information
0.3	IGSG	Aug 2014	Review and update of IGSG membership
0.3	IGSG	July 2015	Reviewed and No Updates required

INDEX TO CONTENTS

1 Introduction

Information Governance is the discipline which, through the means of a formal framework, robust practices and procedures for handling personal confidential and corporately sensitive information is implemented. The Information Governance Steering Group has been established to oversee and monitor the implementation of the Clinical Commissioning Groups (CCG's) Information Governance Framework, including identifying lines of accountability and to ensure that information governance practices and procedures are embedded throughout the CCG.

2 Executive Summary

These Terms of Reference set out the rights and responsibilities of the group, to cover the work areas as follows:

- Confidentiality and Consent;
- Data Protection;
- Data Quality;
- Information Management;
- Information Disclosure and Sharing;
- Information Security;
- Records Management;
- Registration Authority and access control;
- Information Governance Incident Reporting and investigation; and
- Freedom of Information.

3 Purpose

The Information Governance Steering Group will be the organisation's forum with delegated authority to oversee the implementation of Information Governance practices, resolution of issues, development and implementation of appropriate work plans, in order to provide appropriate assurance on behalf of the CCG.

The group will liaise closely with the North Yorkshire and Humber Commissioning Support Unit Information Governance Team who co-ordinate operational Information Governance services on behalf of the organisation.

Overall Purpose

The Information Governance Group is a standing group accountable to the Audit and Information Governance Committee. The group's purpose is to support and embed the broader information governance agenda within the CCG and provide the Governing Body with assurance that effective information governance is in place within the organisation.

The Group is tasked with:

- ensuring organisation-wide engagement in the Information Governance Agenda in line with HSCIC Information Governance Toolkit;

- ensuring that the Information Governance Assurance Framework is documented and embedded across the organisation;
- providing a local forum for Information Governance team leads, disseminating national guidance and best practice; and
- to receive concerns, issues and problems with a view to determining appropriate resolutions.

Specific Responsibilities

Specific Responsibilities are as follows:

- cascade national guidance and advice;
- lead on local implementation of guidance and advice;
- receive and action Information Governance performance reports produced by the North Yorkshire and Humber Commissioning Support Unit, Information Governance Team;
- receive and review Information Governance policies and procedures;
- ensuring that agreed information governance strategies, policies and procedures are embedded within the culture and practice of the organisation and adhered to;
- ensuring that local operational leads are assigned for specific areas of the information governance agenda as appropriate, who will be responsible for providing evidence to support Information Governance Toolkit compliance and reviewing and approving toolkit scores in their designated area(s);
- receive reports of information governance incidents and take forward lessons learned resulting from the investigation of those incidents; and
- monitoring compliance of statutory and mandatory training in respect of Information Governance

4 Accountability and Delegated Authority

The Accountable Officer has overall accountability for ensuring that the organisation operates in accordance with statutory requirements as outlined in the Information Governance Management Framework.

The Chair/Vice Chair of the Information Governance Steering Group will provide quarterly updates to the Audit and Information Governance Committee for assurance. An updated work plan will be submitted to the Audit and Information Governance Committee alongside the organisation's annual submission of the Information Governance Toolkit for formal sign off and formally authorised by the Audit and Information Governance Committee prior to submission of the organisation's end of year toolkit scores.

Delegated Authority

The IG Steering Group is accountable to the Governing body through the Audit and Information Governance Committee and is authorised to:

- investigate any activity within its terms of reference
- seek any information it requires from any employee and all employees are directed to co-operate with any request made by the Group. This remit extends to those working on any of the statutory bodies' behalf; and

- co-ordinate and implement activities in line with these terms of reference, as part of the Information Governance work programme.

Confidentiality

- The Chair shall advise on all aspects of confidentiality with respect to the information presented to and discussed by the membership.
- All person-identifiable information shall be subject to the NHS Code of Confidentiality.

7 Steering Group Membership

The core membership of this group will be as follows:

Role	Responsible Member
Chair	CCG Senior Information Risk Owner (SIRO)
Co-chair and Caldicott Guardian	CCG Caldicott Guardian
Information Governance Operational Lead	CCG BSS Manager
Team Representatives	Delivery Group 1 & 2 Representatives
CSU IGT Team Representative	CSU Information Governance Manager or Officer

Where a member is unable to attend, a deputy or nominated representative should attend in their place.

Other staff may be requested to attend the meeting in relation to specific topics or the requirement to ensure implementation of appropriate information governance practices and procedures. There may also at times be a requirement for representatives from other NYH CSU departments e.g. Communications or Freedom of Information services and staff from the PCU.

8 Requirements for Quorum

The IG Steering Group shall be quorate as long as the either The Senior Information Risk Owner Officer or the Caldicott Guardian, the IG Operational Lead (or their designated representatives) and one member of the NYH CSU Information Governance Team are present.

9 Sub Groups

There are no sub-groups to the Information Governance Steering Group.

10 Schedule of Meetings

The Information Governance Steering Group will meet bi-monthly and synchronise with the Audit and Information Governance Committee holing the meeting 2 weeks prior to Audit and Governance Committee to be able to submit an updated work plan.

11 Reporting Arrangements

Action notes will be documented in the work plan and submitted to the Audit and Integrated Governance Committee and circulated by the North Yorkshire and Humber Commissioning Support Unit Information Governance Team

12 Administration

- the agenda will be managed by the Information Governance Team and circulated to members at least 3 working days prior to the meeting along with relevant papers;
- The work plan including agreed actions will be documented and circulated to all members within 5 working days of the meeting;
- any queries regarding the actions should be referred to the Information Governance Team.

13 Performance and Monitoring

The effectiveness of the IG Steering Group will be measured as part of the Information Governance Toolkit assessment and the associated audit. A report on the effectiveness of the IG Steering Group will be provided to the Audit and Integrated Governance Committee on a least an annual basis.

Approved By: IGSG August 2014. Reviewed July 2015

Annex C

Data Protection 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.