



## **Barnsley Clinical Commissioning Group**

Putting Barnsley People First

# **Information Governance Policy and Management Framework**

<b>Version:</b>	2.0
<b>Approved By:</b>	Governing Body
<b>Date Approved:</b>	February 2014
<b>Name of originator / author:</b>	Richard Walker
<b>Name of responsible committee/ individual:</b>	Governing Body (initial approval), IG Group / QPSC (review)
<b>Name of executive lead:</b>	Vicky Peverelle
<b>Date issued:</b>	December 2015
<b>Review Date:</b>	2 years from issue / review date
<b>Target Audience:</b>	All Barnsley CCG staff

## Amendments Log

Version No	Type of Change	Date	Description of change
DRAFT		January 2014	
1		16 January 2014	<i>Approved by Governing Body</i>
1.1	Annual Review by IG Group	October 2014	Reflect change of SIRO from CFO to Chief of Corporate Affairs (approved by QPSC, Sep 2014) and other minor amendments
2.0	Review	November 2015	General policy review Update of IG framework ( third party contract requirements, policy approval schedule), layout changes

## Contents

Item	Page
1. Introduction	4
2. Scope	4
3. Legislation	5
4. Principles	5
4.1 Openness	5
4.2 Legal Compliance	6
4.3 Information Security	6
4.4 Information Quality Assurance	7
5. Information Governance within WSYB CSU	7
6. Year on Year Improvement Plan and Assessment	7
7. Information Governance Management	7
8. Policy Implementation and Review	8
Appendix A: NHS Barnsley CCG Information Governance Management Framework	9
Appendix B: Policy Approval Schedule	16

## **Information Governance Policy**

### **1. Introduction**

The CCG recognises the importance of reliable information both in terms of the clinical management of individual patients and the efficient management of services and resources.

Information governance plays a key part in supporting clinical governance, service planning and performance management. It also gives assurance to the CCG and to individuals that personal information is dealt with appropriately, lawfully, securely and effectively in order to deliver the best possible care.

The Information Governance Policy and Management Framework sets out how the organisation will meet the key requirements of a wide range of information governance related matters. It establishes and promotes a culture of good practice around the processing of information and use of information systems that supports the provision of high quality care to users of our services. The framework also supports compliance with law and national guidance and standards such as the Information Governance Toolkit.

The CCG will establish and maintain policies, procedures and guidance to implement this framework with which all staff are required to comply.

### **2. Scope**

This policy must be followed by all staff who work for or on behalf of the CCG including those on temporary or honorary contracts, secondments, volunteers, pool staff, Board members, students and the Yorkshire and Humber Commissioning Support (YHCS) staff working on behalf of the CCG. The policy is applicable to all areas of the organisation and adherence should be included in all contracts for outsourced or shared services. There are no exclusions.

This policy and framework covers all aspects of information within the organisation, including (but not limited to):

- Patient/Client/Service User information
- Personnel/Staff information
- Organisational information
- Structured and unstructured record systems - paper and electronic

- Photographic images, digital, text or video recordings including CCTV
- All information systems purchased, developed and managed by/or on behalf of the organisation
- CCG information held on paper, floppy disc, CD, USB/Memory sticks, computers, laptops, tablets, mobile phones and cameras

The processing of all types of information, including (but not limited to):

- Transferring of information – fax, e-mail, post, telephone and removable media such as laptops and memory sticks, etc.
- Sharing of information for clinical, operational or legal reasons
- The storage and retention of information
- The destruction of information

Information governance within an independent contractor's premises is the responsibility of the owner/partners. However, the CCG is committed to supporting independent contractors in their management of information risk and will provide advice, share best practice and provide assistance when appropriate.

The CCG recognises the changes introduced to information management as a result of the Health and Social Care Act 2012 and will work with national bodies and partners to ensure the continuing safe use of information to support services and clinical care.

Failure to adhere to this policy may result in disciplinary action and/or referral to the appropriate regulatory bodies including the police and professional bodies.

### **3. Legislation**

Key law and standards that apply to information governance includes, but is not limited to:

- The Data Protection Act 1998
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice
- Caldicott Guidance
- The Freedom of Information Act 2000
- Protection of Freedoms Act 2012
- Health and Social Care Act 2012
- The Computer Misuse Act 1990
- Mental Capacity Act 2005
- Records Management: NHS Code of Practice
- The Public Records Act 1958
- Current Performance Standards (NHS IG Toolkit)
- Copyright, Designs and Patents Act 1988

- Care Act 2014
- Health and Social Care Act (Safety and Quality) 2015

## **4. NHS Barnsley CCG Principles**

### **4.1 Openness**

- Information on the CCG and its services should be available to the public through a variety of media, in line with the CCG's Freedom of Information Policy (subject to it not being exempt from disclosure). What constitutes 'exempt' information is defined by law and decisions by the Information Commissioner and/or the Information Tribunal.
- The CCG will undertake or commission annual assessments and audits of its information governance policies and its arrangements for openness.
- Patients should have access to information relating to themselves including their own health care, their options for treatment and their rights as patients.
- Staff will have access to information about themselves including their rights as employees.
- The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media.
- The CCG will have clear procedures and arrangements for handling queries from patients and the public.

### **4.2 Legal Compliance**

- The CCG regards all identifiable personal information relating to patients as confidential.
- The CCG will undertake or commission annual assessments and audits of its compliance with legal requirements in relation to information governance.
- The CCG regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise and in the public interest.
- The CCG will establish and maintain policies to ensure compliance with the Data Protection Act, Freedom of Information Act, Human Rights Act and the common law duty of confidentiality.
- The CCG will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation.
- The CCG will investigate all breaches of confidentiality and security, and failure to comply with key information governance policies in line with CCG incident reporting processes.
- The CCG will work with partner NHS bodies and other agencies to establish Information Sharing Protocols to inform the controlled and appropriate sharing of patient information with other agencies,

taking account of relevant legislation (e.g. Health and Social Care Act, Data Protection Act, Crime and Disorder Act, Children Act)

### **4.3 Information Security**

- The CCG will establish and maintain policies for the effective and secure management of its information assets and resources.
- The CCG will undertake or commission annual assessments and audits of its information and IT security arrangements.
- The CCG will promote effective confidentiality and security practice to its staff through the dissemination of its policies, the establishment of local procedures, and staff training and awareness.
- The CCG will establish and maintain incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security.
- The CCG will appoint a Senior Information Risk Owner and assign responsibility to Information Asset Owners to manage information risk.

### **4.4 Information Quality Assurance**

- The CCG will establish and maintain policies and procedures for information quality assurance and the effective management of records.
- The CCG will undertake or commission annual assessments and audits of its information quality and records management arrangements.
- Managers are expected to take ownership of, and seek to improve, the quality of information within their services.
- Wherever possible, information quality should be assured at the point of collection.
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards.
- The CCG will promote information quality and effective records management through policies, local procedures/user manuals and staff training and awareness.
- All new projects, processes and systems (including software and hardware) which are introduced must meet confidentiality and data protection requirements. To enable the organisation to address the privacy concerns a Privacy Impact Assessment (PIA) must be used.

## **5. Information Governance within Yorkshire and Humber Commissioning Support (YHCS)**

Important intelligence functions are carried out on NHS Barnsley CCG's behalf by YCHS. NHS Barnsley CCG will ensure that YCHS' information governance including information security, quality assurance and staff training is carried out to the standards required by this policy.

## **6. Year on Year Improvement Plan and Assessment**

An assessment of compliance with the requirements in the Information Governance Toolkit (IGT) will be undertaken each year. Annual assessments and proposed action/development plans will be presented to the CCG's Quality and Patient Safety Committee. The requirements are grouped into the following initiatives:

- Information Governance Management
- Confidentiality and Data Protection Assurance
- Information Security Assurance
- Clinical Information Assurance

## **7. Information Governance Management**

The details of the NHS Barnsley CCG's management and accountability arrangements for information governance are documented in the Information Governance Management Framework which forms an appendix to this policy.

## **8. Policy implementation and review**

This policy and framework will be implemented with effect from January 2014. The policy will be reviewed at least every 2 years, and sooner if there is a change in legislation.

# Appendix A: NHS Barnsley CCG - Information Governance Management Framework

## A1: Key IG Roles

### IG Lead:

The role of the IG Lead will be carried out by the Head of Assurance. The IG Lead:

- Is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of IG
- Is responsible for liaising with West and South Yorkshire and Bassetlaw CSU, who are providing IG services to the CCG, to ensure IG provision meets legislative and national requirements

### Senior Information Risk Owner (SIRO):

The role of the SIRO will be carried out by the Chief of Corporate Affairs. The SIRO:

- Is responsible for leading and fostering a culture that values, protects and uses information for the success of the organisation and benefit of its customers
- Is responsible for ensuring that organisational information risk is properly identified, managed and that appropriate assurance mechanisms exist
- Owns the CCG's information risk policy and risk assessment processes ensuring they are implemented consistently by Information Asset Owners
- Is responsible for advising the Chief Officer on the information risk aspects of the organisation's statement on internal controls
- Owns the CCG's information incident management framework

### Caldicott Guardian:

The role of the Caldicott Guardian will be carried out by the Chief Nurse. The Caldicott Guardian:

- Is responsible for leading on confidentiality and data protection issues relating to patient information
- Is a champion for confidentiality and information sharing requirements and issues at senior management level
- Is responsible for overseeing all arrangements including protocols and procedures, for the use and sharing of patient information
- Is responsible for ensuring that confidentiality requirements are reflected in CCG strategies, policies and working procedures for staff

## **A2: Key Policies**

NHS Barnsley CCG will maintain the following key policies to support effective Information Governance:

- Information Governance Policy and Management Framework
- Confidentiality Code of Conduct
- Email Policy
- Internet Policy
- Information Quality Assurance Policy
- Information Security Policy
- Network Security Policy
- Records Management Policy
- Remote Working and Portable Devices Policy
- Information Governance Accreditation Process

NHS Barnsley CCG will also maintain a suite of related policies, procedures and guidance supplementary to the key policies listed above.

Details of all the above policies, including where the policy was last approved and the date of last approval are detailed in appendix 2.

Each policy will be subject to an implementation plan:

- All policies will be maintained on the NHS Barnsley CCG Intranet
- Corporate communications tools will be used as appropriate to disseminate policies
- Policies will be incorporated into induction and training sessions as appropriate

## **A3: Key Governance Bodies**

The Information Governance agenda will be led by the Information Governance Group, co-ordinated by the Head of Assurance who and supported by staff of YHCS.

The Information Governance Group will report through the *Quality and Patient Safety Committee* to Governing Body. The annual IG Toolkit submission, IG Action Plan and new or significantly amended strategies and policies will be reported to the Quality and Patient Safety Committee for their consideration and onward approval by Governing Body.

#### A4: Roles and Resources

The key roles and responsibilities for the delivery of the Information Governance agenda in NHS Barnsley CCG and the completion of the IG Toolkit are identified in the table below:

NHS Barnsley CCG Role	Information Governance Responsibilities
Head of Assurance	<ul style="list-style-type: none"> <li>• Information Governance lead</li> <li>• Records Management lead</li> <li>• IG Group member – collates items for consideration</li> </ul>
Chief Finance Officer	<ul style="list-style-type: none"> <li>• IG Group member</li> </ul>
Chief of Corporate Affairs	<ul style="list-style-type: none"> <li>• SIRO</li> <li>• Freedom of Information/ Environmental Information lead</li> <li>• IG Group member</li> </ul>
Chief Nurse	<ul style="list-style-type: none"> <li>• Caldicott Guardian</li> <li>• Confidentiality Lead</li> <li>• IG Group member</li> <li>• Deputy Chair of Quality and Patient Safety Committee</li> </ul>
Governance, Assurance & Engagement Facilitator	<ul style="list-style-type: none"> <li>• Information Governance Support</li> </ul>
IG Lead (CSU)	<ul style="list-style-type: none"> <li>• Information Governance Toolkit lead officer</li> <li>• Data Protection officer</li> <li>• Support to the roles of SIRO, Caldicott Guardian and CCG IG Lead through the provision of expert advice</li> <li>• Lead officer for the development and maintenance of Barnsley wide information sharing policies and protocols</li> <li>• IG Group member</li> </ul>
IT Customer Services and Registration Authority Manager (CSU)	<ul style="list-style-type: none"> <li>• Registration Authority (RA) manager</li> </ul>
Information Security Lead (CSU)	<ul style="list-style-type: none"> <li>• Information Security lead officer</li> </ul>

## **A5: Governance Framework**

**The CCG Information Governance Group** takes a lead on the implementation of this framework and related policies and guidance. It reports to the CCG Quality and Patient Safety Committee with Governing Body oversight via CCG Governance processes.

**The IG Department of YHCS and relevant commissioned services** are responsible for developing and maintaining policies, standards, procedures and guidance, coordinating and raising awareness of Information Governance and identifying and organising training, supporting the roles of the SIRO, Caldicott Guardian and other CCG staff through the provision of expert advice.

**All Managers** within the CCG are responsible for ensuring that the overall IG policy and framework, and its supporting policies, standards and guidance, are built into local processes and that there is on-going compliance. Team/service specific procedures should be put in place where required, for example, regarding the place of storage and retention schedule of specific records. Line managers should inform staff about their information governance responsibilities and what this means in practice through generic and workplace induction and team meetings. Specific information governance and training needs should be identified through the annual performance development review.

**Individuals** working for the CCG, whether permanent, temporary or contractors have a personal common law duty of confidence to patients and to their employer. It is the responsibility of all staff to ensure that they are familiar with the requirements incumbent upon them in relation to information governance and for ensuring that they comply with these on a day to day basis. A confidentiality clause is incorporated into all staff contracts; all staff and any person with access to CCG information are required to sign a declaration of confidentiality and information security. Staff should report any information risks they identify, or information incidents, through organisational processes.

**Information Asset Owners (IAOs)** have been identified for the CCG's key information assets. IAOs are responsible for managing their information assets including associated risks. IAOs required to routinely risk assess their information assets and report these findings to the SIRO and CSU IG Lead via organisational processes. IAOs should know what information is contained within their asset, ensure the asset is held securely, restricting access as appropriate, and is used appropriately.

**Information Asset Administrators** have been identified where appropriate and support IAOs and manage information assets on a day to day basis.

## **A6: Third Party Contracts**

Contracts with third parties providing services to Barnsley CCG must include appropriate, detailed and explicit requirements regarding confidentiality and information governance to ensure that Contractors are aware of their IG obligations.

### **Clinical Services**

All clinical services commissioned by or on behalf of the CCG will be required to:

- Have a suitable contract in place to form a joint data controller relationship regarding the information required to effectively monitor commissioned services.
- Ensure the services commissioned meet the requirements of the Data Protection Act when providing services including, but not limited to, fair processing and maintaining a registration with the Information Commissioners Office.
- Complete the annual Information Governance Toolkit and if requested, undertake an independent audit, to be disclosed to the CCG in order to provide further assurance they have met expected requirements.
- Ensure privacy notices make individuals aware of a CCG's role in commissioning and the personal and sensitive data it may receive to undertake such a role.
- Ensure that where any IG incidents occur that they are reported to the CCG via routes determined within the contract.
- Set out expectations regarding providing information in relation to requests for information made under the Freedom of Information Act.
- Ensure inclusions regarding Exit Plans are addressed following transfer of services or decommission of service e.g. Passing on data/deletion/ retention of data at end of the contract.

### **Support services**

All support services that process information on behalf of the CCG will be required to:

- Ensure a suitable contract/SLA and or as a minimum a confidentiality agreement is in place to form a Data Controller to Data Processor relationship where Personal or Personal Sensitive data is managed on behalf of the CCG.
- Ensure that the services commissioned meet the requirements of the Data Protection Act when providing services including, but not limited to, fair processing and maintaining a registration with the Information Commissioners Office.
- Complete the annual Information Governance Toolkit (if applicable) and at the request of the CCG undertakes a compliance check/ audit, in order to provide assurance they have met expected requirements.
- Ensure that any new processing is within the remit of the contract or seek written confirmation if there is any ambiguity.
- Report any known incidents or risks in relation to the use or management of information owned by the CCG.
- Set out expectations regarding providing information in relation to requests for information made under the Freedom of Information Act.

- Ensure inclusions regarding Exit Plans are addressed following transfer of services or decommission of service e.g. passing on data / deletion/ retention of data at end of the contract.

## A7: Training and Guidance

Appropriate Information Governance Training is delivered via OLMS and the Information Governance Training Tool (IGTT).

The Introduction to Information Governance course is mandatory for ALL staff.

The table below shows the additional training which is required for specific job roles:

Course	Resource	Recommended (unless stated mandatory)	Duration
Information Governance & IG Management (3 modules)	Introduction to Information Governance then <i>IG Refresher</i> on an annual basis thereafter	<b>Mandatory</b> for ALL Staff	1 hours
	Access to Information and Information Sharing in the NHS*	Staff who work with Personal Confidential Data (PCD), IAOs and IAAs	
Information Risk Management (3 modules)	NHS Information Risk Management: Introductory*	<b>Mandatory</b> for IAAs and any staff who work with personal confidential data (PCD)	1 hour
	NHS Information Risk Management: Foundation*	<b>Mandatory</b> for the SIRO, IAOs and members of the IG Group	1 hour
	NHS Information Risk management for SIRO's and IAO's)*	<b>Mandatory</b> for the SIRO, IAOs and members of the IG Group	1 hour
Information Security (3 modules)	Password Management*	For staff who use computers	0.5 hours
	Information Security Guidelines*	Staff who use computers	
	Secure Transfers of Personal Data*	Staff who work with PCD	
Confidentiality and Caldicott (1 module)	The Caldicott Guardian in the NHS and Social Care*	For the Caldicott Guardian	1 hour

Records Management (3 modules)	Records Management and the NHS Code of Practice*	<b>Mandatory</b> for staff with responsibility for Records Management	0.5 hours
	Records Management in the NHS*	<b>Mandatory</b> for staff with responsibility for Records Management	0.5 hours
	Access to Health Records*	Staff handling Subject Access Requests	

\*e-learning available via the IG Training Tool at <https://www.igtt.hscic.giv.uk/igte/index.cfm>

Progress with the completion of mandatory training is monitored and reported to Governing Body as part of the mandatory training programme.

### **A8: Incident Management**

The management of information and IT related incidents in NHS Barnsley CCG is incorporated within CCG Incident Reporting and Management processes.

These processes are brought to all staff attention through the induction process.

A documented Information Security Risk Assessment and Management programme is in place.

The assurance of information risk and information incident management is the responsibility of the IG lead (CCG).

Information Governance and IT related incidents, including cyber security incidents must be reported and managed through the CCG Incident and Near Miss Reporting Policy Incorporating Serious Untoward Incident Procedure. An information governance incident of sufficient scale or severity to be classified as a Level 2 Serious Incident Requiring Investigation (SIRI) or cyber SIRI will be:

- Notified immediately to the CCG's SIRO and Caldicott Guardian
- Reported to the Department of Health, Information Commissioners Office and other regulators via STEIS and the HSCIC Incident reporting tool
- Investigated and reviewed in accordance with the guidance in the HSCIC checklist
- Reported publicly through the CCGs Annual Report and Governance Statement

## Appendix B: Policy Approval Schedule

Policy Name	Owner	Responsible Organisation	Last Approved By	Last Issued Date	Review Date
Information Governance Policy and Management Framework	IG Group	Barnsley CCG	Governing Body	January 2014	November 2015
Confidentiality Code of Conduct	IG Group	Barnsley CCG	Governing Body	February 2014	February 2016
Email Policy	IG Group	Barnsley CCG	Governing Body	February 2014	February 2016
Internet Policy	IG Group	Barnsley CCG	Governing Body	February 2014	February 2016
Information Quality Assurance Policy	IG Group	Barnsley CCG	Governing Body	February 2014	February 2016
Information Security Policy	IG Group	Barnsley CCG	Governing Body	February 2014	February 2016
Network Security Policy	YHCS	YHCS			
Records Management Policy	IG Group	Barnsley CCG	Governing Body	February 2014	February 2016
Remote Working and Portable Devices Policy	IG Group	Barnsley CCG	Governing Body	February 2014	February 2016
Information Governance Accreditation Process	IG Group	Barnsley CCG	Governing Body	February 2014	February 2016