NHS

Bolton Clinical Commissioning Group

Information Governance Policy

Policy Number	**IG001**
Target Audience	**CCG**
Approving Committee	**CCG Chief Officer**
Date Approved	**March 2020**
Last Review Date	**January 2020**
Next Review Date	**January 2022**
Policy Author	**IG Team**
Version Number	**V6.1**

The CCG is committed to an environment that promotes equality, embraces diversity and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the CCG's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Approved documents are valid for use after their approval date and remain in force beyond any expiry of their review date until a new version is available.

Version Control Sheet

Version	**Date**	**Reviewed By**	**Comment**
0.1	August 2013	M Robinson/ D Sankey	Progress to CCG Executive team for approval
1	August 2013	CCG Executive Team	Approved
1.1	January 2014	Andrea Hughes	Amendment to Section 5
	January 2014	IM&T Ops Board	Approved
1.2	November 2015	IG Team	Review document for approval
2.0	December	IM & T Ops Board	Approved
3.0	December 2017	IG Team	Review document for approval
4.0	January 2018	IM & T Ops Board	Approved
5.0	February 2018	CCG Chief Officer	Approved.
5.1	January 2020	IG Team	Reviewed
6.0	February 2020	IG Board	Approved
6.1	March 2020	CCG Chief Officer	Approved.

Analysis of Effect completed	By: M Robinson	Date: August 2013

Contents

1 Introduction

This document sets out minimum policy standards and common policy directions across Bolton Clinical Commissioning Group (here after referred to as ‘the CCG’) for confidentiality, integrity and availability of information also known as Information Governance.

This policy is important in helping the staff who work for the CCG to understand that the CCG has an IG Framework in place to ensure staff are able to look after the information they need to do their jobs, and ensure this information is protected on behalf of patients and staff.

Information Governance is a framework for handling personal information in a confidential and secure manner to appropriate ethical and quality standards in a modern health service. It also provides a consistent way for employees to deal with the many different information handling requirements including:

- Information Governance Management
- Clinical Information assurance for Safe Patient Care
- Confidentiality and Data Protection assurance
- Corporate Information assurance
- Information Security assurance
- Secondary use assurance
- Respecting data subjects’ rights regarding the processing of their personal data

The formal framework that leaders of all health and social care organisations should commit to is set out in the National Data Guardian’s ten data security standards. These are the basis of the Data Security and Protection Toolkit that health and social care organisations must use to assess their information governance performance.

Under data protection legislation, organisations that process personal data are accountable for, and must be able to demonstrate their compliance with the legislation. The arrangements set out in this and related policies and procedures are intended to achieve this demonstrable compliance.

2 Purpose

The purpose of this policy is to inform CCG staff (permanent or otherwise), of their Information Governance responsibilities and the management arrangements and other policies that are in place to ensure demonstrable compliance. This is the central policy in a suite of policies that informs staff of what they should do:

- To maximise the value of organisational assets by ensuring that CCG demonstrates data is:
    - Held securely and confidentially
    - Processed fairly and lawfully

    - Recorded accurately and reliably
    - Used effectively and ethically; and
    - Shared and disclosed appropriately and lawfully

- In order to protect the organisations information assets from all threats, whether internal or external, deliberate or accidental, the CCG will ensure:

    - Information will be protected against unauthorised access
    - Confidentiality of information will be assured
    - Integrity of information will be maintained
    - Information will be supported by the highest quality data
    - Regulatory and legislative requirements will be met
    - Business continuity plans will produced, maintained and tested
    - Information governance and security training will be available to all staff, and
    - All information governance breaches, actual or suspected, will be reported to, and investigated by, the Information Governance Manager in conjunction with the Data Protection Officer.

3 Scope

This policy applies to those members of staff who are directly employed by and for whom the CCG has legal responsibility. For those staff covered by a letter of authority / honorary contract or work experience the organisation's policies are also applicable whilst undertaking duties for or on behalf of CCG. Further, this policy applies to all third parties and others authorised to undertake work on behalf of CCG. The collective term 'staff' is used throughout this policy to mean all these groups.

This policy applies to all forms of information, including but not limited to:

- Paper and electronic filing systems
- Communications, including those sent by post, electronic mail, text messaging
- Information that is stored in and/or processed by information systems including servers, personal computers (PCs), any other mobile device
- Information that is stored, copied, moved or transferred to any type of removable or portable transmission, both internal or externally to a third party.

This policy covers all information systems purchased, developed and managed by or on behalf of, the CCG and any individual directly employed or otherwise by the CCG.

Accurate, timely and relevant information is essential in continuing to deliver the highest quality care throughout the area. As such it is the responsibility of all staff at all levels to ensure and promote the quality of information and to actively use information effectively in decision making processes.

4 Roles and Responsibilities

Chief Officer

Overall accountability for procedural documents across the CCG lies with the Chief Officer as the 'Accountable Officer' that has overall responsibility for establishing and maintaining an effective document management system and the governance of information, meeting all statutory requirements and adhering to guidance issued in respect of information governance and procedural documents.

Responsibilities will be delegated to:

Caldicott Guardian

The Clinical Director for Governance and Safety has been appointed Caldicott Guardian. They will:

- Ensure that the CCG satisfies the highest practical standards for handling patient identifiable information;
- Facilitate and enable information sharing and make decisions on behalf of the CCG following advice on options for lawful and ethical processing of information, in particular in relation to disclosures;
- Represent and champion Information Governance requirements and issues at Board level;
- Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff, and
- Oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS.

Senior Information Risk Owner (SIRO)

The Chief Finance Officer has been appointed SIRO. They will:

- Take overall ownership of the organisation's Information Risk Policy;
- Understand the strategic business goals of the CCG and how other NHS organisations' business goals may be impacted by information risks, and how those risks may be managed;
- Implement and lead the Information Governance Risk Assessment and Management processes within the CCG;
- Advise the Board on the effectiveness of information risk management across the CCG, and
- Receive training as necessary to ensure they remain effective in their role as SIRO.

Data Protection Officer (DPO)

The Associate Director for Governance and Safety has been appointed DPO. The DPO reports directly to the Board about data protection matters. These may include information governance risks to the organisation, privacy concerns or recommendations with regard to potential changes to, or new initiatives that, involve processing of personal data.

With support from the Information Governance Manager they will:

- Provide advice to the CCG on compliance obligations with data protection law;
- Advise on when data protection impact assessments are required;
- Monitor compliance with data protection law and organisational policies in relation to data protection law;
- Co-operate with, and be the first point of contact for the Information Commissioner's Office (ICO);
- Be the first point of contact within the CCG for all data protection matters;
- Be available to be contacted directly by data subjects, and
- Take into account information risk when performing the above.

Information Asset Owners (IAOs)

IAOs under the responsibility of the SIRO will:

- Lead and foster a culture that values, protects and uses information for the success of the CCG and benefit of its patients and staff;
- Know what information comprises or is associated with the asset(s), and understand the nature and justification of information flows to and from the asset;
- Know who has access to the asset, whether system or information, and why, and ensure access is monitored and compliant with policy;
- Understand and address risks to the asset and provide assurance to the SIRO;
- Ensure there is a legal basis for processing and for any disclosures;
- Ensure all information assets are recorded on the Information Asset Register (IAR) and maintained;
- Refer queries about any of the above to the Information Governance Manager, and
- Undertake specialist information asset training as required.

Information Governance Manager

They will:

- Maintain an awareness of information governance issues within the CCG;
- Review and update the information governance policy in line with local and national requirements;

- Ensure that line managers are aware of the requirements of the Information Governance policy, and
- Work with the Caldicott Guardian, SIRO and DPO functions to ensure organisational authority and awareness regarding issues relating to data protection or confidentiality concerns.

Head of IT and the Cyber Security Lead

The role of the Information Governance Manager is supported by the Head of IT and the Cyber Security Lead.

The Head of IT and the Cyber Security Lead are responsible for developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure the CCG's systems and infrastructure remain compliant with data protection legislation.

The Head of IT and the Cyber Security Lead are responsible for ensuring that all CCG electronic equipment and assets have adequate security measures to comply with data protection and data security legislation and regulations.

Information Governance (IG) Board

The IG Board consists of various key members of the CCG including the Data Protection Officer, IG Manager, Head of IT and Cyber Security Lead and will:

- Oversee the implementation of the Information Governance strategy, policy and completion of the annual baseline assessment, Data Security and Protection Toolkit and associated work programme and ad hoc Information Governance related work stream projects, and
- Provide the CCG's Executive Team with regular updates and reports to highlight any risks to compliance.

Line Managers

Line Managers will take responsibility for ensuring that the Information Governance Policy is implemented within their staff group or directorate.

All Staff

It is the responsibility of each employee to adhere to this policy and all associated information governance policies and procedures.

Staff will receive instruction and direction regarding the policy from several sources:

- DPO
- Information Governance Manager
- Policy / strategy and procedure manuals
- Line manager
- Specific training course
- Other communication methods, for example, team meetings; and
- CCG website

All staff are mandated to undertake mandatory information governance training in line with the training needs analysis programme as agreed by the IG Board.

Information governance training is required to be undertaken on an annual basis by all staff.

All staff must make sure that they use the organisation's IT systems appropriately and adhere to the Acceptable Use Policy.

Section 170 (1) of the Data Protection Act 2018: Unlawful obtaining etc of personal data, states it is an offence for a person knowingly or recklessly:

(a) to obtain or disclose personal data without the consent of the controller;
(b) to procure the disclosure of personal data to another person without the consent of the controller, or
(c) after obtaining personal data, to retain it without the consent of the person who was the controller in relation to the personal data when it was obtained.

Staff must report any incident involving a breach or suspected breach of the Data Protection legislation to their line manager immediately and via the Incident Reporting System, Safeguard. The incident will be investigated by the Information Governance Manager with support from the Data Protection Officer, if required.

5 Information Governance Policy Framework

The CCG will maintain an Information Governance Policy Framework. This will be supported by a set of related information governance policies and procedures which are aligned with the NHS Operating Framework and the Data Protection and Security Toolkit requirements.

Associated Information Governance Policies

Policies	Description
Information Governance Management Framework	This document details how the CCG approach Information Governance. Detailing IG roles, IG training for all staff, how incidents will be managed, the key IG documents that are required, the reporting structure in terms of which committee / group IG reports to.
Confidentiality and Data Protection Policy	This policy sets out the roles and responsibilities for compliance with data protection legislation. It lays down the principles that must be observed by all who work within the CCG and have access to personal or confidential business information. All staff must be aware of their responsibilities for safeguarding confidentiality and preserving information security in order to comply with common law obligations of confidentiality and the NHS Confidentiality Code of Practice
Records Management Policy	This policy is to promote the effective management and use of information, recognising its value and importance as a resource for the delivery of

	corporate and service objectives.
Information Risk Policy	This policy aims to provide a consistent way of managing information risk in the CCG, allowing the information to be managed in a way that highlights when information may be at a significantly high risk, thereby providing a layer of protection for patients, staff and the organisation. Highlighting risks allow them to be properly addressed and the risk managed in a way that is most suitable.
Secure Transfer of Information Guidance	This procedure provide guiadance on how to safely and securely transfer confidential information from one place to another.
Corporate Information Security Policy	This policy is to protect, to a consistently high standard, all information assets. The policy defines security measures applied through technology and encompasses the expected behaviour of those who manage information within the organisation

Many of these proposals are supported by underpinning procedures. The Data Security / Information Governance Handbook provides a brief introduction to Information Governance and summarises the key user obligations that support the Information Governance policies and procedures.

In addition, specific procedural documents will be part of the Information Governance suite of policies which will be supported by those framework documents, above.

This policy should be read in conjunction with the Information Governance Management Framework which aims to document and capture the CCG's approach to Information Governance (IG) / Data Security and the Confidentiality and Data Protection Policy which provides specific guidance to staff on their data protection responsibilities.

This policy list is not exhaustive and changes in the organisation may lead to additional documents or changes to this list.

6 Monitoring and Review

This policy will be monitored through staff awareness and supporting evidence to the Data Security and Protection Toolkit.

This Policy will be reviewed on an annual basis, and in accordance with the following, on an as and when required basis:

- Legislative changes
- Good practice guidance
- Case law
- Significant incidents reported; new vulnerabilities, and
- Changes to organisational infrastructure.

7 Legislation

Information will be defined and where appropriate kept confidential, underpinning the principles of:

Legal Acts:

- General Data Protection Regulation
- Data Protection Act 2018
- Freedom of Information Act 2000
- Environmental Information Regulations
- Access to Health Records Act 1990
- Regulation of Investigatory Powers Act
- Health and Social Care Act 2012
- Human Rights Act 1998.

Supporting Documents:

- NHS Code of Confidentiality
- Caldicott Guardian Manual 2017
- NHS Information Risk Management;
- Records Management NHS Code of Practice for Health & Social Care 2016
- Data Security and Protection Toolkit (DSPT)
- Caldicott Reports
- ICO Guidance

8 Other relevant Procedural Documents

A set of Procedural Documents will be made available via the CCG Intranet.

- IG009 Confidentiality Audit Procedure
- IG013 Subject Access Procedure
- IG007 Incident Management Procedures
- IG012 Secure Transfer of Information Procedure

This list is not exhaustive

Staff will be made aware of procedural document updates as they occur via team briefs, team meetings and notification via the CCG staff intranet.