Bolton Clinical Commissioning Group

Information Governance Policy

Policy Number	**IG001**
Target Audience	**CCG/ GMSS Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**February 2018**
Last Review Date	**February 2018**
Next Review Date	**February 2020**
Policy Author	**GMSS IG Team**
Version Number	**V5.0**

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.

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

Contents

1 Introduction and aims

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 (Information Governance). The policy is intended to cover the overlapping areas of the current Data Protection Act 1998 compliance, the General Data Protection Regulation (GDPR) compliance, Freedom of Information Act 2000 compliance, Information Security Management Systems (ISO 27001:2005), Data Quality and Confidentiality (with regard to 'common law').

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.

The CCG recognises the role Information Governance plays in ensuring the organisation processes and handles its personal, sensitive, business information in accordance with UK laws and Department of Health Policy, thus protecting the CCG, its employees and just as importantly, its patients.

Information Governance affects ALL employees, including anyone providing a service on behalf of the CCG, whether permanent or temporary. EVERYBODY has responsibilities for IG on a day-to-day basis, regardless of their working environment (clinical or non clinical). Contractors working for the CCG are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply.

It is of paramount importance to ensure that information is efficiently and legally managed, and that the appropriate policies, procedures, guidance and management accountability and structures provide a robust governance framework for information management.

The Information Governance Agenda of this CCG will be managed by the Greater Manchester Shared Services (GMSS), Information Governance team.

The GMSS IG Team will establish and maintain policies and procedures on behalf of the CCG to ensure compliance with requirements contained in the Department of Health Information Governance Toolkit.

Information Governance sits alongside Clinical Governance, Research Governance and Corporate Governance. It provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of personal information. It also provides a consistent way for employees to deal with the many different information handling requirements including:

- information governance management;
- clinical information assurance;
- confidentiality and data protection assurance;
- corporate information assurance;
- information security assurance; and

- secondary use assurance.

The aims of this document are to maximise the value of organisational assets by ensuring that data is:

- held securely and confidentially;
- obtained 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 breaches of information security, actual or suspected, will be reported to, and investigated by, the GMSS Information Governance Team.

2 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.

3 Information Governance Policy Framework

The CCG will maintain an Information Governance Policy Framework. This will be supported by a set of related policies and procedures to cover all aspects of Information Governance and which are aligned with the NHS Operating Framework and the Information Governance Toolkit requirements.

The Policy framework will encompass the following:

- Records Management Policy
- Corporate Information Security Policy
- Information Risk Policy
- Acceptable Use of IT & Equipment Policy (includes email & internet)
- Encryption Policy
- Confidentiality & Data Protection Policy

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

4 Principles

The CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The CCG fully supports the principles of corporate, clinical and information governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about patients and staff and information of a commercially sensitive nature. The CCG also recognises the need to share information with other health and social care organisations and other agencies in a controlled manner consistent with the interests of the patients and, in some circumstances, the public interest, in the line with the Freedom of Information Act 2000.

Four key strands support the Information Governance Policy:

- Openness:
- Legal Compliance;

- Information Security and Confidentiality;
- Information Quality Assurance;

Openness

- Information will be defined and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations outlined in the General Data Protection Regulation (GDPR) and the Data Protection Act 1998;
- non-confidential information on the CCG and its services should be available to the public through a variety of media, in line with the Freedom of Information Act 2000;
- patients should have ready access to information relating to their own health care, their options for treatment and their rights as patients;
- the CCG will have clear procedures and arrangements for handling queries from patients and public;
- the CCG will have clear procedures and arrangements for liaison with the press and broadcasting media.

Legal Compliance

- The CCG regards all identifiable personal information relating to patients and staff as confidential. Health care related information will be regarded as sensitive along with certain other types of information (e.g. Child protection data);
- the CCG regards all identifiable personal information relating to patients and staff as confidential except where national policy on accountability requires otherwise;
- the CCG regards all corporate information as confidential;
- the CCG is required to establish and maintain policies to ensure compliance with the GDPR, Human Rights Act, Computer Misuse Act, Privacy and Electronic Communications Act, Common Law of Confidentiality and any other relevant legislation;
- the CCG will establish and maintain policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

Information Security and Confidentiality

- The Head of Service for Integrated Governance, provides the following Information Security support:
- use of the Head of Service for Integrated Governance Information Security (IS) qualifications as a qualified lead auditor for Information Security;
- undertake an IS Audit of a key information Asset process and generate a report for the CCG SIRO.
- the CCG will work towards attaining and maintaining compliance against the International / British Standard for Information Security Management ISO 27001;
- the CCG will establish and maintain policies for the effective and secure management of its information assets and resources;

- the CCG will promote effective confidentiality and security practice to its staff through policies, procedures and training;
- the CCG will have regularly maintained business continuity plans for all critical infrastructure components and core information systems;
- 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.

Information Quality Assurance and Records Management

- 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, procedures/user manuals and training.

5 Accountability, Responsibilities and Training

The Chief Officer has ultimate responsibility for the implementation of the provisions of this policy. As the 'Accountable Officer' they are responsible for the management of the organisation and for ensuring that the appropriate mechanisms are in place to support service delivery and continuity.

The CCG has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of and compliance with internal and external governance requirements

Responsibilities will be delegated to:

A Caldicott Guardian who will:

- ensure that the CCG satisfies the highest practical standards for handling patient identifiable information;
- act as the conscience of the CCG;
- facilitate and enable information sharing and advise on options for lawful and ethical processing of information;
- 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;

- oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS.

A Senior Information Risk owner (SIRO) will:

- be an Executive Director or Senior Management Board Member;
- take overall ownership of the Organisations Information Risk Policy
- act as champion for information risk on the Board and provide advice to the Accounting Officer on the content of the Organisation's Statement of Internal Control in regard to information risk;
- 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;
- work with GMSS (supplier of IG) to manage the NHS Information Governance risk assessment and management processes within the CCG;
- advise the Board on the effectiveness of information risk management across the CCG;
- receive training as necessary to ensure they remain effective in their role as SIRO.

A Data Protection Officer (DPO) will:

- report to the highest management level of the CCG;
- have proven expert knowledge of data protection law and practices;
- provide advice to the CCG on compliance obligations, and when data protection impact assessment is required;
- monitor compliance with the GDPR and organisational policies;
- co-operate and liaise with the Information Commissioner;
- take into account information risk when performing the above.

Information Asset Owners (IAO) (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 customers;
- know what information comprises or is associated with the asset, 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 providing assurance to the SIRO.

IM&T Operations Board will:

- oversee the implementation of the Information Governance strategy, policy and completion of the annual baseline assessment and

associated work programme and ad hoc Information Governance related work stream projects;
- provide the Executive Team with regular updates and reports to highlight any risks to compliance;
- ensure the CCG IG Lead is in attendance.

Information Governance Supplier, GMSS will:

- manage the Information Governance Team to deliver Information Governance for the CCG;
- maintain an awareness of information governance issues within the CCG;
- review and update the information governance policy in line with local and national requirements providing template documents to the CCG;
- ensure that line managers are aware of the requirements of the Information Governance policy.

Line managers will:

- Take responsibility for ensuring that the Information Governance Policy is implemented within their staff group or directorate, including any temporary or contract staff;
- ensure staff understand it is their responsibility to adhere to the policy;
- ensure staff will receive instruction and direction regarding the policy from a number of sources:

    - policy/strategy and procedure manuals;
    - line manager;
    - specific training course;
    - other communication methods, for example, team meetings; and staff Intranet.

CCG Employees will:

- comply with this policy whilst working within the CCG and thereafter for as long as the information remains confidential information;

- report any incident involving a breach or suspected breach of the General Data Protection Regulation and the Data Protection Act 1998 to their line manager immediately and via the Incident Reporting System, Safeguard. Where advice is required they will contact the CCG Information Governance Lead and / or the GMSS IG Team;

- undertake the “Introduction to Information Governance” e-learning module. Information Governance training is required to be undertaken on an annual basis. The CCG will decide where relevant further training and education will be required of staff. Staff will be informed via the Information Governance Training Needs Analysis.

6 Monitoring and review

This policy will be monitored through staff awareness and supporting evidence to the NHS IG 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;
- 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 Information Governance: Guidance on Legal and Professional Obligations;
- NHS Code of Confidentiality;
- Information Security Management: NHS Code of Practice April 2007;
- Caldicott Guardian Manual 2017;
- NHS Information Risk Management;
- NHS Records Management Code of Practice 2016;
- The Information Governance Toolkit;
- Caldicott Reports

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.

A number of other policies in the General Policy/Strategy Manual are related to this policy and all employees will be made aware of the full range.