Bolton Clinical Commissioning Group

Information Governance Management Framework

Policy Number	**IG010**
Target Audience	**CCG Staff**
Approving Committee	**CCG Chief Officer**
Date Approved	**July 2018**
Last Review Date	**July 2018**
Next Review Date	**July 2019**
Policy Author	**GMSS IG Team**
Version Number	**7.0**

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.

Bolton Clinical Commissioning Group

Version Control Sheet

Version	Date	Reviewed By	Comment
0.1	September 2013	Suzanne Bell	Document development
0.1	September 2013	Mike Robinson, Annette Walker, Grace Birch, Dr Mercer, Diane Sankey	Document Review
1.0	September 2013	CCG Board	Approved
1.1	September 2014	NWCSU	Section 4, Training and Guidance updated
2.0	November 2014	IM&T Ops Board	
2.0	January 2015	CCG Board	Approved
2.1	June 2015	IG Team	Document Review
2.1	July 2015	IM&T Ops Board	Approved
3.0	June 2016	IG Team	Document Review, Section 3, Senior Roles updated to include Information Security Support. GMSS replacing NWCSU throughout document.
3.1	June 2016	IM&T Ops Board	Approved
4.0	May 2017	IG Team	Document Review
5.0	December 2017	CCG Chief Officer	Approved
6.0	June 2018	IG Team	Document Review – Inclusion of DPO role, DSP Toolkit and minor amendments
7.0	July 2018	CCG Chief Officer	Approved

Analysis of Effect completed	By: Suzanne Bell	Date: 19th September 2013

Contents

1 Introduction

The Information Governance Framework document aims to capture Bolton Clinical Commissioning Group's (CCG) approach to Information Governance (IG), Data Security and Protection.

Robust IG requires clear and effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources. The way that the CCG will deliver this is documented within this Information Governance Management Framework. This will be reviewed annually by the IG Board.

The Information Governance Framework must be read in conjunction with the CCG's Information Governance Policy and associated procedures (for a list, refer to section 7).

The Framework provides a summary / overview of how the CCG is addressing the Information Governance agenda and adapted appropriately to the capacity and capability of the organisation.

There are many different standards and legislation that apply to IG and information handling, including, but not limited to:

Data Protection Act 2018	Health and Social Care Act 2012	Freedom of Information Act 2000
The General Data Protection Regulation May 2018	A Guide for Confidentiality in Health and Social Care	Common Law Duty of Confidentiality
International Information Security standard: ISO/IEC 27002: 2005	Access to Health Records Act 1990	Information Security NHS Code of Practice
Caldicott Guidance	Computer Misuse Act 1990	Mental Capacity Act 2005
Public Records Act 1958	Records Management Code of Practice for Health and Social Care 2016	Human Rights Act 1998

2 Strategic Aims

The aim of this Framework is to set out how Bolton CCG will effectively manage IG. The organisation will achieve compliance by:

- Establishing, implementing and maintaining local CCG policies for the effective management of IG;
- Establishing robust IG processes that conforms to Department of Health standards and comply with all relevant legislation;
- Ensuring information is provided accordingly to service users, stakeholders and shareholders about how information is recorded, handled, stored and shared and managed;
- Providing clear advice, guidance and training to all staff to ensure that they understand and apply the principles of IG to their working practice;
- Sustaining an IG culture through increasing awareness and promoting IG, thus minimising the risk of breaches of personal data;
- Assessing CCG performance using the Data Security and Protection Toolkit and Internal Audits, developing and implementing action plans to ensure continued improvement.

3 Senior Roles

Accountable Officer
The Chief Officer (CO) has overall responsibility for Information Governance within Bolton CCG, this is Susan Long. As Accountable Officer, Susan is responsible for the management of Information Governance and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Information Governance provides a framework to ensure information is used appropriately and is held securely.

Senior Information Risk Owner (SIRO)
The Senior Information Risk Owner (SIRO) is held by a member of the CCG Executive Board. They are responsible for identifying and managing the information risks to the CCG. This includes oversight of the organisation's information security / governance incident reporting and response arrangements and the Registration Authority business process. For Bolton CCG, the SIRO role will be the responsibility of Ian Boyle, Chief Financial Officer.

Caldicott Guardian
The Caldicott Guardian is a senior person responsible for protecting the confidentiality of the patient and service user information and enabling appropriate information sharing. For Bolton CCG, this will be Dr Jane Bradford, CCG Clinical Director.

Data Protection Officer (DPO)
The General Data Protection Regulation (GDPR) May 2018 requires all public authorities to nominate a DPO. This role is a senior role with reporting channels directly to the highest level of management and has the requisite professional qualities and expert knowledge of data protection compliance. The role involves:

- Developing and maintaining comprehensive and appropriate documentation that demonstrates commitments to and ownership of IG responsibilities, for example, production of an IG Framework document supported by relevant policies and procedures
- Advising colleagues on compliance
- Training and awareness raising
- Monitoring compliance and carrying out Audits
- Providing advice regarding Data Protection Impact Assessments
- Being the main point of contact with the Information Commissioners Office
- Main expert knowledge in Data Protection.

The Data Protection Officer for Bolton CCG is the Associate Director of Governance and Safety, Michael Robinson.

CCG Information Governance Lead
The Associate Director of Governance and Safety has been appointed to act as the overall CCG Information Governance Lead for Bolton CCG. This role is the responsibility of Michael Robinson.

The Information Governance Board
The CCG's Information Governance Board which reports to the Executive Team controls the implementation and compliance of data security principles. The responsibilities of the group include, but are not limited to:

- Recommending for approval and adoption all related polices, protocols, strategies and procedures within the IG arena, having due regard to legal and NHS requirements.
- Ensuring the CCG has appropriate evidence available to support the achievement of the Data Security and Protection Toolkit.
- Recommending for approval the annual submission of compliance with the requirements in the Data Security and Protection Toolkit and related action plans.
- To co-ordinate and monitor the IG Policy across the organisation.
- Make recommendations on the necessary resourcing to support requirements.
- To address all issues surrounding the information management and information security that may affect the CCG.
- To identify and approve all necessary staff information and training as outlined in the Data Security & Protection Toolkit.
- Ensure that risks are included on the corporate risk register.

Please refer to the approved Information Governance Board Terms of Reference (TOR) for further detail.

Greater Manchester Shared Services (GMSS) Information Governance Team Responsibilities

The CCG has been assigned a GMSS Information Governance Manager who will be the delegated IG Manager for the CCG's. IG support will also be provided by the GMSS Senior Information Governance Officer(s) and the GMSS–IG Central Team.

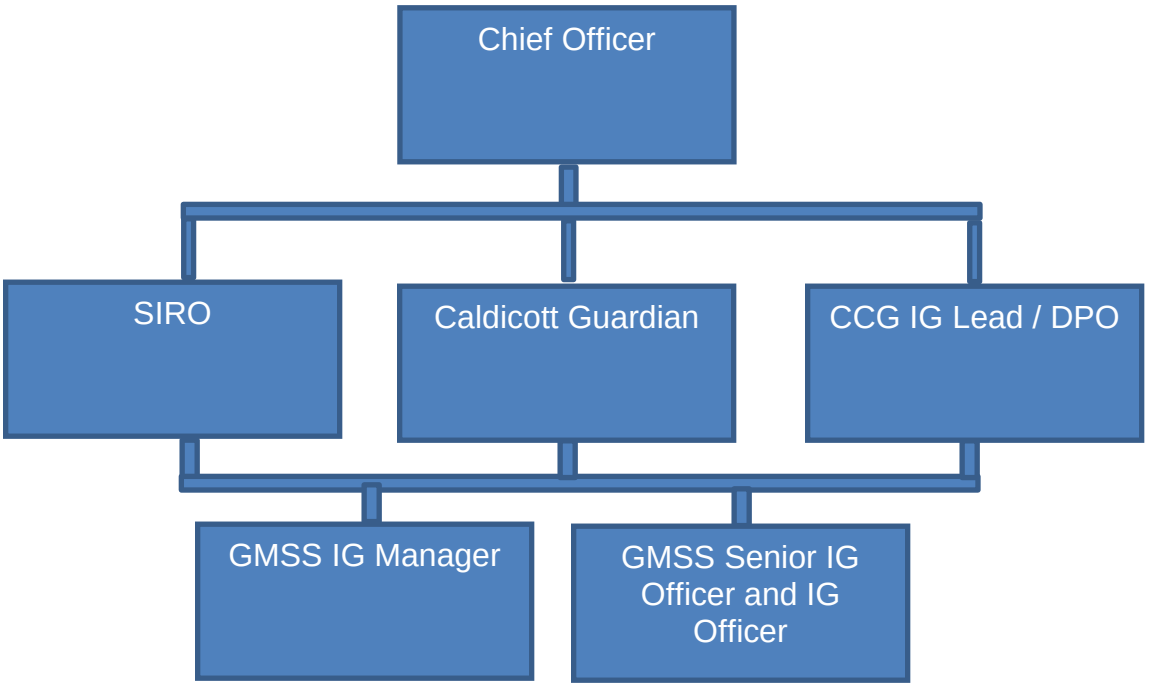
The GMSS Information Governance Manager will be responsible for ensuring all tasks delegated to GMSS meet the required standards in line with any formal undertaking between the parties.

The GMSS IG Team will be responsible for ensuring all tasks delegated to GMSS meet the required standards in line with any formal undertaking between the parties.

Key tasks will include:

- Developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitments to and ownership of IG responsibilities, for example, production of IG Framework document supported by relevant policies and procedures
- Ensure that there is top level awareness and support for IG resourcing and implementation of improvements with the CCG Executive Team
- Establishing working groups, if necessary, to co-ordinate the activities of staff with IG responsibilities
- Ensuring annual assessments and audits of IG are implemented and reported
- Ensuring that annual assessment and regular improvement plans / progress reports are prepared for approval by the Caldicott Guardian, IG Lead, SIRO and DPO
- 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
- 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

- Providing a focal point for the resolution and / or discussion of Information Governance issues
- Take into account the findings of Department of Health Information Governance reports and publications and the impact on the CCG.



All staff

All staff, whether permanent, temporary, contracted or contractors are responsible for ensuring that they are aware of their responsibilities in respect to IG.

4 Governance Framework

Responsibility and accountability for IG is cascaded through the CCG and is co-ordinated by the CCG IG Lead & GMSS IG Team via the following:

- IG Board (agenda / minutes / actions)
- Staff contracts of employment
- Information Sharing Agreement / Data Processor Agreement
- IG Questions for Tender and new and / or changes to services / assets
- Data Protection Impact Assessment Proforma
- Information Asset Ownership – documented within the Information Asset Register
- IG Training
- IG Training Needs Analysis
- IG Updates in CCG Staff bulletins
- IG Policies and Procedures

5 Training & Guidance

Staff in the CCG will receive clear guidelines on expected working practices and the consequences of failing to follow policies and procedures via the methods as outlined above in the Governance Framework section.

Information Governance training is outlined in the IG Training Needs Analysis (TNA).

All staff are mandated to undertake Information Governance Training on an annual basis.

Staff who have additional responsibilities within their role may be required to undertake additional modules as identified in the CCG IG TNA.

All agency / temporary staff must have evidence of adequate Information Governance training and / or undertake the mandatory IG training programme as identified in the CCG IG TNA.

Additional Information Governance training and advice is provided to staff on request.

6 Information Governance Incident Management

All IG incidents are reported using the CCG's IG Incident Reporting Procedure (IG007). Staff must report any IG incident to BOLCCG.Incidents@nhs.net or via the CCG's incident reporting system available on the intranet http://sgmvmresap78/safeguard/ . The IG Incident Reporting Procedure outlines the extra reporting requirements, guidance on the assessment of IG incidents and is available on the CCG Internet.

GMSS IG Officers will score and classify IG / data security incidents in accordance with the NHS Digital "Guide to the Notification of Data Security and Protection Incidents" (May 2018).

Incidents will be assessed following the 'Breach Assessment Grid' which can be found in the above Guide.

Any breaches other than "green breaches" are reportable using the Data Security and Protection Toolkit.

Where an IG / data security incident / breach relates to a vulnerable group in society as defined in the guidance, the minimum score will be a 2 in either significance and likelihood unless incident contained.

Where the incident is assessed that it is (at least) likely that some harm has occurred and that the impact is (at least) minor, full details will be automatically emailed to the Information Commissioners Office and the NHS Digital Data Security Centre.

The Department for Health and Social Care will also be notified where it is (at least) likely that harm has occurred and the impact is at least serious.

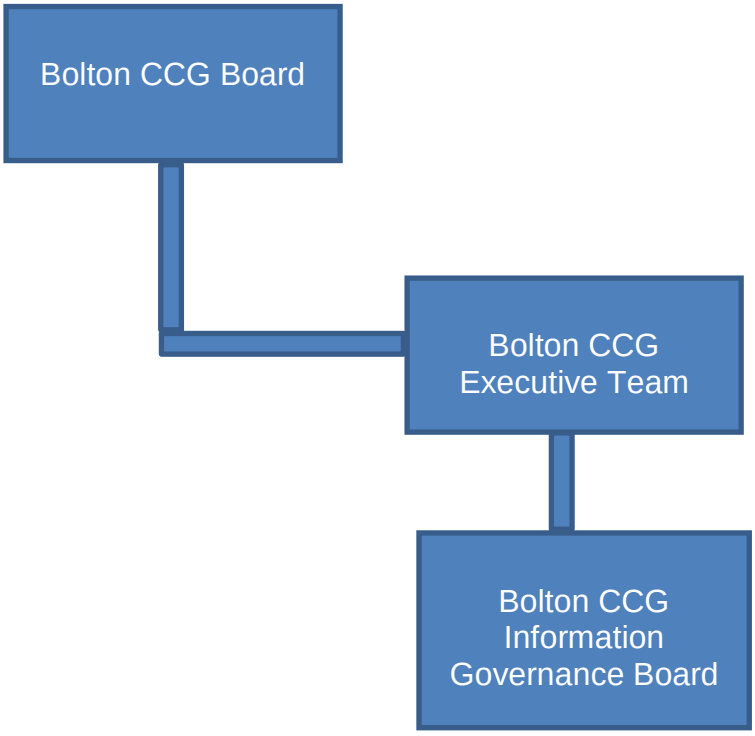
Incidents must be reported within 72 hours. This 72 hours starts when the CCG becomes aware of the breach which may not necessarily be when it occurred. Where the 72 hours deadline is not met an organisation must provide an explanation. Failure to notify promptly may result in additional action by the ICO in respect of GDPR.

7 Reporting Structure

The CCG's IG Board reports to the CCG Executive Team. IG updates are provided as necessary to the Executive Team by the Chief Officer, SIRO and DPO. Please see the IG Board Terms of Reference for further information.

IG related policies including this IG Framework are approved at the IG Board and finally ratification is received from the Chief Officer.

IG Procedures / Guidance, the IG Training Needs Analysis, IG Board Terms of Reference are approved and ratified by the IG Board. Minutes from the IG Board are received by the Executive Team ensuring they are kept abreast of any approval activity.



8 Key Information Governance Documentation

- IG001 Information Governance Policy
- IG002 Confidentiality and Data Protection Policy
- IG003 Corporate Information Security Policy
- IG004 Acceptable Use Policy (IT, Email and Internet)
- IG005 Records Management Policy
- IG006 Information Risk Policy
- IG007 Information Governance Incident Reporting Procedure
- IG008 IG Staff Handbook
- IG009 Confidentiality Audit Procedure
- IG010 Information Governance Management Framework

- IG011 Data Privacy Impact Assessment Procedure & Template
- IG012 Secure Transfer of Information Procedures
- IG013 Subject Access Procedures
- IG Training Needs Analysis