NHS
Bury
Clinical Commissioning Group

Information Governance Framework

Version:	6.0
Ratified by:	Information Governance Operational Group
Date ratified:	20th July 2018
Name of originator /author (s):	GMSS Information Governance Team
Responsible Committee / individual:	Audit Committee
Date issued:	July 2018
Review date:	July 2019
Target audience:	NHS Bury Clinical Commissioning Group Members and Staff
Completed Equality Analysis:	Yes

Further information regarding this document

Document name	Information Governance Framework CCG.GOV.024.6.0
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	GMSS Information Governance Team
This document should be read in conjunction with	Information Governance Policy; Records Management Policy; Information Risk Policy; Freedom of Information Policy; Acceptable Use Policy; Confidentiality Guidelines for staff; Safe Transfer of Information Policy (safe haven).
This document has been developed in consultation with	NHS Bury Clinical Commissioning Group Development Team
Published by	NHS Bury Clinical Commissioning Group Townside Primary Care Centre 1 Knowsley Place, Knowsley Street, Bury, BL9 0SN Main Telephone Number: 0161 762 1500
Copies of this document are available from	The Corporate Office, Bury CCG, Townside PCC

Version Control

Version History:		
Version Number	Reviewing Committee / Officer	Date
4.0 = ratified	NHS Bury Clinical Commissioning Group, Audit Committee	9th September 2016
4.1 = draft revision	NHS Bury Clinical Commissioning Group, Information Governance Operational Group	25th May 2017

5.0 = ratified	NHS Bury Clinical Commissioning Group, Audit Committee	2nd June 2017
5.1 = draft revision	GMSS IG Team	26th June 2018
6.0 = ratified	NHS Bury Clinical Commissioning Group	20th July 2018

Contents

1. Introduction

The Information Governance Framework document aims to capture NHS Bury CCG's 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 the CCG will deliver this is documented within this Information Governance Framework. This Framework will be approved by the Information Governance Operational Group and reviewed annually.

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.

This Information Governance Framework must be read in conjunction with the CCGs Information Governance suite of Policies and Procedures which includes but is not restricted to:

- Information Governance Policy;
- Data Protection and Confidentiality Policy;
- Confidentiality Guidance for Staff;
- Secure Transfer of Information Procedure;
- Information Risk Policy;
- Information Security Policy;
- I.T. Suite of policies;
- Records Management Policy;

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 1
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 Bury 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. Roles and Responsibilities

3.1. Accountable Officer

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

3.2. 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 CCG has appointed a Data Protection Officer

3.3. Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) role should be held by a member of the CCG Executive Board. For Bury CCG, the SIRO role will be the responsibility of Chief Finance Officer and be responsible for identifying and managing the information risks to the CCG. This includes oversight of the organisation's Information Security Incident Reporting and response arrangements and the Registration Authority business process.

3.4. 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.

The CCG has appointed a Caldicott Guardian

3.5. CCG Information Governance Lead

The CCG has been appointed a CCG Information Governance Lead to act as the overall Lead for the CCG.

3.6. Greater Manchester Shared Services (GMSS) Information Governance Team

The CCG has been assigned a GMSS Information Governance Manager who will act as the delegated IG Manager for the CCG's. IG support will also be provided by the GMSS Senior Information Governance Officer 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.

Key tasks will include:

- The development and maintenance of comprehensive and appropriate documentation that demonstrates commitments to and ownership of IG responsibilities, e.g. the production of an overarching high level Framework document supported by relevant policies and procedures;
- ensuring that there is top level awareness and support for IG resourcing and implementation of improvements with the CCG clinical executive;
- the establishment of working groups, if necessary, to coordinate the activities of staff with IG responsibilities and progress initiatives;
- annual assessments and audits of IG and other related policies are carried out documented and reported;
- annual assessment and improvement plans are prepared for approval by the DPO, Caldicott Guardian, SIRO and IG Lead;
- the approach to information handling is communicated to all staff and made available to the public;

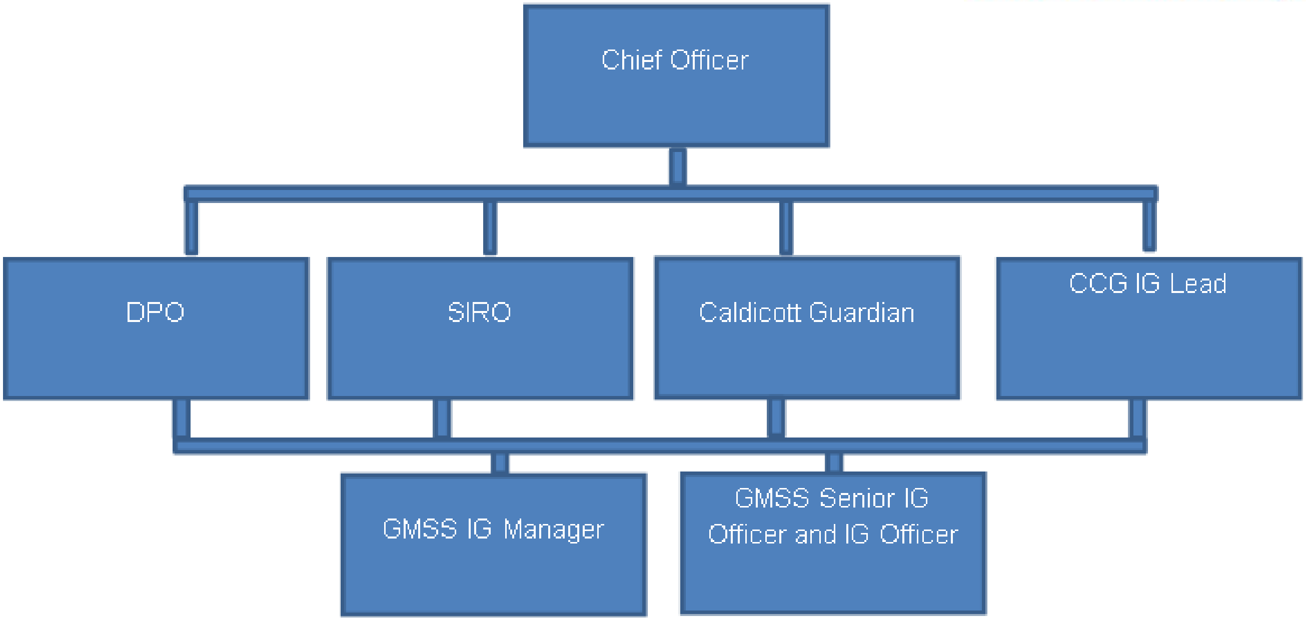
- appropriate training is made available to staff and completed as necessary to support their duties;
- liaison with other committees, working groups and programme boards in order to promote and integrate IG standards;
- the monitoring of information handling activities to ensure compliance with law and guidance;
- there is provision for a focal point for the resolution and/or discussion of IG issues;
- take into account the findings of Department of Health Information Governance reports and publications and the impact on the CCG.

3.7. Information Governance Operational Group

The CCG's Information Governance Operational Group which reports to the Audit Committee and Governing Body, controls the implementation and compliance of IG 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 illegal and NHS requirements;
- 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 and Protection Toolkit;
- ensure that risks are included on the corporate risk register.

Refer to the approved Information Governance Operational Group Terms of Reference (TOR) for further detail.



3.8. 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 and GMSS IG Officers via the following:

- IG Operational Group (see below);
- 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 and related Policies and Procedures.

5 Training and Guidance

All staff in the CCG will receive training consummate with their roles and responsibilities around information handling and management.

As a minimum all staff are required to complete the mandatory IG module using the agreed method detailed in the IG Training Needs Analysis.

The SIRO, Caldicott Guardian, IG Lead and Information Asset Owner's (IAO) must complete relevant additional modules using the agreed method detailed in the IG Training Needs Analysis, and all remaining staff shall be asked to complete additional modules as befitting their roles, as part of their Personal Development Review (PDR) process.

All agency/temporary staff must have evidence of adequate accredited IG training and/or undertake the mandatory IG training programme. This must be evidenced by managers.

New starters who have previously received IG Training within the current financial year at their previous organisation may carry over their IG training certificate. This will be subject to the member of staff providing evidence and the IG Officer checking the quality of the training.

GMSS IG Staff are officially trained in Data Protection and Freedom of Information (ISEB qualification).

Training and advice is provided to staff on request.

6. Information Governance Incident Management

All incidents are reported via the CCG's IG Incident Reporting Procedure.

An IG Incident Reporting Procedure informs staff of the extra reporting requirements regarding IG incidents and is available on the CCG intranet.

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.

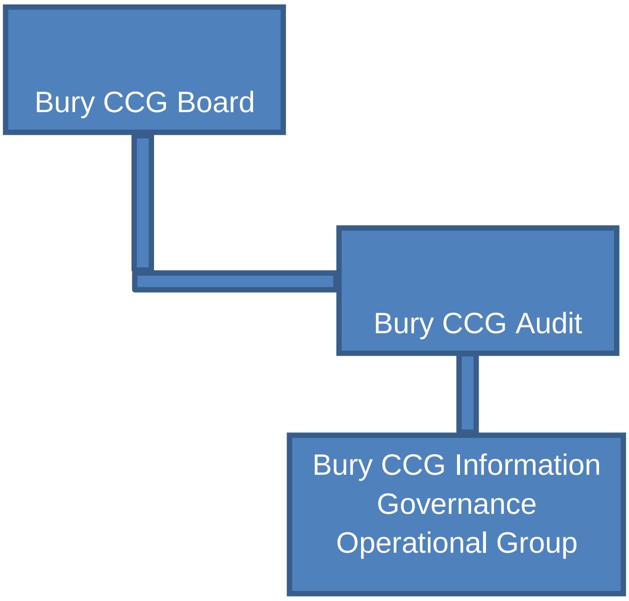
Incidents must be reported within 72 hours. This 72 hours starts when the CCG becomes aware of the breach which may not necessarily be when it occurred. Where the 72 hours deadline is not met an organisation must provide an explanation. Failure to notify promptly may result in additional action by the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

7. Reporting Structure

The CCG's IGOG reports to the CCG Audit Committee. IG updates are provided as necessary to the Audit Committee by the CCG IG Lead. Please see the IGOG's Terms of Reference for further information.

IG related policies including this IG Framework are approved at the IGOG and finally ratification is received from the Audit Committee.

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



Appendix A - Services specified under the GMSS Service Level Agreement

Ref	*Service Area*	Scope of Service
1	*Information Governance Framework*	• Creation of an outline framework covering service provision and which can be added to for local customer requirements
2	*Information Governance parts of Information Security Management System*	• Information Asset Register support and management • Information risk assessment reports and assurance reports on an annual basis • Information risk reviews on requested systems • Information Governance audits and reports
3	*Data Security and Protection (DSP) Toolkit*	• Provide resource to support and manage evidence gathering for DSP Toolkit returns. • Provide information customer auditors – direct auditors to evidence not held locally, for example. • Provide updates and risk/issues advice to customer senior management teams • Manage returns for customers
4	*Information Governance Training*	• Monitor attainment levels for mandatory information governance training using the agreed method detailed in the IG Training Needs Analysis • Provide agreed timescale reporting of training coverage • Provide IG briefings to staff: Articles for publications – 4 per year Face to face – minimum 4 per year (TBA) • Advise on extended/specialist training requirements
5	*IG Policies*	• Produce generic IG policies and procedures suite • Review policies annually • Provide generic staff Handbook • Provide Privacy Notice wording or oversight of Privacy Notices to ensure compliance
6	*Information Incident Management*	• Where information incidents occur, relating to personal and confidential information, provide support and guidance in the management of incidents through to resolution • Provide Root Cause Analysis advice, reporting and guidance
7	*Data Protection Impact Assessments*	• Provide template DPIA process • Provide resource for major projects and major procurement to ensure IG requirements are met • Reports and recommendations for projects to follow

Ref	Service Area	Scope of Service
8	*Subject Access Requests*	• Provide support to teams dealing with SARs to advise, review and provide guidance. • Provide support and reporting for SAR related complaints processes.
9	*Information Sharing*	• Provide guidance and template processes for information sharing • Support information sharing process on behalf of customers • Maintain a register of Information Sharing Agreements
10	*Information Governance Administration*	• Ensure customers are aware of mandatory registrations/returns and their deadlines • Provide Steering Group support for customer IG, with action reports and risks and issues provided to group management • Review and completion of annual "Register of Data Controllers"

Appendix A - Services specified under the GMSS Service Level Agreement Continued

11	*Records Management*	• Provide RM advice and guidance for both personal and corporate RM • Provide audits which will feed Information Asset Registers, annually • Audit RM for IG Toolkit requirements
12	*Compliance Support*	• Telephone IG support • On-Site IG Support • Provided via IG Officers • Support includes Data Protection Act, Regulation of Investigatory Powers Act, Computer Misuse, Information Commissioner Guidance and actions, DH guidance and actions.
13	*SIRO Support & Caldicott Guardian Support*	• Support SIRO & CG via phone and face-to-face for specific issues • Update SIRO & CG where risks or issues require
14	*Third Party Compliance Support*	• Provide audit assurances of third parties to client when requested • Provide oversight of contracts ensuring IG requirements are met for the contract type being awarded. • Support the drafting and management of Information Sharing Agreements.