NHS
Bury
Clinical Commissioning Group

Data Security and Protection Framework

Version:	7.0
Ratified by:	Information Governance Operational Group
Date ratified:	13 November 2019
Name of originator /author (s):	Senior IG Lead
Responsible Committee / individual:	Audit Committee
Date issued:	February 2020
Review date:	January 2021
Target audience:	NHS Bury Clinical Commissioning Group Members and Staff
Completed Equality Analysis:	Yes

Further information regarding this document

Document name	Data Security and Protection Framework CCG.GOV.024.7.0 Superseded Information Governance Framework
Category of Document in The Policy Schedule	Governance
Author(s) Contact(s) for further information about this document	Senior IG lead
This document should be read in conjunction with	Information Governance Policy; Confidentiality 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

Version History:		
Version Number	Reviewing Committee / Officer	Date
5.1 = draft revision	GMSS IG Team	26th June 2018
6.0 = ratified	NHS Bury Clinical Commissioning Group	20th July 2018
6.1 = draft revision	IGOG considered Policy	November 2019
7.0 = Approved	NHS Bury CCG – Full Data Security and Protection update. Renamed DS&P Framework (this replaces Information Governance Framework). Updated with IG in house and in line with GDPR to include DPO	February 2020

Contents

1. Introduction

The Data Security and Protection document aims to capture NHS Bury CCG’s approach to Information Governance (IG) and 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 the suit of Data Security and Protection policies. 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 and Data Security and Protection agenda and adapted appropriately to the capacity and capability of the organisation.

This Data Security and Protection framework must be read in conjunction with the CCGs Data Security and Protection Suite of Policies and Procedures which includes but is not restricted to:

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

Other legislation that relates to Data Security and Protection include:

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 Data Security and Protection. The organisation will achieve compliance by:

- Establishing, implementing and maintaining local CCG policies for the effective management of the data it processes;
- 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 DS&P 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 – Geoff Little

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 GDPR introduces a legal duty to appoint a Data Protection Officer (DPO) for all public authorities and in organisations that carry out certain types of processing activities.

DPOs assist to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments, (DPIAs) and act as a contact point for data subjects and the supervisory authority (ICO).

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

The Trust's DPO will help demonstrate compliance and is part of the enhanced focus on accountability within the Trust.

3.3. Senior Information Risk Owner (SIRO) – Mike Woodhead, Chief Finance Officer

The SIRO is responsible for identifying and managing the information risks to the CCG. This includes:

- Implementing information risk via the Information Asset Management and wider Trust Risk Management Policy.
- Reviewing and agree action in respect of identified information risks.
- Ensuring that the Trust's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Providing a focal point for the resolution and/or discussion of information risk issues.

3.4. Caldicott Guardian – Jeff Schryer, CCG Chair and General Practitioner

The Caldicott Guardian will act as an advocate for information sharing on the Board and in internal discussions. Key tasks will include:

- Ensuring that the Trust and its partner organisations satisfy the highest practical standards for handling patient information.
- Acting as the 'conscience' of the Trust in relation to information sharing.
- Supporting work to enable information sharing where it is appropriate to share.
- Advising on options for lawful and ethical processing of information.

3.5. Senior Information Governance Lead – Deborah Tonkin

The Chief Finance Officer has delegated day to day DS&P and IG responsibility to the Senior IG lead.

Senior Information Governance Lead

They are accountable for ensuring effective management, accountability, compliance and assurance for all aspects of Data Security and Protection and IG. Key tasks will include:

- Developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities.
- Ensuring that there is top level awareness and support for IG along with DS&P resourcing and implementation of improvements.
- Providing support for the SIRO, CG and DPO roles.
- Providing direction in formulating, establishing and promoting IG policies.
- Establishing working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives.
- Ensuring annual assessments and audits of the Data Security and protection policies and arrangements are carried out, documented and reported.
- Ensuring that the annual DS&P assessment and improvement plans are prepared for approval by the senior level of management, i.e. Information Governance Steering Group.
- 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 as necessary to support their duties.

- 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 IG issues.

3.6 Cyber Security Lead – Chief Technology Officer,

Bury CCG outsources its IT to the Manchester CSU.

The Cyber Security Lead will be responsible for ensuring the CSU meet the required IG assurance for the CCG, this includes:

- Ensuring compliance with the information security and cyber security components of the DS&P toolkit, contributing to the annual IG assessment.
- Advising in the development of a Network Security policy and controls for the secure operation of ICT networks, including remote/teleworking facilities.
- Providing advice and guidance regarding the implementation of IG security standards and controls to mitigate against malicious or unauthorised mobile code.
- Assisting in designing and configuring access controls for key systems.

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;
- Co-ordinating and monitoring the IG Policy across the organisation;
- Making recommendations on the necessary resourcing to support requirements;
- Addressing all issues surrounding the information management and information security that may affect the CCG;
- Identifying and approve all necessary staff information and training as outlined in the Data Security and Protection Toolkit;
- Ensuring 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 Senior IG Lead 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 Policy;
- 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, management and cyber security.

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

The CCG will ensure that the IG team appropriately training and received updated training as required.

Please referrer to the TNA document for all other staff member training needs such as new starters, agency etc

6. Information Governance Incident Management

The CCG uses the incident management tool Datix. 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.

The IG lead will review IG incidents to ensure they are scored and classified in accordance with the NHS Digital "Guide to the Notification of Data Security and Protection Incidents" (May 2018) and recommend actions to be carried out.

Incidents will be assessed following the ‘Breach Assessment Grid’ in appendix 1.

Any breaches other than "green breaches" are reportable using the Data Security and Protection Toolkit. Once reported on the tool it will automatically inform the ICO.

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.

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.

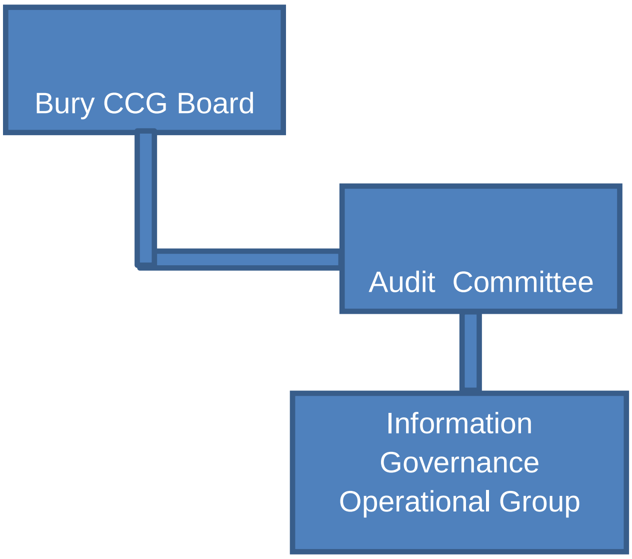
Reportable incidents must be reported to the ICO within 72 hours. This 72 hours starts when the CCG becomes aware of the breach which may not necessarily be when it occurred. Where the 72 hours deadline is not met an organisation must provide an explanation. Failure to notify promptly may result in additional 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 Operational Group. Minutes from the IGOG are received by the Audit Committee ensuring they are kept abreast of any approval activity.



Appendix 1 – IG incident scoring and reporting matrix

Severity (Impact)	Catastrophic	5	5	10	15	20	25
	Serious	4	4	8	12	16	20
	Adverse	3	3	6	9	12	15
	Minor	2	2	4	6	8	10
	No adverse effect	1	1	2	3	4	5
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood that citizens' rights have been affected (harm)				

Red – notified to DHSC and ICO

Yellow – Notified to ICO