NHS

Bristol, North Somerset
and South Gloucestershire
Clinical Commissioning Group

Information Governance Management Framework and Strategy

Shaping better health

Please complete the table below: *To be added by corporate team once policy approved and before placing on website*	
Policy ref no:	
Responsible Executive Director:	Sarah Truelove
Author and Job Title:	IG Team, SCW
Date Approved:	22 September 2020
Approved by:	*Sarah Truelove / IGG*
Date of next review:	September 2022

Version Control ***please remove this box once approved and finalised***		
Version	**Date**	**Consultation**
0.1 (1.0)	14-09-2018	New policy to align to GDPR
1.1	September 2020	Review

Contents

Information Governance Management Framework and Strategy

1. Introduction

This framework sets out the approach taken by Bristol, North Somerset and South Gloucestershire Clinical Commissioning Group (BNSSG CCG) for embedding information governance and details the continuous improvements that the CCG is working towards. The organisation must have a robust information governance management framework and strategy to provide the clarity and context for its information governance activities.

The framework identifies how the CCG will deliver its strategic information governance responsibilities by identifying the accountability structure, processes, interrelated policies, procedures, improvement plans, reporting hierarchy and training within the CCG. The CCG will also ensure that the future management and protection of organisational information is in compliance with legislative and government process and procedure including the National Data Guardian's 10 Data Security Standards.

1.1. BNSSG CCG Values

This information governance management framework and strategy document is aligned with CCG values, in particular:
We act with integrity – compliance with Data Protection Legislation requires the CCG to be open and transparent in our use of personal information this supports the creation of a culture of trust and respect.
We do the right thing – this Framework and Strategy supports the CCG's legal compliance and aims to ensure that all activities are aligned to Data Protection legislation.

2. Purpose and scope

This document applies to all directly and indirectly employed staff within the CCG and other persons working within or on behalf of the organisation. This document applies to all third party contractors or those with similar relationships through their contractual agreement to carry out activities on behalf of the CCG.

'Information governance' describes the approach taken within which information standards are developed, implemented and maintained by the CCG. Information governance ensures best practice is applied, in particular to all information relating to the organisation and individuals.

Information governance management ensures that data is sourced, held and used legally, securely, efficiently and effectively, in order to deliver the best possible care and services in compliance with legislation and advice received from bodies including NHS Digital. Information is a vital asset to the organisation supporting the effective management of commissioned services and resources. Therefore it is essential that all organisational information be managed effectively within a robust information governance management framework.

The organisation requires accurate, timely and relevant information to enable it to commission the highest quality healthcare and to operate effectively and meet its objectives. It is the responsibility of all staff to ensure that information is accurate and current and is used proactively in the conduct of its business. Accurate information that is dependable plays a key role in both corporate and clinical governance, strategic risk, performance management and service planning.

The implementation of this framework will lead to improvements in information handling underpinned by clear standards. The CCG will be able to ensure that all employees manage personal information in compliance with NHS Digital regulations for governance.

Staff will be aware that their records will not be disclosed inappropriately, which will lead to greater confidence in NHS working practices.

The information governance framework should be seen as a tool that will aid the CCG in preparation for embedding a ‘robust governance framework’. Information governance contributes to other standards by ensuring that data required for supporting decisions, processes and procedures are accurate, available and endures.

This framework is augmented by other related documents including those listed in Section 8 below.

3. Duties and responsibilities

3.1 Chief Executive

The Chief Executive has overall responsibility for compliance with information governance legislation and best practices, and the requirements within the ‘Data Security and Protection Toolkit’ (DSPT). The Chief Executive is responsible for the overall management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Information governance is the key to supporting this within the organisation.

3.2 Senior Information Risk Owner (SIRO) - Deputy CEO and Chief Finance Officer

The SIRO is a member of the Executive Management Team, chairs the Information Governance Group and is accountable to the Governing Body for the use of information and will ensure that the organisation conducts its business in an open, honest and secure manner, updating the board in respect to the annual report, the statement of internal controls and any changes in the law or potential risks. The SIRO is supported by the Caldicott Guardian, the Data Protection Officer, IG Manager (SCW) and the Information Asset Owners (IAO’s).

3.3. The Caldicott Guardian - Medical Director (Primary Care and Commissioning)

The Caldicott Guardian is a member of the Executive Management Team and a senior health or social care professional with responsibility for promoting clinical governance or equivalent functions. The Caldicott Guardian acting as the conscience of the organisation plays a key role in ensuring that the CCG satisfies the highest practical standards for handling patient/staff identifiable information. The Caldicott Guardian serves as part of a broader Caldicott function and is supported by the Data Protection Officer.

3.4. Data Protection Officer

The Data Protection Officer (DPO) should report directly to the Board in matters relating to data protection assurance and compliance, without prior oversight by their line manager.

The DPO must ensure that their responsibilities are not influenced in any way, and should a potential conflict of interest arise report this to the highest management level.

The DPOs cannot hold a position within the organisation that can be considered a key decision maker in relation to what personal data is collected and used. Their primary duties are to

- Inform and advise organisation and staff of their IG responsibilities
- Monitor compliance with the GDPR and the DPA 2018
- Provide advice where requested regarding the Data Protection Impact Assessment, and monitor performance
- Cooperate with the supervisory authority
- Be the principle contact point with the Information Commissioners Office – in particular for incidents
- Ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects that the ICO is informed no later than 72 hours after the organisation becomes aware of the incident

They must give due regard to the risks associated with the processing of data undertaken by the organisation and work with the SIRO and Caldicott Guardian to achieve this.

3.5. Information Asset owners (IAO's)

Within the CCG, IAO's are senior members of staff who are owners of one or more identified information assets of the organisation. There are IAO's working in a variety of senior roles to support the SIRO by risk assessing their assets in order to:

- Provide assurance to the SIRO on the security and use of these assets through contribution to an annual report
- Understand and address risks to the information assets they 'own'.

3.6. Information Asset Administrators (IAAs)

IAAs serve as local records managers and are responsible for assisting in the co-ordination of all aspects of information governance requests in the execution of their duties, which include:

- provide support to their IAO
- ensure that policies and procedures are followed locally
- recognise potential or actual IG security incidents
- undertake relevant IG audit tasks

- consult their IAO on incident management
- ensure that information asset registers are accurate and maintained up to date.

3.7. SCW Information Governance Service

SCW provides IG support services in line with the information governance service specification under any Service Level Agreement for IG Service.

3.8. The BNSSG Information Governance Group (IGG)

The Information Governance Group (IGG) oversees and provides leadership within BNSSG CCG for Information Governance (IG), ensuring that it complies with statutory responsibilities and fulfils the requirements of data protection legislation, the common law duty of confidentiality and The Records Management Code of Practice for Health and Social Care 2016.

IGG is responsible:

- To provide a forum for the scrutiny of the IG management framework and assurance model.
- To oversee the annual IG assessment.
- To agree and oversee the organisation’s IG improvement programme.
- To ensure that the organisation’s approach to IG is communicated to all staff and made available to the public as appropriate.
- To offer support, advice and guidance to the Caldicott Function and Data Protection programme within the organisation.
- To monitor the organisation’s information handling activities to ensure compliance with law and guidance
- To ensure that training made available by the organisation is taken up by staff as necessary to support their role.
- To ensure that Corporate records management standards are developed and implemented within the organisation.
- Provide a focal point for the resolution and/or discussion of IG issues.
- Review the flows of information to ensure they are appropriate and supported by relevant documentation especially those involving any transfer of personal data.
- To ensure that all new developments undertake statutorily required Data Protection Impact Assessments (DPIAs) to assess IG implications where required.
- To ensure that Continuity plans for services include appropriate reference to information assets and continuity/recovery activities
- To support the work of the SIRO and Caldicott Guardian (CG), Information Asset Owners (IAO) and Information Asset Administrators (IAA).
- To review all information and information security incidents.

- Review information and information security risks/issues and to escalate where appropriate within the organisation and with customers.
- To ensure a comprehensive suite of IG policies is in place

A quarterly IG report shall be presented to the IGG. Audit Committee will receive annual updates on-progress, information governance audits, training and toolkit evidence requirements, together with updates on any incidents that may have occurred.

The annual audit of information governance shall be reported to the Audit Committee via IGG together with any recommendations identified and the associated improvement plans.

3.9. The BNSSG IAO/IAA Group

The Information Asset Owners and Information Asset Administrators Group has been established to enable the IAO's and IAA's to receive vital information in order to assist in the implementation and assure compliance with the Information Governance (IG) agenda for the CCG.

It is chaired by the SIRO and provides a forum to enable a pro-active environment for the exchange of information. It will provide a platform to debate and discuss areas of concern where difficulties are experienced requiring mitigation, and to exchange good practice.

4. Definitions of terms used

In order to assist staff with understanding their responsibilities under this strategy, the following types of information and their definitions are applicable in all CCG policies and documents:

Personal Data (derived from the GDPR)	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
'Special Categories' of Personal Data (derived from the GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data (f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition (h) Their sexual life
Personal Confidential	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about

Data	identified or identifiable individuals, which should be kept private or secret. The definition includes dead as well as living people and 'confidential' includes information 'given in confidence' and 'that which is owed a duty of confidence'. The term is used in the Caldicott 2 Review: Information: to share or not to share (published March 2013).
Commercially confidential Information	Business/Commercial information, including that subject to statutory or regulatory obligations, which may be damaging to SCW CSU or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

5. Information Governance Principles

Implementation of robust information governance arrangements will deliver improvements in information handling by following the Department of Health standards (known as the 'HORUS' model), these standards require that information will be:

Held securely and confidentially
Obtained fairly and efficiently
Recorded accurately and reliably
Used effectively and ethically
Shared appropriately and lawfully

Information governance provides consistency and best practice for the many different information handling activities. These principles are equally supported by the Caldicott Principles which have been subsumed into the NHS Code of Confidentiality.

There are five interlinked principles, which serve to guide these information governance responsibilities:

- Openness
- Legal compliance
- Information security
- Quality assurance
- Proactive use of information

6. Training requirements

It is the responsibility of the CCG to ensure that all new staff are provided with information governance, information security, freedom of information and records management training as part of their induction. A Data Security Awareness and Information Governance Handbook is shared with shared as part of the induction process. Induction training is to be completed within 1 month of joining the organisation. All new staff as part of their induction must use ConsultOD to access their NHS Digital Data Security and Awareness training. Refresher training will/must be completed through the above tool or where appropriate and agreed via 'Face to Face' training provided by the IG Team on an annual basis.

The CCG, through its learning and development commitment ensures that appropriate annual training is made available to staff and completed as necessary to support their duties.

In addition to the annual mandatory training all IAOs, IAAs, the DPO, the Caldicott Guardian and SIRO are required to have undertaken all of their additional training associated with their identified framework roles.

Supporting People

Fundamental to the success of delivering the information governance strategy is developing a robust information governance culture within the CCG. In order to promote this culture, training needs to be relevant and embedded in working practices. Through the provision of IG services by SCW the IG manager is actively involved in this development through the provision of assistance on specific projects and issues, investigations and the development of remedial action plans and the ongoing provision of relevant information and reminders.

Following a SIRI further training may be delivered as a mandatory requirement where an incident has occurred, as deemed appropriate as part of the investigation findings. Disciplinary procedures may be used where it is proven that an employee has acted in breach of the terms of their contract; acts of gross misconduct will lead to dismissal.

7. Monitoring compliance and effectiveness

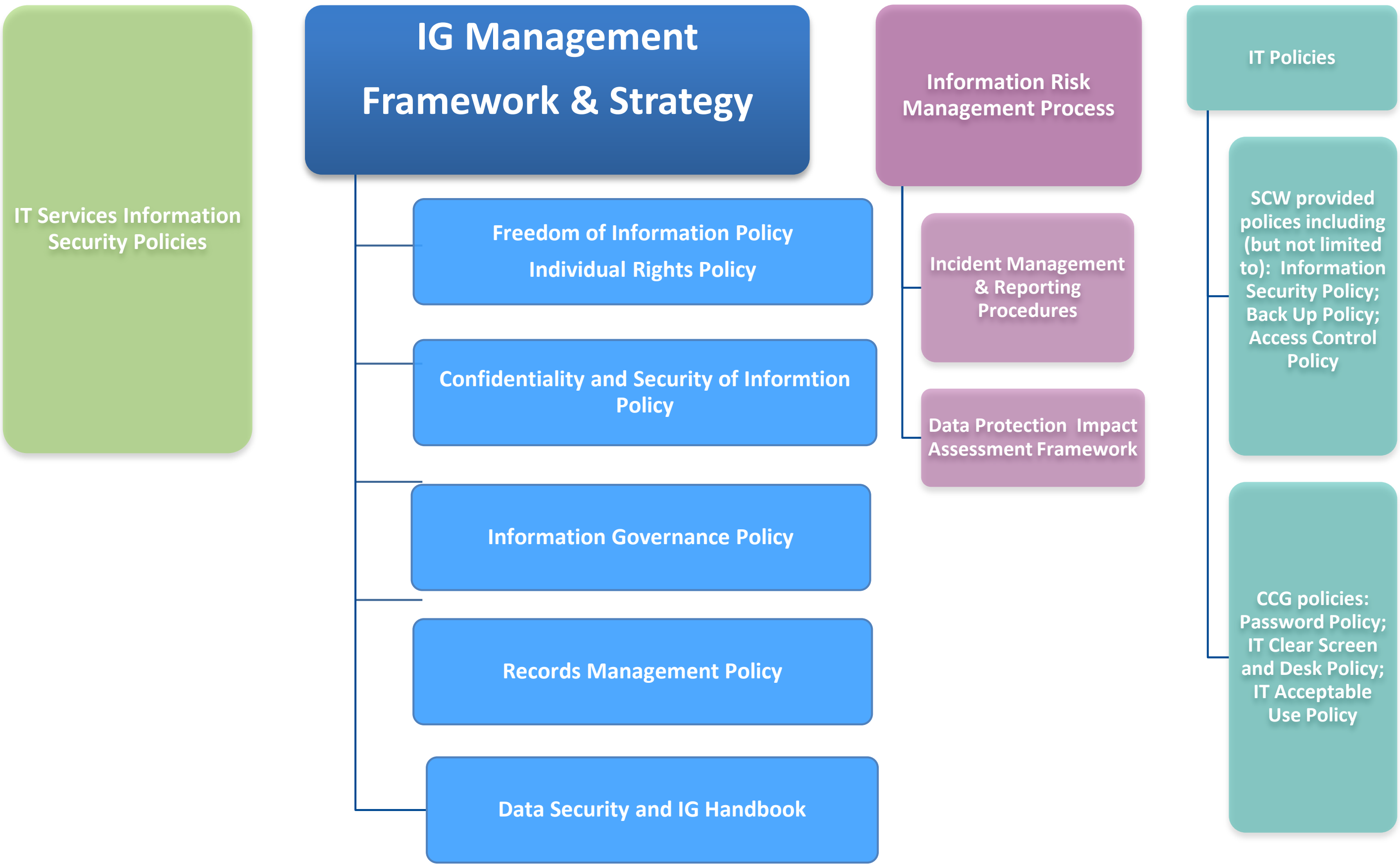
The performance of the strategy will be monitored in two ways:

- Against the criteria set in the Data Security and Protection Toolkit, using the annual submission on 31 March and associated improvement plan.
- The internal audit process and subsequent report to the audit committee.

8. References, acknowledgements and associated documents

This management framework and strategy links to other strategies, policies, procedures and legislation/codes of practice (See Appendix 13.3) that are in place within the CCG to promote and ensure the delivery of information governance standards throughout the organisation, including but not limited to those documents listed below.

Image: IG management framework: strategies, policies and procedures



IT Services Information Security Policies

IG Management Framework & Strategy

Freedom of Information Policy

Individual Rights Policy

Confidentiality and Security of Informtion Policy

Information Governance Policy

Records Management Policy

Data Security and IG Handbook

Information Risk Management Process

Incident Management & Reporting Procedures

Data Protection Impact Assessment Framework

IT Policies

SCW provided polices including (but not limited to): Information Security Policy; Back Up Policy; Access Control Policy

CCG policies: Password Policy; IT Clear Screen and Desk Policy; IT Acceptable Use Policy

9. Appendices

9.1. Legislation

All staff are required to comply with Data Protection Legislation. This includes

- the General Data Protection Regulation (GDPR),
- the Data Protection Act (DPA) 2018,
- the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time

In addition, consideration will also be given to all applicable Law concerning privacy confidentiality, the processing and sharing of personal data including

- the Human Rights Act 1998,
- the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015,
- the common law duty of confidentiality and
- the Privacy and Electronic Communications (EC Directive) Regulations

Consideration must also be given to the

- Computer Misuse Act 1990 and as amended by the Police and Justice Act 2006 (Computer Misuse)
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Other relevant Health and Social Care Acts
- Access to Health Records Act 1990
- Fraud Act 2006
- Bribery Act 2010
- Criminal Justice and Immigration Act 2008
- Equality Act 2010
- Terrorism Act 2006
- Malicious Communications Act 1988
- Counter-Terrorism and Security Act 2015
- Digital Economy Act 2010 and 2017

GUIDANCE

- ICO Guidance
- CQC Code of Practice on Confidential Information
- NHS Digital looking after your information
- Dept. of Health and Social Care 2017/18 Data Security and Protection Requirements

- NHS England Confidentiality Policy
- Records management: Code of Practice for Health & Social care
- Confidentiality: NHS Code of Practice - Publications - Inside Government - GOV.UK
- Confidentiality: NHS Code of Practice - supplementary guidance
- CCTV