BNSSG CCG Governing Body Meeting

Date: Tuesday 5th February 2019
Time: 1.30pm
Location: The Royal Hotel, 1 South Parade, Weston-super-Mare BS23 1JP

Agenda number: 9.3

Report title: Information Governance Management Framework & Strategy

Report Author: Caroline Dominey-Strange
Report Sponsor: Sarah Truelove

1. Purpose

To obtain approval of the Information Governance Policy and the Confidentiality and Security of Information Policy which outline Bristol, North Somerset and South Gloucestershire Clinical Commissioning Group's (BNSSG CCG) strategy with regard to Information Governance.

2. Recommendations

The Governing Body is asked to approve the Information Governance Management Framework and Strategy

3. Executive Summary

This framework and strategy sets out the approach taken within 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.

4. Financial resource implications

There are no financial resource implications to this. However, failure to comply with relevant Data Protection legislation can result in significant fines to the organisation.

5. Legal implications

The framework and strategy support the CCGs compliance with General Data Protection Regulation (GDPR) and Data Protection Act 2018.

6. Risk implications

If an appropriate Information Governance framework and strategy is not adopted or implemented there is a risk of non-compliance with data protection legislation resulting is damage to individuals privacy, breach of confidentiality and potential action (including significant fines) against the organisation.

7. Implications for health inequalities

There are no implications for health inequalities.

8. Implications for equalities (Black and Other Minority Ethnic/Disability/Age Issues)

The Equality Impact Screening Assessment has deemed that a full Assessment is not required.

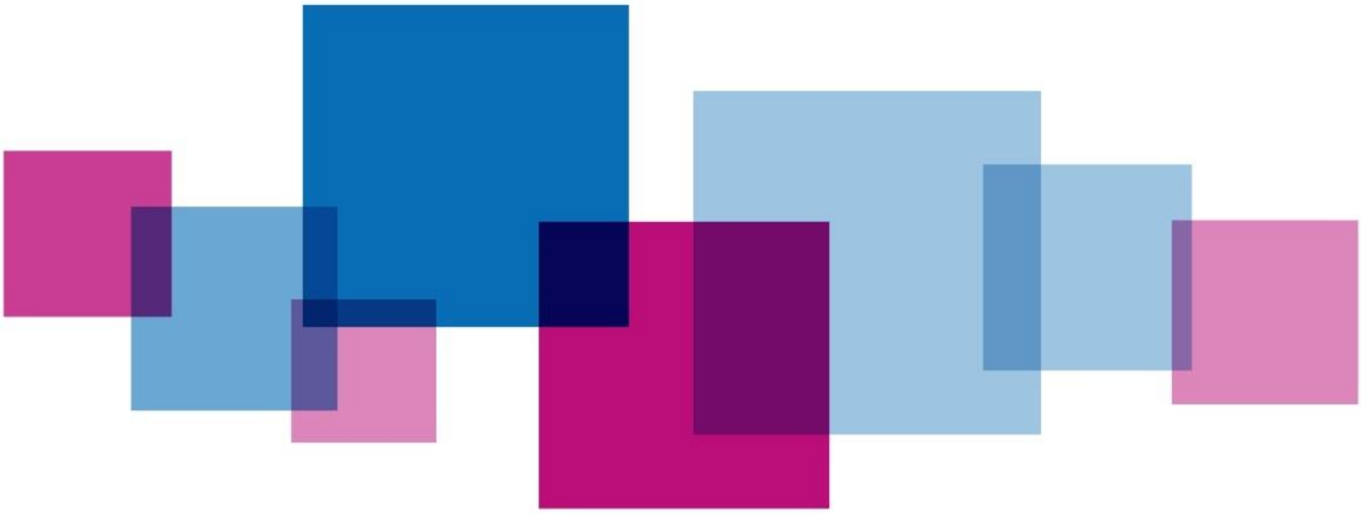
9. Implications for Public Involvement

There has been no public involvement in the creation of this framework and strategy which is aimed at ensuring data protection legislation is reflected in CCG policy.

NHS
Bristol, North Somerset
and South Gloucestershire
Clinical Commissioning Group

70
YEARS
OF THE NHS
1948 - 2018

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:	
Approved by:	
Date of next review:	September 2020

	Yes/No/NA	**Supporting information**
Has an Equality Impact Assessment Screening been completed?	Yes	
Has the review taken account of latest Guidance/Legislation?	Yes	
Has legal advice been sought?	No	Policy provided by SCW IG Team
Has HR been consulted?	Yes	via Policy Review Group
Have training issues been addressed?	Yes	
Are there other HR related issues that need to be considered?	No	
Has the policy been reviewed by JCC?	No	
Are there financial issues and have they been addressed?	No	
What engagement has there been with patients/members of the public in preparing this policy?	N/A	
Are there linked policies and procedures?	Yes	
Has the lead Executive Director approved the policy?	Yes	Sarah Truelove to approve after Policy Review Group
Which Committees have assured the policy?		Policy Review Group
Has an implementation plan been provided?	Yes	Attached
How will the policy be shared with: • Staff? • Patients? • Public?		Strategy will be available via the organisation's website
Will an audit trail demonstrating receipt of policy by staff be required; how will this be done?	No	

Version Control ***please remove this box once approved and finalised***		
Version	**Date**	**Consultation**
0.1	14-09-2018	New policy to align to GDPR

Contents

Information Governance Management Framework and Strategy

1. Introduction

This framework sets out the approach taken within 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.

This information governance management framework and strategy document is aligned with CCG objectives to support the delivery of the CCG operating and strategic plan.

Implementation Objectives

To develop information quality assurance standards in alignment with the content of this framework to support:

- Corporate governance (which ensures organisations achieve their business objectives and meet integrity and accountability standards)
- Clinical governance (ensuring continuous improvements in the quality of healthcare)
- Research governance (which ensures compliance with ethical standards).

The strategic 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.

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 with 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 management framework and strategy will be reviewed annually. Developments will be scheduled via a work plan inclusive of an implementation timetable.

3. Duties and responsibilities

3.1. Chief Executive

The Chief Executive is the ‘information governance lead’ and has overall responsibility for compliance with information governance legislation and best practices, and the requirements within the ‘information governance toolkit’ (IGT). 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)

The SIRO is a member of the Executive Management Team 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 and the Information Asset Owners (IAO’s).

3.3. The Caldicott Guardian

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 IGG is in place to ensure effective management, accountability, and IG resources within each service line in order to improve compliance in all aspects of IG within the CCG structure including:

- Developing, providing direction and maintaining IG corporate policies and guidance
- Providing support to the key roles identified in the IG management structure
- Ensuring board awareness of IG resourcing requirements and implementation of improvements
- Establishing coordinated working groups for the information asset owners and Information Asset Administrators
- Ensuring annual assessments and audits and policy reviews are undertaken where required
- Ensuring the annual assessment and associated improvement plans are prepared for approval by the board as required
- Ensuring that the CCG is in line with the mandatory training requirements of its staff as stated within the Data Security and Protection Toolkit
- Receiving outcomes of investigations into IG Serious Incidents Requiring Investigation (SIRIs) and provide support and advice as necessary in any internal or external investigation, and to make recommendations of actions to be taken to prevent a repeat of a similar incident.

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 SCW 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	‘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

Data (derived from the GDPR)	(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 Data	Personal and Special Categories of Personal Data owed a duty of confidentiality (under the common law). This term describes personal information about 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. Reporting

A quarterly IG report shall be presented to the IGG.

IGG will identify and allocate any associated resource implications incurred by the implementation of the information governance framework, policy and improvement plan.

Audit Committee will receive annual updates on–progress when required with 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.

6. The Information Governance Action Plan/Improvement Programme

Risks and issues will be identified where they may impact upon delivery of the IG action plan.

The IG action plan is a standing item on IGG agenda and is an evolving working document. Any risks and issues identified that may impede delivery of the plan will require decisions are reached to assure a managed approach to delivery of the plan is implemented effectively. The plan is available upon request from the IG Manager.

7. Information Governance Principles

As a commissioner the CCG carries clear responsibilities for handling and protecting information of many types in many differing formats.

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 is a framework to provide consistency and best practice for the many different information handling requests and associated guidance. 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

8. 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. An Information Governance Handbook is shared with shared as part of the inductions process. Induction training is to be completed within 1 month of joining the organisation.

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.

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.

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.

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.

9. Equality Impact Assessment

An Equality Impact Analysis (EIA) screening has been completed. No adverse impact or other significant issues were found. A copy of the EIA screening is attached at Appendix 13.1.

10. 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.

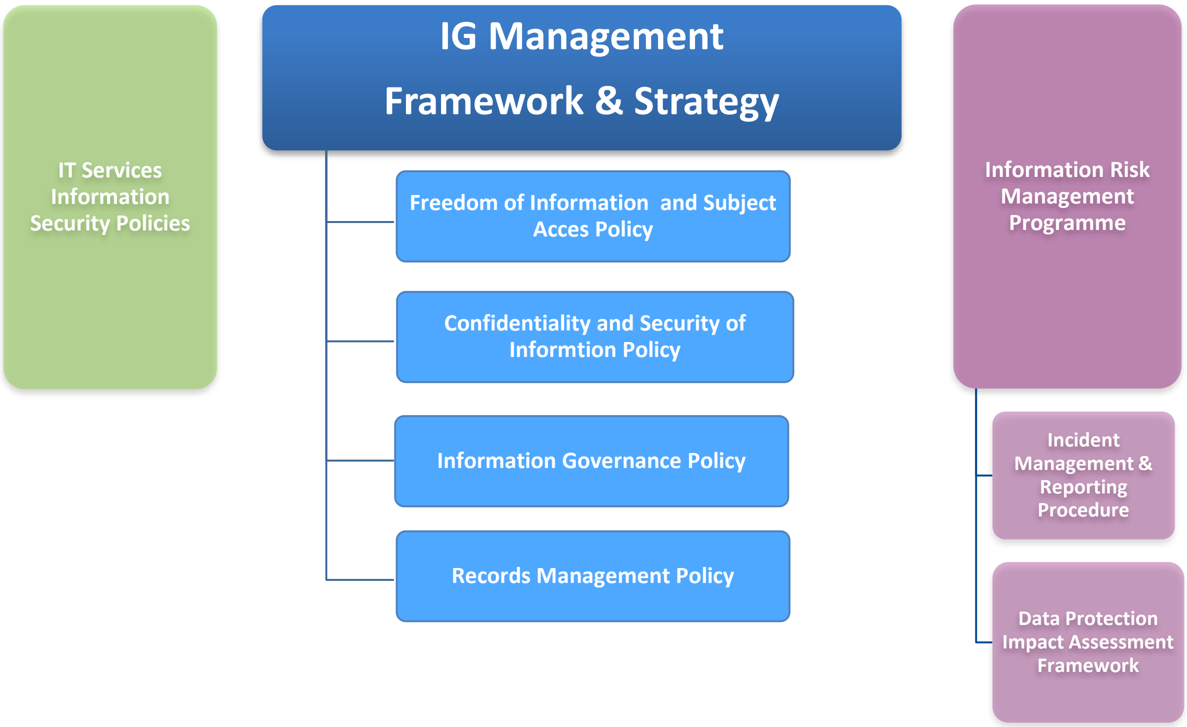
11. Countering Fraud

The CCG is committed to reducing fraud in the NHS to a minimum, keeping it at that level and putting funds stolen through fraud back into patient care. Therefore, we have given consideration to fraud and corruption that may occur in this area and our responses to these acts during the development of this policy document.

12. References, acknowledgements and associated documents

This management framework and strategy links to other strategies, policies, procedures and legislation (See Appendix 13.3) codes of practice 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, procedures and legislation



IG Management Framework & Strategy

IT Services Information Security Policies

Freedom of Information and Subject Acces Policy

Confidentiality and Security of Informtion Policy

Information Governance Policy

Records Management Policy

Information Risk Management Programme

Incident Management & Reporting Procedure

Data Protection Impact Assessment Framework

13. Appendices

13.1. Equality Impact Assessment

Equality Impact Assessment Screening		
Query	**Response**	
What is the aim of the document?	This Strategy sets out the approach taken within 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.	
Who is the target audience of the document (which staff groups)?	All staff	
Who is it likely to impact on and how?	Staff	Yes – impacts how the CCG will manage personal information of staff
	Patients	Yes – impacts how the CCG will manage personal information of patients
	Visitors	Yes – impacts how the CCG will manage personal information of all individuals
	Carers	Yes – impacts how the CCG will manage personal information of all individuals
	Other – governors, volunteers etc	Yes – impacts how the CCG will manage personal information of all individuals
Does the document affect one group more or less favourably than another based on the 'protected characteristics' in the Equality Act 2010:	Age (younger and older people)	No – the policy ensures legal compliance and treat all individuals' data in the same way.
	Disability (includes physical and sensory impairments, learning disabilities, mental health)	No – see above
	Gender (men or women)	No – see above
	Pregnancy and maternity	No – see above
	Race (includes ethnicity as well as gypsy travellers)	No – see above

	Sexual Orientation (lesbian, gay and bisexual people)	No – see above
	Transgender people	No – see above
	Groups at risk of stigma or social exclusion (e.g. offenders, homeless people)	No – see above
	Human Rights (particularly rights to privacy, dignity, liberty and non-degrading treatment)	No – see above

13.2. Implementation plan

Target Group	Implementation or Training objective	Method	Lead	Target start date	Target End date	Resources Required
Staff	To have Strategy available to all staff	To be published on the Hub	Comms/IG	31/07/2018	30/09/2018	Comms team
Staff	To ensure all staff are aware of the policy	To include summary of highlights in The Voice	Comms/IG	31/07/2018	30/09/2018	Comms team

13.3. 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