NHS
Frimley
Clinical Commissioning Group

FRIMLEY
CLINICAL COMMISSIONING GROUP

Information Governance Management Framework and Strategy Policy

Policy number	[Tbc by Governance team]
Version	Version 1.0
Approved by	Audit Committee in Common
Document Author	South Central West CSU
Date of approval	17 March 2021
Next due for review	1 April 2023

Version	Date	Author	Status	Comment
1.0	16/2/2021	SCW CSU	Draft	Version adapted from East Berkshire CCG version

Equality Statement

Frimley Clinical Commissioning Group (CCG) aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others.

Throughout the development of the policies and processes cited in this document, the CCG has:

- Given due regard to the need to eliminate discrimination, harassment and victimisation, to advance equality of opportunity, and to foster good relations between people who have shared a relevant protected characteristic (as cited under the Equality Act 2010) and those who do not share it;

- Given regard to the need to reduce inequalities between patients in access to, and outcomes from, healthcare services and in securing that services are provided in an integrated way where this might reduce health inequalities.

Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the member of staff has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

The CCG embraces the four staff pledges in the NHS Constitution. This policy is consistent with these pledges.

NHS
Frimley
Clinical Commissioning Group

Contents

1. Introduction

This framework sets out the approach taken within Frimley Clinical Commissioning Group, hereafter the 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 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 NHS Digital 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.

2. Scope and Definitions

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 and ensures best practice applies, 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 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.

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 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 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.

3. 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.

4. Reporting

A report shall be presented to the Audit Committee in Common each quarter or when requested.

The Audit Committee in Common group will receive quarterly updates on-progress with information governance audits, training and toolkit evidence requirements, together with updates on any incidents that may have occurred. The committee will also identify and allocate any associated resource implications incurred by the implementation of the information governance framework, policy and improvement plan.

5. The Information Governance Framework

Risks and issues will be identified where they may impact upon delivery against the IG Framework.

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

6. Accountability and Responsibilities

Clinical Chief Officer
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 Data Security & Protection toolkit. 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.

Senior information risk owner (SIRO)
The SIRO is a member of the Senior Leadership 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).

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.

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 contact point with the Information Commissioners Office
- ✓ 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.

Information asset owners (IAO's)
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'.

Data Custodians (DC's)
DCs 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.

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

The Information Governance Working Group (IGWG)
The IGWG 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 data custodians
- 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.

Audit Committee
The Audit Committee has oversight and accountability for Information Governance ensuring that the CCG complies with its statutory responsibilities and fulfils the requirements of administrative law, Data Protection Act 2018, General Data Protection Regulations, the Common Law Duty of Confidentiality and the Records Management Code of Practice for Health and Social Care 2016

7. Training

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 issued upon notification of a new starter; to ensure compliance a signature sheet is required to be returned to the information governance team. Induction training is to be completed within two weeks 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 training all IAOs, DCs, the DPO, the Caldicott Guardian and SIRO are required to have undertaken all of their additional training associated with their identified framework roles in the training matrix.

All new staff as part of their induction must complete Data Security Awareness training. Refresher training will/must be completed online by attending 'Face to Face' training provided by the IG Team (if applicable) on an annual basis.

8. 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. Public Sector Equality Duty- Equality Impact Assessment

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

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 Committees in Common

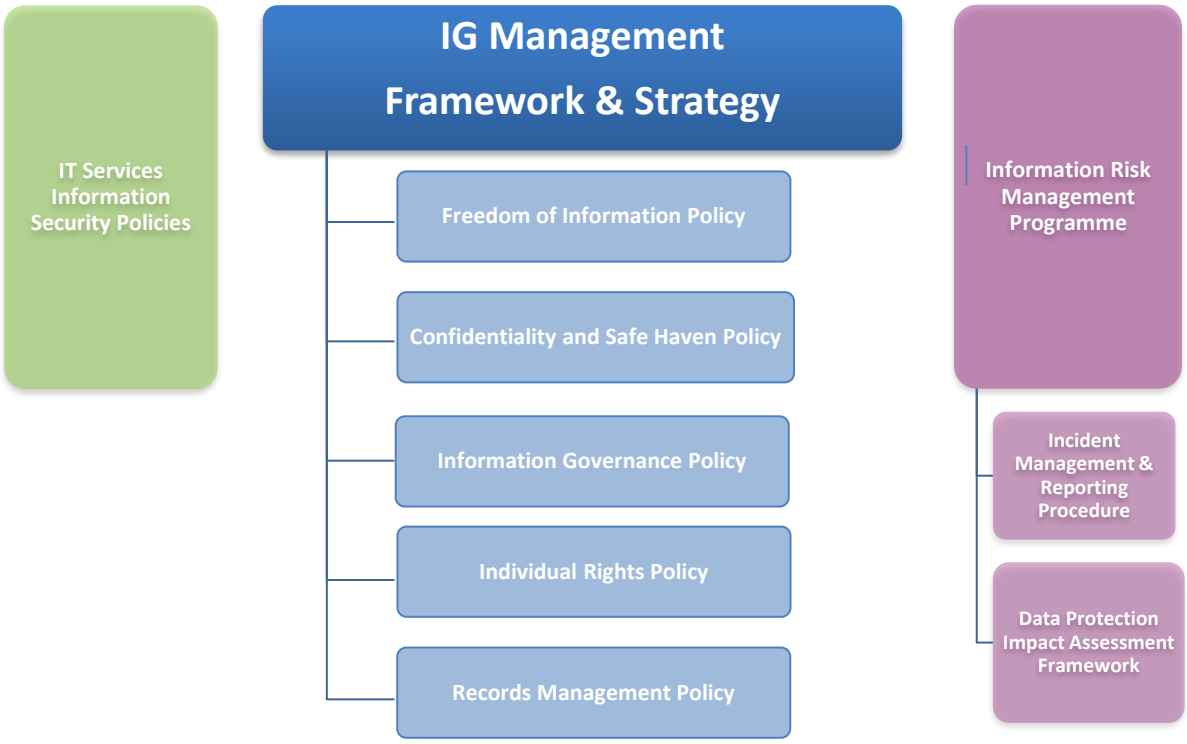
11. Review

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

12. Additional References and Associated Documents

This management framework and strategy links to other strategies, policies, procedures and codes of practice that are in place within the CCG to promote and ensure the delivery of information governance standards throughout the organisation and must be read in conjunction with those listed in Appendix A.

APPENDIX 1 - POLICIES AND PROCEDURES



Policies

Confidentiality and Safe Haven Policy
This document describes the CCG policy on data protection and confidentiality together with employees' responsibilities for the safeguarding of confidential information held both manually (non-computer in a structured filing system) and on computers. This policy also aims to ensure that the CCG operates procedures to safeguard the privacy and confidentiality of information by ensuring that information sent to or from the CCG is handled in such a way as to minimise the risk of inappropriate access or disclosure.

Information Governance Policy
Information is a vital asset, both in terms of the efficient management of services and resources in creating a corporate memory. Information plays a key part in all areas of governance, service planning and performance management.

Individual Rights Policy
This document details how the organisation will handle requests for personal information including health records for living persons (Subject Access Request), deceased persons (Access to Records) and staff records, as well as the other rights under the GDPR This policy will be accompanied by a standard operating procedure to support staff in processing such requests.

Records Management Policy
This policy is written to give the organisation clear information and records management framework, which includes advice and guidance on all aspects of records management and data quality to inform staff of their operational and legal responsibilities.

Information Security: IT Policies and documentation
SCW IT services provide and support the information systems and networks used by the CCG

IT-Services-Information Security Policy
All staff have a responsibility for information security. Therefore awareness and compliance of ALL staff is essential. This document describes the approach to information security and employees' responsibilities for security of information held both manually and on computers.

IT-Services-Anti-Virus Policy
This document contains the anti-virus policy details including actions to be taken if non-compliance occurs.

IT-Services-Access Control Policy
The objective of this policy is to prevent unauthorised access to information systems and networks. The policy describes how access controls are applied by the organisation, covering all stages in the life-cycle of user access, from the initial registration process of new users to the final de-registration of users who no longer require access to information systems and processes.

IT-Services-Asset Management Policy
The Asset Management Policy describes the aims and objectives of asset management. This policy draws from IT industry best practice using the ITIL framework, IT Asset Management (ITAM), the ISO Asset Management System ISO 55001, Controls Objectives in IT (COBIT 5), PRINCE 2.

IT-Services-Disposal Policy
This policy will focus on the disposal and destruction of all SCW hardware. It also provides the guiding principles to adhere to when disposing of or destroying other types of confidential or sensitive information assets.

IT-Services-Patch Management Policy
This policy provides the basis for an ongoing and consistent system and application update policy that stresses regular security updates and patches to operating systems, firmware, productivity applications, and utilities. Regular updates are critical to maintaining a secure operational environment.

IT-Services-Patch Management Policy
The purpose of this Policy is to define the objective, scope, value and basic rules for the ITS continuity management system (BCMS).

IT-Services-Password Policy
This policy describes how users of SCW supported systems should create and manage their passwords.

IT-Services-Clear Screen & Desk Policy
This policy defines how desks should be kept clear of sensitive printed material.

IT-Service-Acceptable Use Policy
The purpose of this policy is to ensure that users of SCW supported computer systems do so in a secure, lawful and responsible manner.

IT-Remote Working and Portable Devices Policy
The purpose of this policy is to protect information that is processed remotely or is stored on portable devices. It applies to all staff who are entrusted with a supplied portable computing and data storage device, or who use any other portable computing and data storage device not directly managed by the SCW IT providers, for purposes connected with the work of the organisation.

IT-System Level Security Policy
The aim of this policy is to assist with the development of system level security controls

IT-Network Security Policy
The aim of this policy is to ensure the security of the CSU network.

IT-Services: Backup & Business Continuity Policy
This document provides the policies that govern the design and operation of CSU information technology services to ensure adequate business continuity arrangements for the CSU and all customer organisations.

IT-Change Management Policy
The objective of the change management process is to ensure that all changes within systems supported by SCW CSU IT Services are assessed, implemented and reviewed in a controlled manner.

Registration Authority Policy
The SCW Registration Authority (RA) is responsible for verifying the identity of health care professionals and workers who wish to register to use National NHS services including GP clinical systems, pharmacy systems, Choose and Book, the electronic Prescription (EPOS), Secondary Use Service (SUS), Map of Medicine (MoM), Summary Care Record (SCR). This policy details the roles and responsibilities of the RA in issuing and monitoring the use of Smartcards to access these systems.

Supporting Guidance

The Information Risk Management Programme

The purpose of this document is to establish relevant lines of responsibility and conduct for all members of staff regarding information risk management. All information risks will be recorded, managed and escalated in accordance with the organisation's Risk Management Policy and Procedure.

On the identification of a potential risk, a discussion will be held to determine the likelihood, consequence and the treatment of the risk. Depending on the outcome of this assessment, the risk will be recorded and monitored.

Incident Management and Reporting Procedure
This procedure and documentation sets out the approach taken within the CCG for the management of information governance risk incidents.

Data Protection Impact Assessments
Article 35 of the General Data Protection Regulation 2016 (GDPR) requires that a Data Protection Impact Assessment (DPIA) is undertaken where there are 'high risks to the rights and freedoms of natural persons resulting from the processing of their personal data'.

The use of Privacy Impact Assessments has become common practice in the NHS and the GDPR identifies a number of situations where the processing could be considered high risk and where a DPIA is a legal requirement, including the use of special categories of personal data including sensitive data (health and social care).

Training Needs analysis
This identifies the various IG training requirements dependent on role.

Terms of Reference
Terms of reference are in place and updated on an annual basis for the following core groups with IG responsibilities:

- ✓ The Information Governance Steering Group
- ✓ The Information Governance Working Group
- ✓ The Audit Committee in Common

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

APPENDIX 2 - EQUALITY IMPACT ASSESSMENT

1.	**Title of policy/ programme/ framework/ strategy being analysed.**		
2.	**Please state the aims and objectives of the work and intended equality outcomes** *This policy forms part of the wider commitment across the NHS to be an employer of choice and recognises that there are significant advantages in terms of employee recruitment, motivation and retention, where flexible working arrangements are offered in conjunction with a commitment to service to patients.*		
3.	**Who is likely to be affected? Eg staff, patients, service users, carers**		
4.	**What evidence do you have of potential impact (positive and negative)**		
		Yes/No	**Comments**
1.	**Does the document/guidance affect one group less or more favourably than another on the basis of:**		
	• Race		
	• Ethnic origins (including gypsies and travellers)		
	• Nationality		
	• Gender		
	• Culture		
	• Religion or belief		
	• Sexual orientation including lesbian, gay and bisexual people		
	• Age		
	• Disability - learning disabilities, physical disability, sensory impairment and mental health problems		
2.	**Is there any evidence that some groups are affected differently?**		
3.	**If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?**		

4.	**Is the impact of the document/guidance likely to be negative?**		
5.	**If so, can the impact be avoided?**		
6.	**What alternative is there to achieving the document/guidance without the impact?**		
7.	**Can we reduce the impact by taking different action?**		

Who	Date of Assessments