NHS
Frimley
Clinical Commissioning Group

FRIMLEY
CLINICAL COMMISSIONING GROUP

Information Governance 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.

Contents

1. Introduction 5
2. Purpose 5
3. Legal Compliance 6
4. Scope and Definitions 7
5. Processes/Requirements 8
6. Information Security 9
7. Information Quality Assurance 9
8. Commissioning of New Services 10
9. Roles and Responsibilities 10
10. Training 13
11. Public Sector Equality Duty- Equality Impact Assessment 13
12. Monitoring Compliance And Effectiveness 13
13. Review 14
14. Additional References and Associated Codes of Practice 14
Appendix 2 - Equality Impact Assessment 15

1. Introduction

The role of NHS Frimley Clinical Commissioning Group, hereafter the CCG, is to support the commissioning of healthcare, both directly and indirectly, so that valuable public resources secure the best possible outcomes for patients. In doing so, the CCG will uphold the NHS Constitution. This policy is important because it will help the people who work for the CCG to understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients.

2. Purpose

Information is a vital asset. It plays a key part in ensuring the efficient management of service planning, resources and performance management. It is therefore of paramount importance to ensure that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management.

Information Governance looks at the way the NHS handles information about patients, staff, contractors and the healthcare provided, with particular consideration of personal and confidential information. Without access to information it would be impossible to provide quality healthcare and good corporate governance. A robust governance framework needs to be in place to manage this vital asset, providing a consistent way to deal with the many different information handling requirements including:

- Information Governance Management
- Confidentiality and Data Protection Legislation assurance
- Corporate Information assurance
- Information Security assurance
- Secondary Use assurance

The aims of this document are to maximise the value of organisational assets by ensuring that information is:

- Held securely and confidentially;
- Obtained fairly and efficiently;

- Recorded accurately and reliably;
- Used effectively and ethically;
- Shared appropriately and lawfully

To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental, the CCG will ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met
- Business continuity plans will be produced, maintained and tested
- Information security training will be available to all staff

3. Legal Compliance

The CCG regards all identifiable personal information as confidential except where national policy on accountability and openness requires otherwise.

The CCG will maintain policies to ensure compliance with Data Protection Legislation. This includes the General Data Protection Regulations (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.

The CCG, when acting as a Controller, will identify and record a condition for processing, as identified by the GDPR under Articles 6 and 9 (where appropriate), for each activity it undertakes. When relying on Article 6, 1 (e) ' processing is necessary for the performance of a task carried out in the public interest or in the

exercise of official authority vested in the Controller', the CCG will identify the official authority (legal basis) and record this on relevant records of processing.

4. Scope and Definitions

The scope of this document covers

- All permanent employees of the CCG and;
- Staff working on behalf of the CCG (this includes contractors, temporary staff and secondees).

The CCG recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The CCG fully supports the principles of corporate governance and recognises its public accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard information. The CCG also recognises the need to share information in a controlled manner. The CCG believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of managers and staff to ensure and promote the quality of information and to actively use information in decision making processes.

In order to assist staff with understanding their responsibilities under this policy, the following types of information and their definitions are applicable in all relevant 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	'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

(derived from the GDPR)	(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. Processes/Requirements

The CCG will ensure that it meets its national requirements in respect of its submission of the annual self-assessment Data Security and Protection Toolkit (DSPT).

Non-confidential information about the CCG and its services will be available to the public through a variety of media.

The CCG will maintain policies to ensure compliance with the Freedom of Information Act. Please refer to the Freedom of Information Policy.

The CCG will have clear procedures and arrangements for liaison with the press and broadcasting media. Please refer to the Communications Strategy**.**

The CCG will maintain clear procedures and arrangements for handling requests for information from the public. Please refer to The CCG Individual Rights Policy in accordance with the General Data Protection Regulations (GDPR) and the Data Protection Act (DPA) 2018.

The CCG will maintain policies to ensure compliance with the Records Management Code of Practice for Health and Social Care (2016). Please refer to The CCG Records Management Policy.

6. Information Security

The CCG will maintain policies for the effective and secure management of its information assets and resources.

The CCG will promote effective confidentiality and security practice to its staff through policies, procedures and training. Please refer to The CCG Information Security, Remote Working and Portable Devices and Network Security policies.

The CCG will adhere to the NHS Guidance for reporting, managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation (IG SIRI) and as part of this, will review and maintain incident reporting procedures and monitor and investigate all reported instances of actual or potential breaches. Under Data Protection Legislation, where an incident is likely to result in a risk to the rights and freedoms of the Data Subject/individuals the Information Commissioner's Office (ICO) must be informed no later than 72 hours after the organisation becomes aware of the incident. Please refer to The CCG IG SIRI Policy.

7. Information Quality Assurance

The CCG Information Governance Steering Group (ISGS) will maintain policies and procedures for information quality assurance and the effective management of records. Please see the CCG Records Management Policy.

The CCG will undertake or commission annual assessments and audits of its information quality and records management arrangements.

Managers are expected to take ownership of, and seek to improve, the quality of information within their services.

Wherever possible, information quality should be assured at the point of collection.

Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

8. Commissioning of New Services

The Data Protection Officer should be consulted during the design phase of any new service, process or information asset and contribute to the statutory Data Protection Impact Assessment (DPIA) process when new processing of personal data or special categories of personal data is being considered. Responsibilities and procedures for the management and operation of all information assets should be defined and agreed by the CCG SIRO and the Information Asset Owner's.

All staff members who may be responsible for introducing changes to services, processes or information assets must be effectively informed about the requirement to complete a statutory DPIA and where required, seek review from the SCW IG Data Protection Impact Assessment Panel prior to approval or further work.

The CCG will maintain a DPIA framework that includes an approved template, guidance and supporting checklists.

9. Roles and Responsibilities

The CCG has a responsibility for ensuring that it meets its corporate and legal responsibilities and for the adoption of internal and external governance requirements.

The Hierarchical Management Structure and associated roles is detailed in the Information Governance Framework Document.

Clinical Chief Officer

The Chief Executive has overall responsibility for governance. As Chief Executive he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity

Caldicott Guardian

The Caldicott Guardian is seen as the 'conscience' of the organisation regarding the use of personal confidential data. They are responsible for ensuring all personal confidential data is shared in an appropriate and secure manner

Senior Information Risk Owner

The senior information risk owner (SIRO) is responsible for leading on information risk and for overseeing the development of an information risk policy. For ensuring the corporate risk management process includes all aspects of information risk and for ensuring the appropriate Committee is adequately briefed on information risk issues

Data Protection Officer

The Data Protection Officer (DPO) has the responsibilities as set out in the GDPR guidance, such as monitoring compliance with IG legislation, providing advice and recommendations on Data Protection Impact Assessments, giving due regard to the risks associated with the processing of data undertaken by the organisation and acting as the contact point with the and ICO.

NHS South, Central and West Commissioning Support Unit Head of Governance

The Head of Governance is responsible for ensuring that this policy is implemented and that information governance systems and processes are developed and training is available and is also responsible for the overall development and maintenance of information management practices.

NHS South, Central and West Commissioning Support Unit Information Security Manager

The SCW Information Security Manager is responsible for all aspects of information governance relating to IT systems including the production of all relevant IT policies and for the monitoring and audit of the hosted IT provider

Data Custodians

To raise the profile of information governance throughout the CCG and to provide local 'champions', the CCG has established a network of data custodians. These individuals are directly accountable to the information asset owner and indirectly to the SIRO and will provide assurance that information risk is being managed effectively for their assigned information assets and for ensuring all staff complete information governance training via E Learning for health. This role is in addition to their duties and should be fully supported by their manager and recognised in their job description.

Data custodians will also, on an annual basis, be responsible for local assessment of data collections to establish an information asset register (IAR) and Data Flow Map (DFM) and also audit staff compliance with Information handling requirements. This important task provides a CCG wide inventory to inform the annual registration with the Information Commissioner and highlights potential risk areas that may need risk management intervention. Information assets (IAs) should include any operating systems, infrastructure, business applications, off the shelf products, services, user-developed applications, records and information held.

The data custodians will be briefed on information governance developments and receive specific training.

Support in the role is available at any time from the SCW information governance team. The CCG values staff comments regarding information handling arrangements and training and it is hoped that each data custodian will act as a further conduit to voice these comments

Governing Body

It is the role of the Governing Body to define the policy in respect of information governance, taking into account legal and NHS requirements. The Governing Body is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Audit Committee

The Audit Committee is responsible for overseeing day to day information governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating information governance and raising awareness of information governance.

Staff

All staff, whether permanent, temporary, contracted, or contractors are responsible for ensuring that they are aware of and comply with the requirements of this policy.

10. Training

All staff whether permanent, temporary or contracted are required to comply with the IG Staff Handbook which stresses the importance of appropriate information handling and incorporates legislation, the common law and best practice requirements. Information Governance is the framework drawing these requirements together therefore it is important that staff receive the appropriate training. On joining the organisation, staff will receive a copy of the Information Governance staff handbook and will be required to sign and return a receipt to the IG Team.

The CCG will ensure that all staff receives annual Information Governance training appropriate to their role through the ConsultOD portal or face to face training (where available) delivered by the SCW Information Governance Team. Managers are responsible for monitoring staff compliance. New starters and any temporary, contract or agency staff must also complete the Information Governance Training when beginning their employment and annually thereafter.

11. 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 A.

12. Monitoring Compliance And Effectiveness

This policy will be monitored by the Audit Committee to ensure any legislative changes that occur before the review date are incorporated.

Compliance with the Data Security and Protection Toolkit will be assessed by NHS Digital including a review of evidence, as part of the CCG performance assessment. The CCG will ensure that information governance is part of its annual cycle of internal audit. The results of audits will be reported to the Audit Committee in Common Group

Compliance with the policies is stipulated in staff contracts of employment. If staff members are unable to follow the policies or the policy requirements cannot be applied in a specific set of circumstances, this must be immediately reported to the Line Manager, who should take appropriate action. Any non-compliance with the policies or failure to report non-compliance may be treated as a disciplinary offence

13. Review

This policy will be reviewed annually by the SCW IG team, or if required by law.

14. Additional References and Associated Codes of Practice

- NHS Digital Codes of Practice https://digital.nhs.uk/codes-of-practice-handling-information/confidential-information
- Department of Health Code of Practice https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice
- CQC Code of Practice http://www.cqc.org.uk/sites/default/files/20160906%20Code%20of%20practice%20on%20CPI%202016%20FINAL.pdf
- Health and Social Care (Safety and Quality) Act 2015 http://www.legislation.gov.uk/ukpga/2015/28/contents/enacted
- NHS England Policy https://www.england.nhs.uk/publication/confidentiality-policy/

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