Information Governance Policy Version 2.0

NHS North Hampshire Clinical Commissioning Group

DOCUMENT CONTROL

Document Name	Version	Status	Author
Information Governance Policy	2.0	GDPR Update	Information Governance Services
Document objectives:	This policy supports SCW staff in compliance with Data Protection legislation, achieving best practice in the area of Information Governance and in meeting the requirements of the Data Security and Protection Toolkit		
Target audience:	All staff		
Committee/Group Consulted:	SCW Information Governance Steering Group		
Monitoring arrangements and indicators:	This policy will be monitored by the Information Governance Steering Group to ensure any legislative changes that occur before the review date are incorporated.		
Training/resource implications:	All Staff - Dissemination will take place using the Staff bulletin and will be displayed on the intranet IG team pages		
Approved and ratified by:	SCW Information Governance Steering Group Corporate Governance and Assurance Group	Date: 07-06-18 Date: 25-06-18	
Equality Impact Assessment:	Yes	Date: 07-06-18	
Date issued:	31-07-18		
Review date:	**April 2019**		
Author:	SCW Information Governance Team		
Lead Director:	Head of Information Governance		

Change Record

Date	Author	Version	Page	Reason for Change
05.07.13	Jackie Thomas	1.1	1	Amend version number and review date
05.07.13	Jackie Thomas	1.1	3	Insert information handling requirements
05.07.13	Jackie	1.1	4	Insert new policy name for Data

	Thomas			Protection Policy
05.07.13	Jackie Thomas	1.1	8	Health and Social Care Information entre
11.06.15	Beverly Carter	1.2	Various	Amend to NHS South, Central and West Commissioning Support Unit
03.12.15	Shelley Brown	1.3	Various	Minor amendments
11.12.15	Shelley Brown	1.4	Various	Removal of reference to audits
09.08.16	Shelley Brown	1.5	8	Reference to codes of practice on confidential information
01.11.16	Shelley Brown	1.6	2	Restructure document information table
10.11.16	Hayley Matthews	1.7	7	HSCIC changed to NHS Digital
30.08.17	Jackie Thomas	1.8	2	Replace policy statement wording
30.08.17	Jackie Thomas	1.8	4	Include GDPR review information
30.08.17	Jackie Thomas	1.8	5	Include additional introduction information in line with NHS England IG Policy
30.08.17	Jackie Thomas	1.8	5	Update titles of SCW Data Subject Access Request Policy and Records Management Code of Practice
30.08.17	Jackie Thomas	1.8	8	Update mandatory IG training information
30.08.17	Jackie Thomas	1.8	8	Include IGSG and CGAG role and responsibilities
30.08.17	Jackie Thomas	1.8	Throughout document	Minor amendments and formatting
04.09.17	Angela Oakley	V1.8 Draft GDPR Update V1.0	Throughout document	Draft amendments in line with GDPR
13.03.18	Angela Sumner	V2.0 Draft Legislat	Throughout document	Draft amendments in line with GDPR and the Data Protection Act 2018

		ive update		

Reviewers/contributors

Name	Position	Version Reviewed & Date
Jackie Thomas	Information Governance Manager	V1.1 05.07.13
Beverly Carter	Head of Information Governance	V1.2 11.06.15
Shelley Brown	Regional Information Governance Lead	V1.3 03.12.15
Shelley Brown	Regional Information Governance Lead	V1.4 11.12.15
Shelley Brown	Regional Information Governance Lead	V1.5 09.08.16
Shelley Brown	Regional Information Governance Lead	V1.6 01.11.16
Hayley Matthews	Information Governance Manager	V1.7 10.11.16
Jackie Thomas	Information Governance Manager	V1.8 30.08.17
Angela Sumner	Senior Information Governance Manager	

Contents

Version Number: 2.0	Issue/approval date: 25-06-18
Status: Final	Next review date: April 2020

1. INTRODUCTION

The role of NHS North Hampshire Clinical Commissioning Group (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 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.

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 (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.

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 Regulation (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 Finance and Performance Committee 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 CCG Finance & Performance Committee is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

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

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

CCG Caldicott Guardian
The CCG 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

CCG Senior Information Risk Owner
The CCG 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 CCG Finance & Performance Committee is adequately briefed on information risk issues

CCG 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 Information Governance

The Head of Information 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 throughout the CCG.

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

The SCW CSU 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 CCG's hosted IT provider

CCG 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 CSU 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

CCG Governing Body

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

CCG Finance & Performance Committee

The CCG Finance & Performance Committee is responsible for overseeing day to day information governance issues; developing and maintaining policies, standards, procedures and guidance, coordinating information governance in the CCG and raising awareness of information governance.

CCG 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 CCG 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, CCG 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 online E-Learning for Health training tool https://www.e-lfh.org.uk 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 SCW Information Governance Steering Group 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 CCG Finance & Performance Committee

Compliance with the CCG policies is stipulated in staff contracts of employment. If staff members are **unable** to follow the CCG 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 CCG 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/

- All THE CCG Policies, procedures and guidance relating to the management and processing of information within the organisation

APPENDIX A: EQUALITY IMPACT ANALYSIS

Equality Impact Analysis on the

Information Governance Policy

1 What is it about?	***Refer to the Equality Act 2010***
a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve The Information Governance Policy details how the CCG will meet its legal obligations and NHS requirements concerning the management of information and the governance arrangements in place to support this.	
b) Who is it for? All staff	
c) How will the proposal/policy meet the equality duties? The policy will have no adverse effect on equality duties as it considers the management of information to be of equal status across all groups of people.	
d) What are the barriers to meeting this potential? There are no barriers.	
2 Who is using it?	***Consider all equality groups***
a) Describe the current/proposed beneficiaries and include an equality profile if possible The policy is applicable to all.	
b) How have you/can you involve your patients/service users in developing the proposal/policy? Patients and service users have not been involved in developing the policy as this is an operational policy.	
c) Who is missing? Do you need to fill any gaps in your data? There are no gaps.	
3 Impact	***Consider how it affects different dimensions of equality and equality groups*** Using the information from steps 1 & 2 above:
a) Does (or could) the proposal/policy create an adverse impact for some groups or individuals? Is it clear what this is? It is not anticipated that any adverse impact will be created.	
b) What can be done to change this impact? If it can't be changed, how can this impact be mitigated or justified?	

This is not applicable.
c) Does (or could) the proposal/policy create a benefit for a particular group? Is it clear what this is? **Can you maximise the benefits for other disadvantaged groups?** This policy is equal across all groups.
d) Is further consultation needed? How will the assumptions made in this analysis be tested? No.
4 So what (outcome of this EIA)? ***Link to the business planning process***
a) What changes have you made in the course of this EIA? None.
b) What will you do now and what will be included in future planning? Not applicable.
c) When will this EIA be reviewed? At policy review.
d) How will success be measured? No equality issues are created.

Sign-off

Name of person leading this EIA: **Angela Sumner** **angelasumner@nhs.net**	Date completed: **08-06-18** Proposed EIA review date: **01-04-19**
Signature of director/decision-maker **Add signature** Name of director/decision-maker **Insert Name and Position**	Date signed **Insert date**