NHS
Hampshire, Southampton and Isle of Wight
Clinical Commissioning Group

INFORMATION GOVERNANCE POLICY

Document number	IG/007/V1.2
Version	Version 1.2
Approved by	Policy Sub Group
Document author	Information Governance Consultant, South Central & West Commissioning Support Unit
Executive lead	Chief Finance Officer (Senior Information Risk Owner)
Date of approval	12 August 2021
Next due for review	April 2022

Version control sheet

Version	Date	Author	Comment
V1.0	11/02/21	Hayley Matthews	Review and update in line with planned merger of HIOW Partnership of CCGs, West Hampshire CCG and Southampton City CCG to form NHS Hampshire, Southampton and Isle of Wight CCG on 1st April 2021. Update includes removal of EU GDPR, replaced with UK GDPR.
V1.1	15/05/21	IG Transition Group	Amendments recommended by IG Transition Group
V1.2	23/08/21	Governance Manager	Minor amendments recommended by Policy Sub Group of 12/08/21 and reformat into CCG approved template

EQUALITY STATEMENT

Equality, diversity and human rights are central to the work of the Hampshire, Southampton and Isle of Wight (HSI) CCG. This means ensuring local people have access to timely and high quality care that is provided in an environment which is free from unlawful discrimination. It also means that the CCG will tackle health inequalities and ensure there are no barriers to health and wellbeing.

To deliver this work CCG staff are encouraged to understand equality, diversity and human rights issues so they feel able to challenge prejudice and ensure equality is incorporated into their own work areas. CCG staff also have a right to work in an environment which is free from unlawful discrimination and a range of policies are in place to protect them from discrimination.

The CCGs' equality, diversity and human rights work is underpinned by the following:

- NHS Constitution 2015.
- Equality Act 2010 and the requirements of the Public Sector Equality Duty of the Equality Act 2010.
- Human Rights Act 1998.
- Health and Social Care Act 2012 duties placed on CCGs to reduce health inequalities, promote patient involvement and involve and consult the public.

Contents

1. Introduction

The role of 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 (IG) 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:

- IG 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:

- **H**eld securely and confidentially
- **O**btained fairly and efficiently
- **R**ecorded accurately and reliably

- **U**sed effectively and ethically
- **S**hared 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 UK General Data Protection Regulation (UK 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, Section 22 of the Gender Recognition Act 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 UK 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.

Managing protected information about transsexual people. Section 22 of the Gender Recognition Act 2004 says that:

> *'It is an offence for a person who has acquired protected information in an official capacity to disclose the information to any other person.'*

'Protected information' means information which relates to a person who has made an application under the Gender Recognition Act. This covers both the fact of the application itself and, if the application was successful, the fact that the individual was previously of the opposite gender to the one in which they are now legally recognised.

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 UK 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 UK 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 or gender identity
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 South Central & West Commissioning Support Unit (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 UK General Data Protection Regulation (UK 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 (2021). 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 IG and Cyber Security Serious Incidents Requiring Investigation (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 Incident Management and Reporting Procedure.

7. Information quality assurance

The Policy Sub Group 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 (DPO) 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 Senior Information Risk Owner (SIRO) and the Information Asset Owners (IAOs).

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 seek review from the SCW CSU IG Consultant for the CCG 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 IG Framework Document.

Accountable Officer
The Accountable Officer has overall responsibility for governance. As Accountable Officer they are 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 DPIAs, giving due regard to the risks associated with the processing of data undertaken by the organisation and acting as the contact point with the 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 IG 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 and Isle of Wight NHS Trust Information Security Managers

The Information Security Managers are responsible for all aspects of IG 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 IG throughout the CCG and to provide local 'champions', the CCG has established a network of Data Custodians (DCs). These individuals are directly accountable to the IAOs 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 IG training via e-Learning for Healthcare (e-LfH). This role is in addition to their duties and should be fully supported by their manager and recognised in their job description.

DCs also, on an annual basis, are 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 ICO and highlights potential risk areas that may need risk management intervention. Information assets should include any operating systems, infrastructure, business applications, off the shelf products, services, user-developed applications, records and information held.

The DCs will be briefed on IG developments and receive specific training.

Support in the role is available at any time from the SCW CSU IG Team. The CCG values staff comments regarding information handling arrangements and training and it is hoped that each DC 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 IG, 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.

Information Governance Steering Group *(to be confirmed)*
The *'Group'* is responsible for overseeing day to day IG issues; developing and maintaining policies, standards, procedures and guidance, coordinating IG and raising awareness of IG.

Service Leads
Service Leads are responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. Part of this obligation is to ensure that all staff are trained and made aware of confidentiality requirements and procedures. DCs are responsible for carrying out annual audits and to implement local remedial actions in response to audit findings.

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. Equality Act 2010 – Equality analysis

An Equality Impact Analysis (EIA) has been completed as this policy was assessed as having a medium impact on individuals with characteristics protected under the Equality Act. There is a risk of negative impact if this and related policies are not followed; note particular requirements under Section 22 of the Gender Recognition Act 2004. A copy of the EIA is attached at Appendix A.

11. 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. IG 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 IG Staff Handbook and to ensure compliance, an email is required to be returned to the IG Team directly from the email account of the relevant member of staff, confirming the IG Handbook has been read and understood.

The CCG will ensure that all staff receive annual IG training appropriate to their role through the online e-Learning for Healthcare training tool https://www.e-lfh.org.uk or face to face training (where available) delivered by the SCW CSU IT Team. Managers are responsible for monitoring staff compliance. All new staff and any temporary, contract or agency staff must also complete Data Security Awareness training within two weeks of joining the organisation and annually thereafter. For existing staff, refresher training must be completed on an annual basis.

12. Dissemination

This policy will be made available to staff on the IG page of the CCG website, with a link to the appropriate page also available on the staff intranet / StayConnected portal.

13. Monitoring compliance and effectiveness

This policy will be monitored by the Policy Sub 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 IG is part of its annual cycle of internal audit. The results of audits will be reported to the CCG Audit and Risk Committee.

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. Compliance will be monitored through the following mechanisms:

- Receipt of email confirmation that staff have received a copy of the IG Staff Handbook and understand their responsibilities
- Completion of induction and annual IG training
- Completion of IG modules / training relevant to the roles of the SIRO, Caldicott Guardian, DPO, IAO and DCs.

14. Review

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

15. Stakeholder / consultation information

This policy was already in place in the HIOW Partnership of CCGs, West Hampshire CCG and Southampton City CCG prior to the merger to form NHS Hampshire, Southampton and Isle of Wight CCG on 1 April 2021.

It has been through an internal process and reviewed by the IG Team, South Central & West Commissioning Support Unit, with input from the IG Transition Group, DPO, Governance Managers and reviewed by the SIRO.

16. 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
- 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/
- Section 22 of the Gender Recognition Act 2004
  https://www.legislation.gov.uk/ukpga/2004/7/section/22
- All CCG Policies, procedures and guidance relating to the management and processing of information within the organisation

Appendix A: Equality Impact Analysis

Equality Impact Analysis (SCW CSU Template) 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. Negative impact if this and related policies are not followed. Note particular requirements under Section 22 of the Gender Recognition Act 2004	
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. Negative impact if this and related policies are not followed. Note particular requirements under Section 22 of the Gender Recognition Act 2004	

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? The policy was amended to recognise that there is a risk of negative impact if the policy is breached; note particular requirements of Section 22 of the Gender Recognition Act 2004.
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. Negative impact if this and related policies are not followed. Note particular requirements under Section 22 of the Gender Recognition Act 2004

Sign-off *(to be completed on approval of the policy)*

Name of person leading this EIA: **CSU IG Team**	Date completed: **12 February 2021** Proposed EIA review date: **March 2023**
Name of director/decision-maker **Roshan Patel, Chief Finance Officer (Senior Information Risk Owner).**	