Hampshire, Southampton and Isle of Wight
Clinical Commissioning Group

INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK AND STRATEGY

Policy number	IG/002/V1.3
Version	1.3
Approved by	Audit and Risk Committee
Document author	SCW CSU Information Governance Services
Executive lead	Chief Finance Officer (Senior Information Risk Owner)
Date of approval	14 July 2021
Next due for review	June 2022

Version control sheet

Version	Date	Author	Comment
V1.1	09/02/21	Jackie Thomas	Amalgamate, 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.
V1.2	18/02/21	IG Transition Group	Pg 7: Section 3: Add Patients to start of 3rd paragraph, and Section 5: Reword 3rd paragraph Pg 11: Section 7: Remove signature sheet return. Replace with email confirmation. Add timescale of 2 weeks to new starter Data Security Awareness training completion Pg 14: Appendix A: Include IoW NHS Trust IG Services and policies
V1.3	27 July 2021	Governance Manager	Reformatted into CCG policy 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

This framework sets out the approach taken within the CCG for embedding information governance (IG) and details the continuous improvements that the CCG is working towards. The organisation must have a robust IG management framework to provide the clarity and context for its IG activities.

The framework identifies how the CCG will deliver its strategic IG 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 IG 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.

IG 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 is managed effectively within a robust IG 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 CCG 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
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 the CCG 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.

Patients and staff will be aware that their records will not be disclosed inappropriately, which will lead to greater confidence in NHS working practices.

The IG framework should be seen as a tool that will aid the CCG in preparation for embedding a 'robust governance framework'. IG 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 Hampshire, Southampton and Isle of Wight CCG Audit and Risk Committee when requested.

The CCG Audit and Risk Committee will receive bi monthly updates on progress with IG 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 IG framework, policy and improvement plan.

The annual audit of IG shall be reported to the CCG Audit and Risk Committee together with any recommendations identified and the associated improvement plans.

The Audit and Risk Committee will receive an annual IG report.

5. The Information Governance action plan / improvement programme

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

The IG action plan is a standing item on the CCG Audit and Risk Committee agenda and is an evolving working document. Any risks and issues identified that may impede delivery of the plan will require decisions to be reached to assure a managed approach to delivery of the plan is implemented effectively. The plan is available upon request from the South Central & West Commissioning Support Unit (SCW CSU) IG Lead.

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

Implementation of robust IG 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

IG 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 IG responsibilities:

- Openness
- Legal compliance
- Information security
- Quality assurance
- Proactive use of information

6. Accountability and responsibilities

Chief Executive Officer

The Chief Executive Officer is the 'IG lead' and has overall responsibility for compliance with IG legislation and best practices, and the requirements within the Data Security & Protection toolkit. The Chief Executive Officer is responsible for the overall management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. IG is the key to supporting this within the organisation.

Senior Information Risk Owner

The Senior Information Risk Owner (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 (IAOs).

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 DPO 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 the organisation and staff of their IG responsibilities
- Monitor compliance with the UK 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 (ICO)
- 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

Information Asset Owners (IAOs) are senior members of staff who are owners of one or more identified information assets of the organisation. There are IAOs 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

Data Custodians (DCs) serve as local records managers and are responsible for assisting in the co-ordination of all aspects of IG 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, maintained and up to date.

SCW CSU Information Governance Service

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

Information Governance Working Group – *To be confirmed*

The Information Governance Working Group (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 IAOs and DCs
- Ensuring annual assessments, 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 and Risk Committee

The Audit and Risk Committee has oversight and accountability for IG ensuring that the CCG comply with their statutory responsibilities and fulfil the requirements of administrative law, Data Protection Act 2018, UK General Data Protection Regulation, the Common Law Duty of Confidentiality and The Records Management Code of Practice for Health and Social Care 2016.

7. Supporting people

Developing a robust IG culture within the CCG is fundamental to the success of delivering the IG strategy. 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.

8. Equality analysis

The CCG is committed to equality, diversity and inclusion for all, as well as to meeting the Public Sector Equality Duty (Equality Act 2010).

Both new policies / procedures, and existing policies / procedures when reviewed, come within the Public Sector Equality Duty. This means that authors must consider whether the policy will be effective for all patients and/ or staff. This process is called Equality Impact Assessment (EIA).

These procedures have been assessed as having a low impact on people with characteristics protected by the Equality Act. As such a full EIA is not required.

9. Training

It is the responsibility of the CCG to ensure that all new staff are provided with IG, information security, freedom of information and records management training as part of their induction. An IG Handbook is issued upon notification of a new starter; 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. 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 the SIRO are required to have undertaken all of the 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 within two weeks of joining the organisation. For existing staff, refresher training must be completed online on an annual basis.

10. Dissemination/publication

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.

11. 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 and Risk Committee.

12. Review

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

13. Stakeholder /consultation information

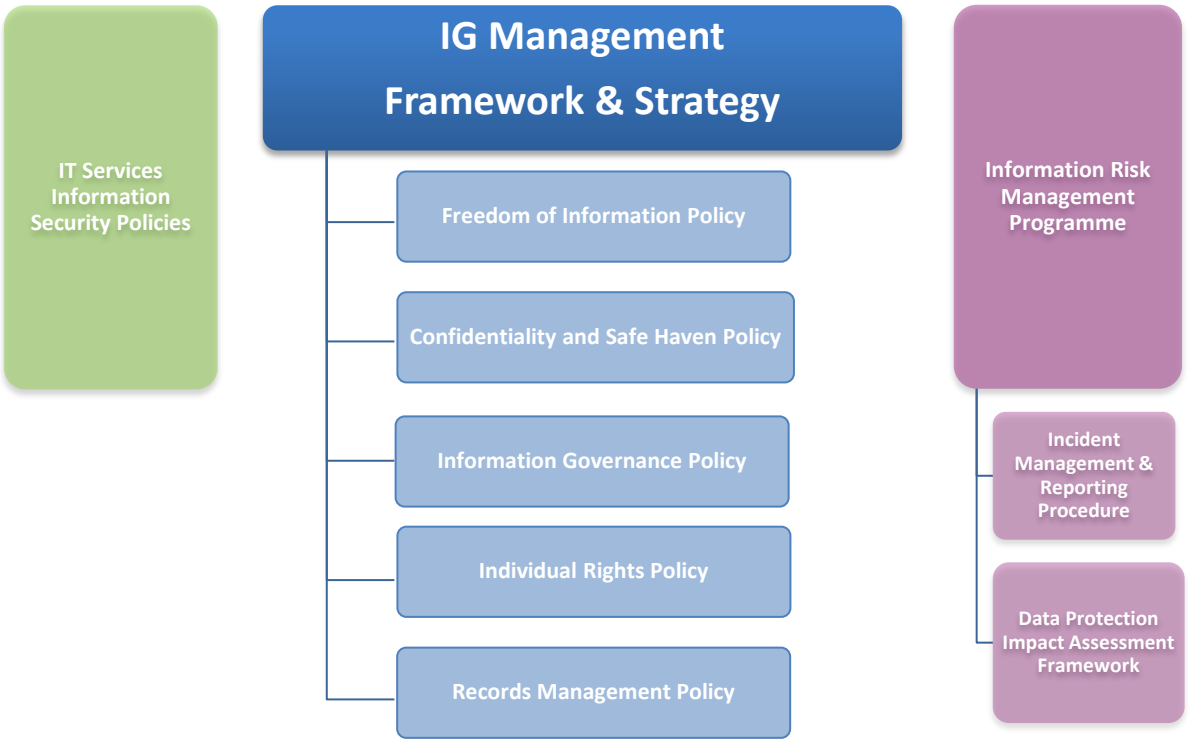
This policy was already in place in the HIOW Partnership of CCGs, West Hampshire CCG and Southampton City CCG prior to the merger to form NHS Hampshire, Southampton and Isle of Wight CCG on 1 April 2021.

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.

14. 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 IG standards throughout the organisation and must be read in conjunction with those listed in Appendix A and are available on the CCG website.

APPENDIX A: Policies and Procedures



POLICIES

Freedom of Information Act 2000 Policy
This policy outlines the organisation's responsibilities in complying with the Freedom of Information 2000 Act, the Environmental Information Act 2004, the Re-use of Public Sector Information and the relation to the Data Protection Legislation. This policy is a statement of what the CCG intends to do to ensure and maintain compliance with the Act and regulations. It is not a statement of how compliance will be achieved; this will be a matter for operational procedures.

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 UK 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 and Isle of Wight NHS Trust IT services provide and support the information systems and networks used by the CCG.

SCW CSU Information Security Policy and IoW NHS Trust Information Security Policy
All staff have a responsibility for information security. Therefore, awareness and compliance of ALL staff is essential. These documents describe the approach to information security and employees' responsibilities for security of information held both manually and on computers.

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

SCW CSU 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.

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

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

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

SCW CSU IT-Remote Working and Portable Devices Policy and IoW Trust 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 and Isle of Wight Trust IT providers, for purposes connected with the work of the organisation.

SCW CSU IT-Security Incident Handling Policy
This document provides a framework for handling security breaches. It outlines the steps to be taken after a security breach has been reported.

SCW CSU IT-Service Equipment Disposal Policy
The objective of this policy is to ensure that the proper guidance is followed for IT hardware disposal, especially in relation to the destruction of information which the equipment and hardware may have processed and may still contain or have stored.

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

SCW CSU IT-Network Security Policy and IoW NHS Trust Information Technology Network Security Policy
The aim of this policy is to ensure the security of the SCW and Isle of Wight Trust network.

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

SCW CSU IT-Security Framework
This document provides a high-level explanation of the framework in use at both SCW and the CCG to secure information assets.

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

SCW CSU Core GPIT Service Provision Policy
This is a standard policy by which GP practices can procure a modern functional phone / telephone system with minimal risk to their data security and existing N3 network.

SCW CSU IT-Services – Information Security Assurance Plan
This document provides a high-level summary of the mechanisms that SCW use to manage information security.

SCW CSU IT Services 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 set out the approach taken within the CCG for the management of IG risk incidents.

Data Protection Impact Assessments
Article 35 of the UK General Data Protection Regulation (UK 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 Data Protection Impact Assessments has become common practice in the NHS and the UK 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 Working Group - TBC
- The Risk and Audit Committee

LEGISLATION

All staff are required to comply with Data Protection Legislation. This includes

- the UK General Data Protection Regulation (UK GDPR),
- the Data Protection Act (DPA) 2018,
- 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 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 B: Equality Impact Assessment

Equality Impact Analysis (SCWCSU template) on the

Information Governance Framework and Strategy

1 What is it about?
a) Describe the proposal/policy and the outcomes/benefits you are hoping to achieve The Information Governance Framework and Strategy 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 strategy 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?
a) Describe the current/proposed beneficiaries and include an equality profile if possible The strategy 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 strategy 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 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 strategy 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)?
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 review.
d) How will success be measured? No equality issues are created.

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

Name of person leading this EIA: **CSU IG Team**	Date completed: **18 February 2021** Proposed EIA review date: **June 2022**
Name of director/decision-maker **Roshan Patel, Chief Finance Officer (Senior Information Risk Owner).**	