NHS Oxfordshire Clinical Commissioning Group

Policy	**Information Governance Management Framework, Strategy & Policy**
Version Number	2.0
Version Date	January 2019
Review Date	January 2021
Responsible Owner	OCCG Governance Manager
Approving Body	OCCG Executive Committee
Target Audience	All Staff

Document Control

Reviewers and Approvals

This document requires the following reviews and approvals:

Name	Version Approved	Date Approved
Oxfordshire CCG IG Group	2.0	
OCCG Executive Committee	2.0	

Revision History

Version	Revision Date	Details of Changes	Author
V2.0 Draft Legislative update	November 2018	Throughout document	SCW CSU Information Governance
V2.0	January 2019	Review	OCCG Governance Team

Links or Overlaps with Other Key Documents and Policies

Document Title	Version and Issue Date	Link
IG Staff Handbook	V.2.0 Jan 2019	

Acknowledgement of External Sources

Title / Author	Institution	Link

Freedom of Information

If requested, this document may be made available to the public and persons outside the healthcare community as part of OCCGs commitment to transparency and compliance with the Freedom of Information Act.

Equality Analysis

OCCG aims to design and implement services, policies and measures that are fair and equitable. As part of the development of this policy its impact on staff, patients and the public have been reviewed in line with OCCG's legal equality duties.

Contents

1. INTRODUCTION

The role of Oxfordshire Clinical Commissioning Group is to support the commissioning of healthcare, so that valuable public resources secure the best possible outcomes for patients. In doing so, the CCG will uphold the NHS Constitution. The Information Governance Management Framework, Strategy & Policy is important because it will help the people who work for OCCG to understand how to look after the information they need to do their jobs, and to protect this information on behalf of patients, the public and staff.

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.
Implementation of robust information governance arrangements will deliver improvements in information handling by following the Department of Health standards (known as the 'HORUS' model), these standards require that information will be:

Held securely and confidentially
Obtained fairly and efficiently
Recorded accurately and reliably
Used effectively and ethically
Shared appropriately and lawfully

Information governance is a framework to provide consistency and best practice for the many different information handling requests and associated guidance. These

principles are equally supported by the Caldicott Principles which have been subsumed into the NHS Code of Confidentiality.

There are five interlinked principles, which serve to guide these information governance responsibilities:

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

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

The Information Governance Management Framework, Strategy & Policy identifies how the CCG will deliver its strategic information governance responsibilities by identifying the accountability structure, processes, interrelated policies, procedures, improvement plans, reporting hierarchy and training within the CCG. The CCG will also ensure that the future management and protection of organisational information is in compliance with legislative and Government process and procedure including the NHS Digital 10 Data Security Standards.

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.

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.

Information governance management ensures that data is sourced, held and used legally, securely, efficiently and effectively, in order to deliver the best possible care in compliance with legislation and advice received from bodies including NHS Digital. Information is a vital asset to the organisation supporting the effective management of commissioned services and resources. Therefore it is essential that all organisational information be managed effectively within a robust information governance management framework.

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 OCCG or a commercial partner if improperly accessed or shared. Also as defined in the Freedom of Information Act 2000 and the Environmental Information Regulations.

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.

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 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.

OCCG will 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 policy will lead to improvements in information handling underpinned by clear standards. OCCG will be able to ensure that all employees manage personal information in compliance with NHS Digital regulations for governance.

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

The information governance framework should be seen as a tool that will aid the CCG in preparation for embedding a ‘robust governance framework’. Information governance contributes to other standards by ensuring that data required for supporting decisions, processes and procedures are accurate, available and endures.

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 OCCG Information Governance Incident Management and Reporting Procedure.

7. INFORMATION QUALITY ASSURANCE

The CCG Executive Committee will maintain policies and procedures for information quality assurance and the effective management of records. Please see the OCCG 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.

Reporting: A report shall be presented to the Information Governance Group (IGG): The IGG will receive updates on progress with information governance audits, training and toolkit evidence requirements, together with updates on any incidents that may have occurred. The committee will also identify and allocate any associated resource implications incurred by the implementation of the information governance framework, policy and improvement plan.

The annual audit of information governance shall be reported to the IGG together with any recommendations identified and the associated improvement plans.

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 IGG agenda and is an evolving working document. Any risks and issues identified that may impede delivery of the plan will require decisions are reached to assure a managed approach to delivery of the plan is implemented effectively. The plan is available upon request from the IGG.

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

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 SIRO (Senior Information Risk Owner) and the Information Asset Owners.

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.

8. 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 Executive Committee is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

Oxfordshire Clinical Commissioning Group Executive Committee

It is the role of the Executive Committee to define CCG policy in respect of Information Governance, taking into account legislative and NHS requirements. The Executive Committee is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy.

OCCG Information Governance Group (IGG) & Information Governance Working Group (IGWG)

The CCG IGG & IGWG are 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.

Oxfordshire Clinical Commissioning Group 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. Data Custodians are responsible for carrying out annual audits and to implement local remedial actions in response to audit findings.

Oxfordshire Clinical Commissioning Group 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.

Director of Governance

The Director of Governance is the ‘information governance lead’ and has overall responsibility for compliance with information governance legislation and best practices, and the requirements within the ‘Data Security and Protection toolkit’ (DSPT). The Director of Governance is responsible for the overall management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Information governance is the key to supporting this within the organisation.

Senior Information Risk Owner (SIRO)

The SIRO is a member of the Executive Management Team and is accountable to the Governing Body for the use of information and will ensure that the organisation conducts its business in an open, honest and secure manner, updating the board in respect to the annual report, the statement of internal controls and any changes in the law or potential risks. The SIRO is supported by the Caldicott Guardian, the Data Protection Officer and the Information Asset Owners (IAO's).

The Caldicott Guardian

The Caldicott Guardian is a member of the Executive Management Team and a senior health or social care professional with responsibility for promoting clinical governance or equivalent functions. The Caldicott Guardian acting as the conscience of the organisation plays a key role in ensuring that the CCG satisfies the highest practical standards for handling patient/staff identifiable information. The Caldicott Guardian serves as part of a broader Caldicott function and is supported by the Data Protection Officer.

Data Protection Officer

The Data Protection Officer (DPO) should report directly to the Board via the Director of Governance on matters relating to data protection assurance and compliance. The DPO must ensure that their responsibilities are not influenced in any way, and should a potential conflict of interest arise report this to the highest management level. The DPOs cannot hold a position within the organisation that can be considered a key decision maker in relation to what personal data is collected and used. Their primary duties are to:

- Inform and advise organisation and staff of their IG responsibilities
- Monitor compliance with the GDPR and the DPA 2018
- Provide advice where requested regarding the Data Protection Impact Assessment, and monitor performance
- Cooperate with the supervisory authority
- Be the contact point with the Information Commissioners Office
- Ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects that the ICO is informed no later than 72 hours after the organisation becomes aware of the incident

They must give due regard to the risks associated with the processing of data undertaken by the organisation and work with the SIRO and Caldicott Guardian to achieve this.

Information Asset Owners (IAO's)

Within the CCG, IAO's are senior members of staff who are owners of one or more identified information assets of the organisation. There are IAO's working in a variety of senior roles to support the SIRO by risk assessing their assets in order to:

- Provide assurance to the SIRO on the security and use of these assets through contribution to an annual report
- Understand and address risks to the information assets they 'own'.

Data Custodians/Information Asset Administrators (DC's/IAAs)

DCs/IAAs serve as local records managers and are responsible for assisting in the co-ordination of all aspects of information governance requests in the execution of their duties, which include:

- provide support to their IAO
- ensure that policies and procedures are followed locally
- recognise potential or actual IG security incidents
- undertake relevant IG audit tasks
- consult their IAO on incident management
- ensure that information asset registers are accurate and maintained up to date.

SCW Information Governance Service

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

The Information Governance Group (IGG)

The IGG is in place to ensure effective management, accountability, and IG resources within each service line in order to improve compliance in all aspects of IG within the CCG structure including:

- Developing, providing direction and maintaining IG corporate policies and guidance
- Providing support to the key roles identified in the IG management structure
- Ensuring board awareness of IG resourcing requirements and implementation of improvements
- Establishing coordinated working groups for the information asset owners and data custodians/Information Asset Administrators

- Ensuring annual assessments and audits and policy reviews are undertaken where required
- Ensuring the annual assessment and associated improvement plans are prepared for approval by the board as required
- Ensuring that the CCG is in line with the mandatory training requirements of its staff as stated within the Data Security and Protection Toolkit
- Receiving outcomes of investigations into IG Serious Incidents Requiring Investigation (SIRIs) and provide support and advice as necessary in any internal or external investigation, and to make recommendations of actions to be taken to prevent a repeat of a similar incident.

9. 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. Please see the training Requirements Policy for guidance.

Supporting People

Fundamental to the success of delivering the information governance strategy is developing a robust information governance culture within the CCG. In order to promote this culture, training needs to be relevant and embedded in working practices.

Following a SIRI further training may be delivered as a mandatory requirement where an incident has occurred, as deemed appropriate as part of the investigation findings. Disciplinary procedures may be used where it is proven that an employee has acted in breach of the terms of their contract; acts of gross misconduct will lead to dismissal.

10. 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

11. MONITORING COMPLIANCE AND EFFECTIVENESS

This policy will be monitored by the CCG Information Governance Group to ensure any legislative changes that occur before the review date are incorporated.

The CCG IG action plan, along with regular progress reports will be monitored by, the CCG Information Governance Group and Executive Committee.

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 Information Governance Group along with relevant action plans which they will monitor. Reports will also be provided to the Audit Committee.
Compliance with 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
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 Committee.

12. ADDITIONAL REFERENCES AND ASSOCIATED DOCUMENTS

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

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.

Individual Rights Policy

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

Records Management Policy

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

IT Policies: The policies cited below may sit within other overarching policies

Information Security: IT Policies and documentation

SCW IT services in collaboration with Oxford University Hospital NHSFT provide and support the information systems and networks used by the CCG

IT-Services-Information Security Policy

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

IT-Services-Anti-Virus Policy

This document contains the anti-virus policy details including actions to be taken if non-compliance occurs.

IT-Services-Access Control Policy

The objective of this policy is to prevent unauthorised access to information systems and networks. The policy describes how access controls are applied by the organisation, covering all stages in the life-cycle of user access, from the initial

registration process of new users to the final de-registration of users who no longer require access to information systems and processes.

IT-Services-Password Policy

This policy describes how users of SCW supported systems should create and manage their passwords.

IT-Services-Clear Screen & Desk Policy

This policy defines how desks should be kept clear of sensitive printed material.

IT-Service-Acceptable Use Policy

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

IT-Remote Working and Portable Devices Policy

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

IT-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.

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.

IT-System Level Security Policy

The aim of this policy is to assist with the development of system level security controls

IT-Network Security Policy

The aim of this policy is to ensure the security of the CSU network.

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

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

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

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.

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

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.

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

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

Incident Management and Reporting Procedure

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

Data Protection Impact Assessments

Article 35 of the General Data Protection Regulation 2016 (GDPR) requires that a Data Protection Impact Assessment (DPIA) is undertaken where there are 'high risks to the rights and freedoms of natural persons resulting from the processing of their personal data'. The use of Privacy Impact Assessments has become common practice in the NHS and the GDPR identifies a number of situations where the processing could be considered high risk and where a DPIA is a legal requirement, including the use of special categories of personal data including sensitive data (health and social care).

Training Requirements Policy

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 Group
- The Executive Committee

Legislation

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

- the General Data Protection Regulation (GDPR)
- the Data Protection Act (DPA) 2018
- the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time

In addition, consideration will also be given to all applicable Law concerning privacy confidentiality, the processing and sharing of personal data including

- the Human Rights Act 1998,

- the Health and Social Care Act 2012 as amended by the Health and Social Care (Safety and Quality) Act 2015,
- the common law duty of confidentiality and
- the Privacy and Electronic Communications (EC Directive) Regulations

Consideration must also be given to the

- Computer Misuse Act 1990 and as amended by the Police and Justice Act 2006 (Computer Misuse)
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Electronic Communications Act 2000
- Freedom of Information Act 2000
- Other relevant Health and Social Care Acts
- Access to Health Records Act 1990
- Fraud Act 2006
- Bribery Act 2010
- Criminal Justice and Immigration Act 2008
- Equality Act 2010
- Terrorism Act 2006
- Malicious Communications Act 1988
- Counter-Terrorism and Security Act 2015
- Digital Economy Act 2010 and 2017

Guidance

- ICO Guidance
- CQC Code of Practice on Confidential Information
- NHS Digital looking after your information
- Dept. of Health and Social Care 2017/18 Data Security and Protection

Requirements

- NHS England Confidentiality Policy
- Records management: Code of Practice for Health & Social care
- Confidentiality: NHS Code of Practice - Publications - Inside Government - GOV.UK
- Confidentiality: NHS Code of Practice - supplementary guidance
- CCTV
- 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 https://www.cqc.org.uk/file/4201
- 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: **Oct 2020**
Signature of director/decision-maker **Add signature** Name of director/decision-maker **Insert Name and Position**	Date signed **Insert date**