Information Governance Framework

Version 4

Document revision history

Date	Version	Revision	Comment	Author/Editor
23/08/2018	3.2	Review	GDPR update	Senior Internal and Assurance Information Governance Manager
24/08/2018	3.3	Prior to CCGS review and adoption	Edited for use by Merton & Wandsworth CCGSs CCGS to check items highlighted in blue	Anjna Shinh, IG Compliance Manager
10/10/2018	3.4	Replaced Integrated Governance Committee with Integrated Quality & Governance Committee	IGSG Members	IGSG members
08.12.2018	3.5	Edited – transferred clauses from IG Policy	IGSG Members/Merton CCG	IGSG Members

Document approval

Date	Version	Revision	Role of approver	Approver
31.12.2018	4	Final	Information Governance Steering group Meeting	Caldicott Guardian/Senior Information Risk Owner Merton & Wandsworth CCG.

Contents

1. Introduction

This Information Governance Framework provides a solid basis upon which Information Governance (IG) and all its component parts will be implemented throughout Merton & Wandsworth CCGSs.

The Framework outlines the roles and responsibilities of those who are tasked with overseeing that IG is appropriately supported, effective management and accountability structures, governance processes, documented policies and procedures, trained staff and adequate resources.

The framework provides a summary/overview of how Merton and Wandsworth CCG is addressing the Information Governance Agenda and has adapted appropriately to the capacity and capability of the organisation.

This Framework must be read in conjunction with Merton and Wandsworth CCG's information Governance Suite of Policies and Procedures which includes, but is not restricted to the Information Governance Policy, Data Protection and Confidentiality Policy, Information Security Policy and the Information Quality Policy.

The Framework is based upon the following standards and legislation that apply to Information Governance and management, including, but not limited to the following:-

Data Protection Act 2018	Health and Social Care Act 2012	Freedom of Information Act 2000
General Data Protection Regulation May 2018	A Guide for Confidentiality in Health and Social Care	Common Law duty of Confidentiality
International Information Security Standard ISO/IEC 27002:2005	Access to Health Records Act 1990	Information Security NHS Code of Practice
Caldicott Guidance	Computer Misuse Act 1990	Mental Capacity Act 2005 1
Public Records Act 1958	Records Management code of Practice for Health and Social Care 2016	Human Rights Act 1998.

NHS Constitution – Department of Health	NHS Data Security and Protection Toolkit (DSPT)	Notification of Data Security and Protection incidents (May 2018)

2. Aims

The aim of this Framework is to set out how Merton and Wandsworth CCG will effectively manage Information Governance. The organisation will achieve compliance by the following actions:-

- The establishment, implementation and maintenance of local CCG policies for the effective management of Information Governance.
- The establishment of transparent, robust Information Governance processes that conform to Department of Health Standards and comply with all relevant legislation.
- To ensure that information is provided to service users, stakeholders and Commissioners about how information is recorded, processed, handled, stored, shared and managed.
- To provide clear advice, guidance and training to all staff to ensure that they understand and apply the principles of Information Governance to their working practice.
- To encourage an Information Governance culture through increasing aware ness and promoting Information Governance to minimise the risk of a breach of Person Identifiable Information.
- The assessment of CCG performance using the Data Security and Protection Toolkit, internal Audits, the development and implementation of action plans to ensure continued improvement.

3. Scope

The framework applies to all staff of Merton and Wandsworth CCG and includes health providers who work for and on behalf of the CCG's. In addition, this framework applies to (non-staff) groups working for the CCG collectively as 'affiliates'including, but not limited to :-

- Board and Committee Chairs and Members, remunerated expert advisers
- Non-Executive Directors
- Agency workers, contractors on temporary contracts or employed through an agency to work for Merton and Wandsworth CCG,
- Secondees (Employees who are seconded to Merton and Wandsworth from other organisations)

- Unpaid student, volunteers or placement staff.

The framework will provide assurance to service users and several stakeholders and audiences interested in the safe custody and use of sensitive , or secondary personal confidential information in healthcare.

4. Key Principles

The IG Framework is based on the following key principles:

4.1 Data Protection

For the purposes of Data Protection legislation, the CCG as Data Controllers and Data Processors will take a privacy (and Data Protection) by design and default approach to Information Governance using a risk-based methodology for decision making and delivery. As a commissioner of services, the CCGSs:

- are responsible for guiding and validating assurances regarding the appropriate management of information from its commissioned providers;
- shall seek assurance that its providers are meeting their NHS Information Governance obligations; and
- Ensure any new staff are supported in undertaking relevant and appropriate Information Governance training.

4.2 Openness and transparency

The CCG will put in place systems and process to ensure where appropriate unrestricted information is made available to the public. This will include how the public can access this and their own information in accordance with legal, regulatory or NHS requirements. Merton and Wandsworth CCG will apply an appropriate balance in accordance with General Data Protection Act (2018) on openness and confidentiality in the management and use of information.

4.3 Confidentiality

Effective standards of confidentiality and data protection applicable to staff and affiliates through policies, procedures and training and in accordance with legislative requirements of the Data Protection Act (2018) and the General Data Protection Regulations (2018).

4.4 Security

Strong information security arrangements which are documented in the Information Security Policy are applied to safeguard personal information about staff and affiliates, those that do business with Merton and Wandsworth CCG and to commercially and personally sensitive confidential information.

5. Key workstreams:

Information Governance Steering Group

The Information Governance Steering Group leads, monitors and coordinates information governance across Merton and Wandsworth CCG, with responsibility to ensure Information Governance and records management policies are cascaded to all teams via Information Asset Owners and ensure effective management of sensitive personal data and confidential information.

5.1 General Information Governance Work Plan

To ensure on-going assurance, the CCGSs will undertake a series of checkpoints each year to ensure regular scrutiny of the use of information. This supports the submission of the DSPT and any other assurance model, should it be required, for example, external audits. These key checkpoints are:

- Information Flows (mapped and risk reviewed);
- Information Asset Register (risk review);
- Information Risks reviews and impact assessments;
- Confidentiality Audit and Staff Survey;

- Information Governance audit exercises for the CCGSs;
- IG Incident Reporting and action plan implementation review;
- Governance Review; and
- Annual statement of assurance from Information Asset Owners/ Risk Owners to the SIRO.

These will be quality assured and supported by the NEL Information Governance function

The general IG work plan will co-ordinate with the specific work plans detailed below to complete an on-going assurance framework with a yearly assessment of standards and risks. The CCGS will maintain a quarterly review cycle to ensure appropriate scrutiny.

5.2 Data Protection Work Programme

The key elements of the CCGSs Data Protection Work Programme are to:

- Ensure compliance with all aspects of the Data Protection Act 2018, the General Data Protection Regulations (GDPR) 2018 and related provisions and provide reports, including undertaking audits, to the relevant governance body of the Merton and Wandsworth CCGs.
- Ensure compliance with the Information Governance related pledges and rights set out in the NHS Constitution;
- Draft and/or maintain the currency of data protection legislation requirements within relevant policies (see section 11)
- Review Data Protection Impact Assessments and Governance reviews and direct decisions to take forward and implement;
- Advise patient and public involvement fairness and transparency strategies;
- Promote data protection awareness throughout the CCGSs by organising training and providing written procedures that are widely disseminated and available to all staff;
- Co-ordinate the work of other staff with data protection responsibilities, such as Information Asset Owners;
- Ensure service users are provided with information on their rights under Data Protection Legislation;
- Assist with investigations into complaints about breaches of the Act

- If required, develop and deliver a data protection audit, proportionate and appropriate to the current and evolving requirements of the CCGSs.

5.2.1 Data Protection Impact Assessment (DPIA)

The DPIA identifies and assesses privacy implications where data about individuals is processed, i.e. collected, stored, transferred, shared and managed. It enables organisations to identify the impact that any project might have on the rights of the public/staff when processing their data. Systems can be designed to avoid unnecessary privacy intrusion or breaches, and features to reduce privacy intrusion can be built in from the outset.

A DPIA enables an organisation to anticipate and address the likely impacts of new initiatives, foresee problems, and negotiate solutions. Risks can be identified through the gathering and sharing of data and consulting with stakeholders to allow suitable controls to be put in place.

The DPIA will assist in the mitigation of data risks and facilitate the modification of plans. A DPIA should be process rather than output orientated.

A DPIA must be completed when the following activities occur:

- Developing or procuring any new programme, policy, procedure, service, technology or system ("project") that handles or collects data relating to individuals; and
- Developing revisions to an existing programme, policy, procedure, service, technology or system which significantly change how data is managed.
- The DPIA must be undertaken by the project team and identify areas for action in order to satisfy the statutory/mandatory framework for processing PCD, including identifying information risks to be added to the project risk register.

5.2.2 Privacy by Design and Default

Privacy by design means building privacy into the strategy, operation and management of a system specification.

The following are security areas that should be considered when creating bespoke technology or engaging existing technology.

Further reading: Information Commissioner's Office (ICO) Privacy by Design.

5.3: Specific Information Governance Work Plan

To meet specific requirements of the assurance framework, key tasks and evidence will be sought and evaluated from particular functions and commissioned providers where required. This will be elaborated in any contract or written agreement with service providers, which will outline the timeframe and particulars of quality assurance. Details of the evidence in place, schedule of delivery and evaluation will be maintained by the Information Governance function for the CCGS.

5.3.1 Information and Informatics IG Work Programme

The Clinical Commissioning Groups will appoint or ask, where appropriate, the provider of its Informatics services to nominate an Informatics Lead. This requirement will be outlined in the relevant written agreement.

The Informatics Lead will lead on the following areas for the statutory body:

- Secondary Use Assurance;
- Data Quality, benchmarking and auditing;
- Support the confidential use of patient information by leading, as appropriate, the use of pseudonymisation and anonymisation techniques; and
- Identify and report Information Risks related to the secondary use of patient data for key business functions (such as commissioning, performance and informatics).

5.3.2 Information and Communications Technology (ICT) IG Work Programme

The CCGS will appoint or ask, where appropriate, the provider of its Information Communication and Technology services to nominate an Information Communication and Technology lead for IG (ICT IG Lead). This requirement will be outlined in the relevant written agreement.

The ICT IG Lead will lead on the following areas for the CCGS:

- Information Security Risk Management and Assurance Plan/Strategy (see section 7 below)
- Outline the requirements for assurance, scrutiny and performance monitoring in conjunction with the CCGS;
- Lead on key Information Governance schemes to deliver assurance or effect information; and
- Identify and report Information Risks related to information security as part of the ICT Risk register and Information Risk register

5.3.3 Caldicott Function Work Programme

- The Caldicott Guardian work programme will:
- Ensure the confidentiality and data protection work programme is successfully co-ordinated and implemented;
- Ensure that assurance of confidentiality is developed and delivered including an appropriate and proportionate confidentiality audit;
- Ensure compliance with the principles contained within the NHS Constitution, the Guide to Confidentiality in Health and Social Care, the NHS Care Records Guarantee and any subsequent national guidance;
- Ensure staff are made aware of individual responsibilities through policy, procedure and training;
- Receive details of any information incidents, near misses or breaches of confidentiality;
- Complete the Confidentiality and Data Protection Assurance component of the Data Security and Protection Toolkit, contributing to the annual assessment; and
- Provide routine reports to the relevant governance body on Confidentiality and Data Protection issues.

5.3.3. Change Control

The CCGS will ensure that Information Governance requirements are included within its change control processes and systems and those that provide services to it.

5.3.4 Assurance from commissioned services

The CCGs will develop an Information Governance assurance framework for its commissioned services in line with expectations from the Department of Health and relevant contracts.

i) Healthcare Providers

Where Information Governance assurance frameworks are not in place the CCGs will negotiate with healthcare providers to ensure that contracts or informal agreements require the Healthcare providers to:

- undertake relevant assurance framework (such as the Data Security & Protection toolkit (DSPT) and CQC Regulations);
- ensure self-assessments are independently audited;

- have any audit report scruntinised by the Information Governance Steering Group; and
- ensure any IG incidents or data losses are escalated to the CCGS as commissioner, and provide assurance on the appropriate handling of these issues

Where necessary the CCGS will seek assurance as part of overall performance monitoring and resolve any failure to meet the expected contractual standard.

ii) Non-Healthcare Providers

For providers of non-healthcare services, the CCGS will ensure that appropriate contractual standards are in place and assurance sought in an appropriate and proportionate manner.

Those non-healthcare providers who provide key information management technology support or tools, such as NEL or local authority shall be asked to complete an Information Governance Assurance model, such as the DSPT. The standard expected will be outlined in the required contract or service level agreement. It is envisioned that in addition to evidencing its own assurance framework such support organisations will be asked to provide evidence in a timely and appropriate manner. This evidence will be subject to quality assurance and any action required as a consequence will be taken in a timely and appropriate manner, with the expectation that this will incur no additional cost to the CCGS.

iii) Contracts

All contracts with third parties managing personal data or confidential information on behalf of Merton & Wandsworth CCG's include standard information and GDPR clauses relating to the safe handling and management of that data.

iv) IT Cybersecurity and business continuity

Merton & Wandsworth IT Information Performance and Technology apply a comprehensive set of controls to the IT network that complies with NHS Digital requirements to ensure resilience and disaster recovery in the event of temporary or partial outages of IT systems and these are replicated in office and remotely. The full set of controls and disaster scenarios must be reported to the Audit and Risk Committee.

Merton & Wandsworth IT systems complies with the OWASP 10 steps to Cyber Security recommended by the Cabinet Office and endorsed by NHS Digital as baseline security standards and Information Security Management Systems (ISMS) including ISO/IEC27001:2005

ISO/IEC27002:2005, 2013 and ISO/IEC27005:2008.

Portable media, devices and phones are encrypted where appropriate. The Details are set out in the M& W Information Technology Policy (Audit committee- Wandsworth CCG / Audit & Governance Committee Merton CCG)

v) Records Management

Merton and Wandsworth CCG's have a planned policy approach to records management across the lifecycle of records. This is from creation to disposal to support information governance and ensures adequate records are maintained, managed, and controlled commensurate with legal, operational and information needs.

Dedicated systems will be developed to manage guidance development information with associated industry standard records and information protocols.

5.4 Accountability and Governance structure – Roles and Responsibilities.

5.4.1 Overview

Senior management involvement and leadership demonstrates the CCGs commitment to a risk management approach, and to ensure compliance with Information Governance requirements and understanding resource implications.

1) Governing Body: In line with the Guidance for NHS Boards: Information Governance the Governing Body will ensure that its organisation has taken appropriate steps to meet Information Governance standards.

2) **Accountable Officer:** Has overall accountability and responsibility for governance within the organisation. The Officer must provide assurance that all risks to the organisation, including those relating to information are effectively managed and mitigated.

3) **Senior Information Risk Owner (SIRO):** Has overall responsibility for ensuring that effective systems are in place to address the Information Governance agenda defined in Appendix A of the NHS Information Risk Management Guidance
4) **Caldicott Guardian**: The role of the Caldicott Guardian is an advisory Role acting as the conscience of the organisation for management of patient information and a focal point for patient confidentiality and information sharing issues.
5) **Information Security**: This role is fulfilled by the CSU IG Team, IT Team and local facilities management depending on the requirement. Responsible to provide advice to information owners on potential information risks and controls. Support in any risk reviews with departments.
6) **Information Asset Owners**: All senior staff at Director Level are required as Information Asset Owners for the information asset within their remit. They will provide assurance to the SIRO that information risk is managed effectively for the information assets identified within their remit. The Role and responsibility are defined in Appendix A of the NHS Information Risk Management Guidance.
7) **CSU IG Team:** Provide specialist advice and support, under contract, to the organisation in relation to IG subject matters. They will also form part of the Caldicott function and associated plan.
8) **All Substantive/Permanent Staff**: Staff working for the CCG have legal obligations under the Data Protection Act 2018, common law duty of confidentiality, and professional codes of conduct to manage information appropriately. These are in addition to their contractual obligations as employees which include adherence to policy, and confidentiality clauses in their contracts.
9) **Third Parties**: The same responsibilities for permanent staff apply to those working on behalf of the organization, as contractors, work placements, temporary employees, volunteers and students. Those working on behalf of, but not directly employed by the organisation are required to sign a third party agreement outlining their duties and obligations.
10) **CCG Member Practices:** The CCG's Governance Information Framework and policies should be followed where any member is processing information on behalf of or in relation to the CCG delivery of its functions. It is however, recommended that similar policy standards are in place within each member practice regarding the management of its own data and information.

5.4.2 Responsibilities

The CCG will put in place suitable controls to:

- Assign responsibilities to oversee delivery of standards set out in this policy

- Report on compliance against Information Governance to an authorised body in the organisation
- Ensure that staff are made aware of their responsibilities, how to comply with them and have adequate advice, training programmes and guidance to do so
- Ensure consistency of Information Governance across the organisation
- Develop Information Governance policies and procedures
- Ensure compliance with data protection, and other information security related legislation
- Provide support to the Team who manage freedom of Information and Subject Access Requests.
- Provide support to the Caldicott Guardian and Senior Information Risk Owner (SIRO)

5.4.3 Policy Standards

This Policy as part of a suite of Information Governance related policies sets out the standards that those working on behalf of a CCG will share when managing data or information.

5.4.4 Managing Information Risk

The CCG will put in place suitable mechanisms to ensure staff identify and manage information risks in line with existing risk management policy and processes to prevent reputational damage, financial loss and failure to comply with legal, regulatory or NHS requirements.

5.4.5 Integrated Governance & Quality Committee

The Integrated Governance & Quality Committee shall have the following responsibilities:

- Ensure a coordinated approach to the information agenda is developed for, and adhered to, throughout the CCGS and with contracted service providers;
- Ensure that an Information Governance (IG) Framework is in place that provides an appropriate assurance framework and management of associated risk across the information agenda;
- Consider and agree resource requirements including capacity and capability;
- Identify and endorse the appointment of senior roles and responsibilities for Information Governance;

- Scrutinise the effectiveness of strategy and consider and approve policies and procedures across the Information Governance agenda;
- Sign off approved strategies, policies and procedures on behalf of the CCGS;
- Seek assurance that risk management arrangements are in place and adhered to and assess assurance arrangements;
- Scrutinise any audit or external reports and direct the response to recommendations and recommend input into the annual audit plans; and
- Report key findings to the Governing Body and Quality Committee.

5.4.6. Information Governance Steering Group (IGSG)

The Information Governance Steering Group shall have the following responsibilities:-

- To support the Data Security and Protection Toolkit assessment by providing guidance, support and information.
- To ensure that the strategic objectives of information governance align with the Toolkit as well as serving the broader business needs of the CCGS.
- The Information Governance Steering Group will have delegated authority from the CCGS Governing Body through the CCGS Quality Committee to oversee operational work and work plans across the Information Governance agenda.
- To act as a focus point for the reporting, investigation and response to information incidents.
- To support the Caldicott function within the CCGS, and acts as the Records and Information management group.
- To provide assurance to the Quality Committee on variance and risk through the provision of a regular report, the provision of copies of its minutes and actions points and reviewing its work. Its terms of reference and work plan will be signed off by Quality Committee.
- The Information Governance Steering Group of the CCGS will at agreed intervals submit its minutes, workplan and action points to the Integrated Quality & Quality Committee [once approved].
- The Information Governance Steering Group will be chaired by the Caldicott Guardian or SIRO of the CCGS. The Information Governance Steering Group of the CCGS has delegated authority to form working groups to deal with particular Information Governance issues or work streams.

6. Information Incident Management and Reporting

6.1 Management of Incidents

Incidents will be managed in accordance with the CCGS's Incident and Serious Incidents Policy and Processes. All information incidents will be investigated by the relevant manager or if not appropriate by a manager nominated by the SIRO. The Information Governance Manager from NEL will provide guidance and support to the investigation manager.

Categorisation of the Incident will be undertaken in accordance with the CCGS policy and procedure.

In accordance with the NHS Digital Guide to Notification of Data Security and Protection incidents (May 2018)

All information incidents (whether involving PCD or not) must be reported to the Senior Information Risk Owner and the CCGS Information Governance Lead immediately on detection of the breach. Contact details can be found in Annexe A.

These incidents include:

- Near misses of information incidents;
- Suspected information incidents (such as losses of data or breaches of confidentiality);
- Information Incidents (data losses and breaches of confidentiality and Data Protection Legislation);
- Patient Identifiable Data sent to the wrong individual; and
- Loss of access to data which has or has the potential to cause a risk.

6.2 Incident Management

Incidents must be reported in 72 hours. This 72 hours starts when the CCG becomes aware of the breach which may not necessarily be when it occurred. Where the 72 hours deadline is not met an organisation must provide an explanation. Failure to notify the ICO promptly may result in additional action taken by the ICO in respect of GDPR.

Incidents will be assessed following the 'Breach Assessment Grid' which can be found in the above guide

Breaches other than 'Green Breaches' are reportable using the Data Security and Protection Toolkit.

Where an IG/Data Security Incident /breach relates to a vulnerable group in society as defined in the guidance, the minim um score will be a 2 in either significance and likelihood unless incident contained.

Where the incident is assessed that it is (at least) likely that some harm has occurred and that the impact is (at least) minor full details automatically emailed to the Information Commissioners Office and the NHS Digital Data Security Centre.

The Department for Health and Social Care will also be notified where it is (at least) likely that harm has occurred and that the impact is at least serious.

6.3 Incident Conclusion

Any report on the incident will be provided to the Information Governance Group and escalated as appropriate. These reports will be based on a Root Cause Analysis template and will provide a timeline of the incident, the background and highlight key points.

Any follow up actions will be taken in accordance with policy, at the direction of the relevant senior manager and in discussion, where relevant, with Human Resources.

7. ICT Information Security

7.1 Responsibility for ICT Information Security

All staff are responsible for maintaining the security of Information. Overall responsibility for information security rests with the Governing Body and Accountable Officer.

7.2 Management of IT Information Security Incidents and Events

The management of Information Security incidents will follow the CCGS's ICT Provider Helpdesk procedures for issue resolution and escalation as necessary. The nominated Information Security Officer will advise the Information Governance Lead or SIRO as appropriate for further guidance.

7.3 ICT Information Security Risk Management and Assurance Plan / Strategy

To ensure that there is effective implementation of Information Risk processes, the CCGS ICT Provider will ensure a comprehensively scoped, continuously reviewed and formally documented information risk

management plan and programme is in place. This plan and programme will consider the security risks to Information Assets; including the systems and media used in processing or storing that information; consideration of the potential impacts on the continued delivery of services; and the protection of PCD and corporate data are all essential elements of the plan and programme.

The Information Security Assurance plan will utilise the risk assessment methodology of the CCGS. Each risk will be clearly scoped, systematic and seek to identify, quantify and prioritise the information risks to the CCGS business functions. Consideration should also be given to information risks that may affect the CCGS business partners. Where appropriate, controls (countermeasures) should then be put in place and their effectiveness monitored to ensure that the deployed controls are effective in treating the risks. System log files and incident reports may identify ineffective or poorly deployed controls. Periodic update reviews of existing risk assessments should be undertaken, to take account of possible changes.

The risk assessment process will address a Plan, Do, Check and Act cycle:

- Risk Identification.
- Risk Analysis.
- Risk Treatment.
- Risk Review.

8. Staff Awareness and Training

Intranet pages, or their equivalent, will be provided for all staff on key Information Governance issues including, but not limited to:

- Principles of Information Governance;
- Information Management;
- Data Protection;
- Consent;
- Confidentiality; and
- Records Management.

These pages will be supported by an active communication campaign to all staff.

8.1 Training

All staff, including volunteers, students, contractors and temporary employees are required to complete and pass Information Governance training on an annual basis.

Information Asset Owners are required to ensure staff have provided them with proof that they have passed their training and are asked to ensure a copy of relevant certificates is kept on the member of staff's personnel file.

An online Information Governance training programme will be provided which is mandatory for all staff.

The online Information Governance training programme will be supported by face to face training where required.

The current training requirements will be updated when there are changes to the Information Governance assurance framework as outlined by the Department of Health, NHS England and NHS Digital.

8.2 Training Needs Assessment

A full Information Governance Training Needs Assessment will be reviewed and approved by the Information Governance Steering Group of the CCGS. This will address the expected training for staff at all levels of the CCGS and those that are working within particular specialities.

8.3. Resources

The resources available to support the Information Governance Assurance will be outlined in the relevant contract or service level agreement for the provision of the service.

9. Equality and Diversity

This policy and its impact on staff, patients or the public have been reviewed in line with the Equality Act 2010. In application of this policy the CCG has taken due regard of the need to eliminate unlawful discrimination, promote equality of opportunity and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act 2010; age disability, gender, gender reassignment, marriage and civil partnership, pregnancy and

maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership or political affiliation.

10. Monitoring and Compliance

This framework and the associated controls: Policies, Protocols, Procedures - will be monitored through the Risk Management system for the CCGS. The Information Governance Risk Register will be reviewed on a regular basis and additionally in response to any information incident or enforcement action by the Information Commissioner's Office. Information Risk Management is a key component of wider assurance and control in setting the priorities for the Information Governance work plan.

Information Asset Owners, assisted by Information Asset Administrators, will be required to routinely review the Risks and Information Flows associated with the Information Assets utilised to fulfil the business functions and activities within their remit.

11. Review

Review will take place every three years or earlier until rescinded or superseded, due to legal or National Policy changes.

The audience of this document should be aware that a physical copy may not be the latest version. The latest version, which supersedes all previous versions, is available in the policy register for the organisation. Those to whom this policy applies are responsible for familiarising themselves periodically with the latest version and for complying with policy requirements at all times.

12. Implementation and dissemination of document

12.1 Information is communicated to staff via the Information Governance Steering Group which includes all information asset owners and is cascaded to individual teams for action.

12.2 A SharePoint Repository will be added to The Intranet provide a centralised resource and point of reference for staff for information governance and records management, including policies, good practice guides and key contact information. Staff forum/Intranet

12.3 The framework, once approved, will be shared with all staff through the all staff email, intranet, included in staff briefings and placed in the policy register.

The Framework will be made available publicly if requested via a Freedom of Information request.

13. Further Reading / References

CCGS

Information Quality Policy

Information Security Policy

Information Governance Policy

Information Management Policy

Confidentiality Code of Conduct

NHS England

Risk Stratification

Invoice Validation

Data Services for Commissioners

Caldicott

National Data Guardian

Information: To share or not to share? The Information Governance Review

Government Response to the Caldicott Review

Review of data security, consent and opt-outs

Information Governance Alliance (IGA)

Information Governance Alliance

NHS

The NHS Constitution - the NHS belongs to us all

NHS Confidentiality Code of Practice

NHS codes of practice for handling information in health and care

Health Research Authority (HRA)

Health Research Authority

Section 251 and the Confidentiality Advisory Group (CAG)

British Medical Association (BMA)

Principles for sharing local electronic patient records for direct patient care

Legislation

The General Data Protection Regulations 2018

The Data Protection Act 2018

Annexe A – Key Post Holders

Contact Details for Key Post Holders: As of 19th September 2018

Role	Post Holder	Email	Telephone
CCGS Governance Lead			
Information Governance Lead (NEL team)	Claire Clements Anjna Shinh	claireclements@nhs.net Anjna.shinh@nhs.net	07824 361322 07818 013 095
Senior Information Risk Owner (SIRO)	John Atherton	John.Atherton@swlondon.nhs.uk	
Caldicott Guardian	Julie Hesketh	Julie.hesketh@swlondon.nhs	

Role	Post Holder	Email	Telephone
Data Protection Officer	Claire Edgeworth	nelcsu.dpo@nhs.net	03000 428438

Current NEL Key Post Holders

Role	Post Holder	Email	Telephone
Senior Information Risk Owner (SIRO)	David Thomas	davidthomas3@nhs.net	
Caldicott Guardian	Anna Dorothy	annadorothy@nhs.net	
Data Protection Officer	Claire Edgeworth	nelcsu.dpo@nhs.net	03000 428438