NHS
Surrey Downs
Clinical Commissioning Group

Information Governance Framework

Policy ID	IG01
Version	3.0
Owner	Justin Dix, Governing Body Secretary
Approving Committee	Executive Committee
Date agreed	27th October 2015
Next review date	29th October 2017

Improving care together across Surrey Downs

Summary

The purpose of this Information Governance Framework document is to demonstrate that there is a clear effective IG management and accountability structures, governance processes, documented policies and procedures, trained staff and resources in the CCG to manage IG effectively.

Version History

Version	Review Date	Name of Reviewer	Ratification Process	Notes
1.0	27/11/2013	NHS South CSU IG Team	Final	Approved by Executive Committee
1.1	03/12/2014	NHS South CSU IG Team	Final	Complete revision to incorporate NHS South East IG Team guidance.
1.2	15/12/2014	NHS South CSU IG Team	Final	Complete revision to incorporate NHS South East IG Team guidance.
1.3	03/07/2015	Interim Information Governance Manager – Surrey Downs CCG	Draft	Reviewed and updated to reflect to recent IG Toolkit guidelines Caldicott 2 Review and SAR accountability and responsibility in the CCG.
2.0	21/07/2015	Interim Information Governance Manager – Surrey Downs CCG	Final	Approved by Executive Committee
2.1	22/10/2015	Interim Information Governance Manager – Surrey Downs CCG	Draft	Reviewed and updated to reflect new CCG SIRO
3.0	27/10/2015	Interim Information Governance Manager – Surrey Downs CCG	Final	SIRO changes approved by Executive Committee
Contributors		Governing Body Secretary, Head of Planning & Performance and, South East CSU Information Governance Principle Associate.		
Audience		All CCG officers, Governing Body members and staff (which includes temporary staff, contractors and seconded staff) and CCG members in their capacity as commissioners.		

Equality Statement

Surrey Downs Clinical Commissioning Group (Surrey Downs CCG) aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. It takes into account the Human Rights Act 1998 and promotes equal opportunities for all. This document has been assessed to ensure that no-one receives less favourable treatment on grounds of their gender, sexual orientation, marital status, race, religion, age, ethnic origin, nationality, or disability.

Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the person requesting has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

Surrey Downs CCG embraces the four staff pledges in the NHS Constitution. This policy is consistent with these pledges.

Equality Analysis

This policy has been subject to an Equality Analysis, the outcome of which is recorded below.

1. Does the document/guidance affect one group less or more favourably than another on the basis of:			
	Race	Yes, No or N/A	Comments
	Ethnic origins (including gypsies and travellers)	No	
	Nationality	No	
	Gender	No	
	Culture	No	
	Religion or belief	No	
	Sexual orientation including lesbian, gay and bisexual people	No	
	Age	No	
	Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
2	Is there any evidence that some groups are affected differently?	No	
3	If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?	No	
4	Is the impact of the document/guidance likely to be negative?	N/A	
5	If so, can the impact be avoided?	N/A	
6	What alternative is there to achieving the document/guidance without the impact?	N/A	
7	Can we reduce the impact by taking different action?	N/A	

Contents

Information Governance Framework

1. Introduction

Surrey Downs Clinical Commissioning Group (CCG) has implemented this Information Governance Framework for the purpose of supporting Information Governance (IG) within the organisation and for all staff working in or on behalf of the organisation.

It provides a solid basis upon which IG and all its component parts will be implemented throughout the CCG. The framework outlines the roles and responsibilities of those who are tasked with overseeing that IG is appropriately supported and that all necessary guidance and advice is available in an effective and efficient manner as well as the responsibilities of all staff.

The framework is based upon the legal requirements of the Data Protection Act 1998 (DPA), Common Law Duty of Confidentiality and Human Rights Act 1998, and the Department of Health's assurance regime, the IG Toolkit (IGT).

This framework underpins the organisation's IG policies, procedures and processes upon which the organisation relies in its duty to provide and support the business of the CCG.

1.1 Key Principles

The following key principles are reflected in the framework:

- Any staff appointed will be required to meet required standards in relation to information governance and will be supported in this with the provision of mandatory and other relevant and appropriate IG training.
- As a commissioner of services, the organisation is responsible for the appropriate management of information by both healthcare and non-healthcare providers.

As a commissioner of services, both healthcare and non-healthcare, the CCG must seek assurance that these organisations are meeting their IG obligations.

2. Duties

2.1 Accountable Officer

The CCG Accountable Officer (Chief Officer) has overall responsibilities for the management of information governance and ensuring appropriate mechanisms are in place to support service delivery and continuity in the organisation. The Accountable Officer has delegated IG operational responsibilities to the Senior Information Risk Owner (SIRO).

2.2 Senior Information Risk Owner

The role of Senior Information Risk Owner (SIRO) in the CCG has been assigned to the Chief Finance Officer (CFO). The SIRO takes ownership of the organisation's information risks and act as advocate for information risk to the CCG Governing Body, Executive Committee and Audit Committee by providing written advice on the organisation's information security incident reporting and response arrangements.

2.2.1 Overview

Senior level ownership and understanding of information risk management is vital and ensures a clear link to the overall risk management culture of the organisation. Senior leadership demonstrates the importance of the issue and is critical in obtaining commitment to ensuring information security remains high on the Governing Body's agenda and that resource requirements needed to support this agenda are understood.

The SIRO is expected to understand how the strategic business goals of the organisation may be impacted by information risks and will report on these to the Audit and Risk Committee and the Governing Body.

The SIRO provides an essential role in ensuring that security risks are identified and actions taken to address them. They must also ensure that a framework for managing information incidents and risk is in place, used and understood. They provide leadership and guidance to a number of *Information Asset Owners* (IAO).

The key responsibilities of the SIRO are to:

Ensure the issue of information risk, governance and management are represented at the Governing Body and are taken into account when setting strategic objectives.

- Ensure the Audit Committee and Governing Body are adequately briefed on information risk issues.
- Provide updates to the Audit Committee and Governing Body on the management of information in the organisation, potential risks, and outline the potential impacts on strategic goals.
- Provide a written overview on the organisation's information risks and issues which can be included in the Annual Governance Statement (a mandated section of the CCG's Annual Report) where required.
- Oversee the development of an Information Risk Policy (as an integral part of the organisation's Risk Policy), and a Strategy for implementing the policy within this Information Governance Framework.
- Take ownership of the risk assessment process for information risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control.
- Ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.
- Have oversight of and agree action for identified information risks, providing a focal point for the resolution and/or discussion of information risk issues.

- Fulfil the role as outlined in the current IG suite of policies and associated documentation.
- Review and oversee the information risk assessment process, which contributes to the submission of the IGT, or relevant equivalent.
- Ensure regular updates on the Information Asset Register from the appointed IAOs. Ensure key risks are analysed and incorporated into the Information Risk Register or Risk Register by these staff of the organisation.
- Require annual assurance statements from all IAOs on the identification and management of Assets within their remit.
- Ensure that secondary use of Personal Confidential Data (PCD) is de-identified or pseudonymised, meets legal requirements and that appropriate processes and procedures are in place.
- Ensure that IAOs fulfil their responsibilities and provide assurance on information asset, information flows, information risks and provisions of service that involve Personal Confidential Data.

To fulfill this role, there are a number of activities that the SIRO should undertake:

- Completion of annual strategic information risk management training.
- Undertaking annual SIRO training.
- Ensure that the organisation's Information Risk Policy, as part of the overall Risk Policy, meets requirements, and is embedded in the working practice of the CCG
- Fulfill the functions required of the SIRO in the current IGT or equivalent assurance model, as agreed by the organisation's Governing Body
- Ensure that IAO understand and fulfil their responsibilities and provide assurance on information assets, information flows, information risks and provisions of service that involve PCD consult with CCG colleagues, where required, to promote IG best practice, including the engagement of GP members of the CCG to endorse and promote best practice
- Consult with CCG colleagues, where required, to ensure the appropriate management of IG risks and any incidents, including the engagement of GP members of the CCG to endorse and promote best practice.

Sign-off responsibilities:

The SIRO's sign-off is required on the following:

- Projects, programmes or work-streams that impact on patient or staff information (see Change Control)
- Contracts or service level agreements where patient or staff information is being transferred to another organisation or commercial supplier
- Procurements and/or decommissioning of all systems that hold PCD in any format
- Requirements within the IG Toolkit and overall annual submission.

2.2 Caldicott Guardian

Caldicott Guardians in the NHS ensure a harmonised approach to information management and the protection of patient/service-users' confidentiality. The CCG's Caldicott Guardian is a member of the Governing Body from clinical background.

2.2.1 Overview

The Caldicott Guardian plays a key role in ensuring that the CCG satisfies the highest practical standards for managing patient data, particularly PCD. Acting as the 'conscience' of the CCG, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to share and will advise on options for lawful and ethical processing of information.

The Caldicott Guardian also has a strategic role which involves representing and championing confidentiality, information sharing requirements and issues at senior management level and, where appropriate, across the organisation's overall governance framework. The Caldicott Guardian is supported by the IG Manager.

The Caldicott Guardian role is particularly important in relation to the implementation of the Health and Social Care Information Centre (HSCIC) Standards for PCD, Management in CCG functions and the development of Electronic Social Care Records and Common Assessment Frameworks.

In order to ensure a thorough and robust assurance model, the Caldicott Guardian works alongside the broader Caldicott Function or IG function contributing to the work as required.

2.2.2 Caldicott Guardian Responsibilities

The Caldicott Guardian is expected to:

- Undertake and completes annual training on data protection and confidentiality
- Undertake annual Caldicott Guardian training as required and, where possible, attend events.
- Ensure that the organisation's Data Protection and Confidentiality assurance model is fit for purpose and is reflected in the strategic objectives of the organisation.
- Fulfill the functions required of the Caldicott Guardian in the current IGT or equivalent assurance model as agreed by the organisation's Governing Body.
- Review reports and make recommendations following confidentiality audits carried out within the organisation.

Sign-off responsibilities include:

- Information sharing agreements, or protocols, with support from the IG Manager.
- Proposed routine transfers of patient, or staff, information outside of the UK.
- Projects, programmes or work-streams that impact on patient or staff information.
- Contracts or service level agreements where patient or staff information is being transferred to another organisation or commercial supplier.

Sign off is required on several requirements within the IGT and on its overall annual submission.

2.2.3 Caldicott Function Work Programme

With support from the IG manager, this work programme will:

- Ensure the confidentiality and data protection work programme is successfully co-ordinated and implemented.
- Review reports following data protection audits and making recommendations for the organisation.
- Approve Privacy Impact Assessment for a new processes or changes to existing processes within the CCG.
- Ensure that assurance on confidentiality is developed and delivered including an appropriate and proportionate confidentiality audit
- Oversee compliance with the principles contained within the *Confidentiality: NHS Code of Practice* and subsequent guidance.
- Receive details of any information incidents, near misses or breaches of confidentiality.
- Advise on the Confidentiality and Data Protection Assurance component of the IGT, contributing to the annual assessment.
- Provide routine reports to the Governing Body and/or its relevant committees on Confidentiality and Data Protection issues.

2.3 Information Asset Owners (IAOs)

Designated Information Asset Owners (IAOs) are senior members of staff (Directors and Heads of Departments) responsible for providing assurance to the SIRO that information risks, within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate those risks.

Ownership of assets is related to the position held and remit, rather than an individual. Any handover of responsibilities should be accompanied by a formal handover of information assets, all relevant information, processes and procedures.

IAOs should:

- Ensure all Information Assets within their remit are identified.
- Ensure a complete entry on the Information Asset Register is provided and maintained for each entry.
- Ensure that an up-to-date data flow map is maintained and reviewed on a regular basis for all information assets within their remit.

- Identify, manage and escalate all information security, e.g. dependencies and access control) and information risks as appropriate.
- Understand the information that is held in each asset, how information is updated or removed, who has access, the basis of this access and how information is moved or transmitted.
- Provide an annual statement to the SIRO providing assurance and details of usage of the asset.

These functions can be delegated and co-ordinated with Data Custodians identified for each asset where they are identified and appointed.

IAOs are responsible for ensuring that all new data flows are mapped, appropriately approved and recorded. IAOs should ensure all new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with IG security accreditation, information quality and confidentiality and data protection requirements. For example any new database or collection of personal data (whether staff or patient) is accompanied by a Privacy Impact Assessment which details any actions required for:

- Data Protection registration
- Information provided to patients

IAOs support the IGT assessment, or other assurance model, by conducting work required in a timely and efficient manner. They will also be required to provide evidence relevant to the information assets and flows under their remit.

2.4 Data Custodians

Information Asset Owners can appoint Data Custodians to support in the delivery of their information risk management responsibilities. Data Custodians ensure that policies and procedures are followed, recognise actual or potential security incidents and **take** steps to mitigate those risks, consult with their IAOs on incident management and ensure that information asset registers are accurate and up to date.

Data Custodians for the organisation have been identified as existing post-holders of varying levels of seniority, dependent on the business need of the team.

Data Custodians should be:

- An authorised of the system or asset
- Understand what it allows the business to do.
- Understand how it works and how it is used.

Data Custodians will:

- Support the IG Work Plan and colleagues in recording the flows of information internally and externally to the team.
- Help identify any system, spreadsheet or database that holds personal data.
- Provide details about these assets to help assess risks and dependencies.
- Ensure that access to the Information Asset is appropriately controlled and that there are regular reviews to ensure that appropriate access, procedures and working practice are in place

2.5 NHS South East Commissioning Support Unit IG Team

The NHS South East CSU IG Team will support the CCG SIRO, Caldicott Guardian and IAOs and Data Custodians in delivering assurance on the IG agenda.

Key responsibilities are:

- Develop and maintain comprehensive and appropriate documentation that demonstrates commitment to and ownership of IG responsibilities.
- Ensure that there is top level awareness and support for IG resourcing and implementation of improvements.
- Provide direction in formulating, establishing and promoting IG policies.
- Establish working groups, if necessary, to co-ordinate the activities of staff given IG responsibilities and progress initiatives.
- Ensure annual assessments and audits of IG policies and arrangements are carried out, documented and reported.
- Ensure that the annual assessment and improvement plans are prepared for approval by the senior level of management, e.g. the Board or senior management team in a timely manner.
- Ensure that the approach to information handling is communicated to all staff and made available to the public.
- Ensure that appropriate training is made available to staff and completed as necessary to support their duties.
- Liaise with other internal and external committees, working groups and programme boards in order to promote and integrate IG standards.
- Monitor information handling activities to ensure compliance with law and guidance.
- Provide a focal point for the resolution and/or discussion of IG issues.

Further responsibilities are detailed in the job descriptions of the designated IG Manager and IG Compliance Officer from NHS South East CSU, which provides the IG service for the CCG.

2.6 All Staff

The majority of staff handle information in one form or another. Staff who in the course of their work create, use or otherwise process information have a duty to keep up to date with, and adhere to, relevant legislation, case law and national guidance.

The CCG's policies and procedures will reflect such guidance and compliance with these polices and will ensure a high standard of information governance compliance within the organisation. All staff and officers, whether permanent, temporary, contracted or contractors are responsible for ensuring that they are aware of their responsibilities in respect of information governance.

Breaches of confidentiality may be treated as serious disciplinary incidents which in some circumstances can lead to dismissal. All staff should ensure they are aware of the relevant policies and procedures in respect of any personal information they may process.

3. Accountability and Reporting Structure

3.1 CCG Governing Body

The Governing Body is accountable for ensuring that as a statutory body, it has an effective programme for IG and assurance. Verification of the effectiveness of IG and delivery against objectives is provided by the IGSG. Records of minutes and assurance reports will be submitted to the Audit Committee.

In addition, the Governing Body is accountable for data protection, confidentiality, the registration authority, records management and information lifecycle management across the organisation. It must seek assurance that the required standards are being maintained and that information is managed across the organisation in a secure, efficient and effective manner.

The Governing Body is required to support this strategy by the adequate resourcing and support of those tasked with leading this agenda, as well as staff across the organisation supporting this work. This is in addition to monitoring the delivery of key performance indicators.

3.2 Audit Committee

The Audit Committee has delegated responsibilities for ensuring the delivery and audit of the CCG IG Toolkit submission, which identifies key areas of weakness and strengths to be addressed in the on-going work plans across the IG agenda, and reporting to the Governing Body and Executive Committee on any identified issues.

3.3 Information Governance Steering Group

The CCG's Information Governance Steering Group (IGSG) has delegated authority from the Executive Committee to oversee operational work and work plans across the IG agenda. The

group acts as a focus point for the reporting, investigation and response to information incidents. It is responsible for supporting the Caldicott Function within the organisation, and acts as the Records and Information management group. The IGSG is chaired by the SIRO. It has delegated authority to form working groups to deal with particular IG issues or work streams.

IGSG provides assurance to the Governing Body via both the Executive Committee and the Audit Committee on variance and risk around all of these agendas. It does so in the provision of a regular report, by providing copies of its minutes and actions points, and reviewing its work. Its terms of reference and work plan are signed off by the Executive Committee.

The IGSG is tasked with supporting the IGT assessment by providing guidance, support and information. It must ensure that the strategic objectives of IG align with the IGT as well as serving the broader business needs of the organisatio.

The IGSG provides oversight, guidance and sign-off on a number of work streams:

- Information Assets
- Data Flow mapping
- Information Risk
- Provision of service involving identifiable data
- Information and Data Quality
- IG assurance from Projects
- Information Sharing Agreements and Protocols
- Information Security (both technical and non-technical) Data Protection Notification and Registration
- Consent
- Confidentiality
- IG audit reports
- Investigations into information incidents
- Information Risks identified through incidents and/or associated with assets or as part of a review
- IG Training
- Appropriate content in all contracts (for staffing and commissioned services)

Please see:

- Appendix A: CCG's IG reporting structure/arrangement.
- Appendix B: IGSG Terms of Reference.

4. IG Work Programme

4.1 General IG Work plan

In order to ensure on-going assurance, the CCG will undertake a series of checkpoints each year to ensure regular scrutiny of the use of information. This supports the submission of the IGT and any other assurance model, should it be required. These will be elaborated in more detail but are these key check points.

- Data Flows
- Information Asset Register
- Confidentiality Audit and Staff Survey
- Annual statement of assurance from IAOs to the SIRO

The General 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 CCG will attempt to maintain a quarterly review cycle to ensure appropriate scrutiny.

4.2 Specific IG Work Plan

To meet specific requirements of the assurance framework key tasks and evidence will be sought and evaluated from particular functions and providers. 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 IG Function for the CCG.

5. Information and Communications Technology (ICT) Work Programme

Technical information security issues, operational and strategic authority rests with the Information Communication Technology (ICT) Service Provider – South East Commissioning Support Unit (SE CSU). The ICT Service Provider will ensure that the following key areas are addressed:

A documented Information Security Assurance Plan is developed and shared with the CCG.

- Outline the requirements for assurance, scrutiny and performance monitoring in conjunction with the CCG.
- Identify and report Information Risks related to information security as part of the ICT Risk register.

5.1 ICT Security Responsibilities

The ICT Service Provider (SE CSU) will have a nominated Information Security Officers/Manager) with appropriate duties and resources.

The Information Security Officers/Manager will occupy a key role in the delivery of information security activities, and the responsible individual/s should be tasked with providing advice on all aspects of information security and risk management, utilising either their own expertise or external advice.

The quality of their assessment of information security risks, threats and advice on controls will contribute significantly to the effectiveness of the CCG's information security.

The key responsibilities of the Information Security Officers/Manager are to:

- Draft and/or maintain the currency of the appropriate ICT Security Policies;
- Ensure security accreditation of information systems in line with the organisation's approved definitions of risk;
- Ensure compliance with the information security components of the IG toolkit, contributing to the annual IG assessment;
- Ensure all arrangements for managing information security are effective and aligned with the organisation's Information Security and Risk Policies;
- Provide information security reports to the CCG's senior management (e.g SIRO or equivalent) who has responsibility for Information Governance;
- Develop and maintain an information security assurance plan to ensure the appropriate management and prioritisation of risks;
- Co-ordinate the work of other staff with information security responsibilities;
- Advise the CCG in the development of a network security policies and controls for the secure operation of ICT networks, including remote/teleworking facilities.
- Provide advice and guidance regarding the implementation of controls to mitigate against malicious or unauthorised mobile code.

6. Risk Assessment Management Programme

In conjunction with the ICT Service Provider, the CCG will ensure that a methodical information security risk assessment and management process is in place to identify, implement and manage controls in place to reduce the risk to the organisation's assets. The process will be a comprehensively scoped and formally documented plan/programme that considers the security risks to Personal Confidential Data (PCD), commercially sensitive information and critical Information Assets.

A formal information security risk assessment will be carried out on all information assets to ensure threats and vulnerabilities are mitigated. Consideration will be given to the following areas of risk analysis and risk treatment:

Risk Analysis

Risk analysis steps will include risk identification, risk estimation and risk evaluation. These steps will require:

- Good working knowledge of the information asset scope, structure and its valuation.
- Detailed risk assessment consideration of threats to and vulnerabilities of the asset and its components.
- Impact assessment of likely direct and indirect consequences of loss, damage or disruption to the asset.

Risk Treatment

Risk treatment steps will include risk reduction, risk retention, risk avoidance and risk transfer. These steps will require consideration of:

- Risk assessment results for accuracy and completeness.
- Risk treatment options and their implications.

The CCG's overarching Risk Management Strategy was approved by the Governing Body on 24th April 2015.

A formal information risk assessment and management programme has been documented in the CCG's Information Risk Management Programme. The document was approved by IGSG on 16th July 2015.

7. Managing and Investigating IG and Cyber Incidents

All IG incidents including cyber will be managed in line with the CCG's Information Governance and Cyber Security Incident Management and Reporting Procedures. Nominated IAOs will be involved in the investigated process and CCG IG Manager will provide guidance and support for the investigation.

Categorisation of the Incident will be undertaken in accordance with the Health and Social Care Information Centre (HSCIC) *Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation.*

In addition to the requirements of the Information Incident Management and Reporting Procedures, it is vital to identify what personal confidential data was affected or may be affected in any incident or suspected incident. It is important to quickly recreate what data may have been lost or breached, in order to ensure that the investigation and response is comprehensive and can address the organisation's obligations under the DPA.

Please see the CCG's Information Incident Management and Reporting Procedures further guidance.

7.1 Management of IT Security and Information Security Incidents and Events

The management of Information Security incidents will follow helpdesk procedures for issue resolution and escalation as necessary. The SE CSU ICT Security Manager/IG Manager will advise the SIRO and provide reports on any ICT incident that occurs.

8. Openness

The CCG recognise the need for an appropriate balance between openness and confidentiality in the management and use of information. Information will be defined and where appropriate kept confidential, underpinning the Caldicott principles and the regulations outlined in the Data Protection Act 1998 and Freedom of Information Act 2000.

Non-confidential information about the CCG and their services will be available to the public through a variety of means including the procedures established to meet requirements in the Freedom of Information Act.

8.1 Caldicott 2 Review

The CCG will ensure that, where it holds Personal Confidential Data (PCD) with clear legal basis to do so, the data will be shared with registered and regulated health and social care professionals who have a legitimate relationship with the patient/service user for the purposes of direct patient. Further on guidance Caldicott 2 review (to share or not to share) can be found on the HSCIC website: http://www.hscic.gov.uk/article/3638/Personal-data-access-FAQs

8.2 Resource

The resources available to support the IG Assurance will be outlined in the relevant contract and Service Level Agreement for the provision of the service.

9. Training Mandatory IG Training for all staff

The CCG recognise the importance of an effective training structure and programme to deliver compliant awareness of IG and its integration into the day-to-day work and procedures.

All permanent/temporary/contract staff including lay members will complete the online mandatory training modules within first week of employment, with further training required for managers / team leaders, staff who process personal information, and staff with specific information roles.

In line with the existing contract/SLA responsibility for delivering training programmes in accordance with Training Needs Analysis (TNA) is assigned to NHS South East Commissioning Support Unit (CSU).

10. Auditing and Monitoring Compliance with this Framework

The CCG will use a variety of methods to monitor compliance with the processes in this document, including as a minimum the following two methods:

- **IG Toolkit** – Overall compliance with this framework will be annually through review arrangements for IG required by the IG Toolkit and reported to the Audit Committees and the Governing Bodies.
- **IG Incidents -** Information Governance compliance will be monitored quarterly through the monitoring of reported IG incidents by IGSG.

In addition to the monitoring arrangements described above the CCG may undertake additional monitoring of this framework document as a response to the identification of any gaps, or as a result of the identification of risks arising from the framework prompted by incident review, external reviews or other sources of information and advice.

11. Dissemination and Implementation

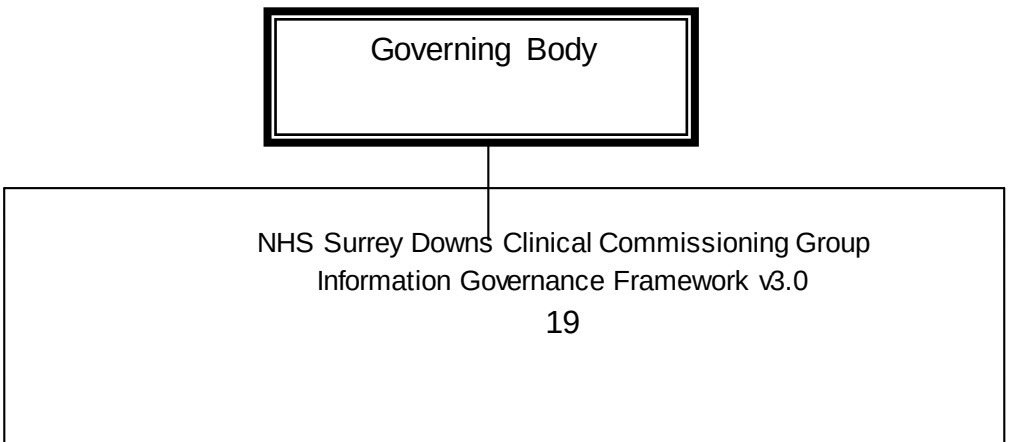
This Framework document will be publicised on the CCG website. Managers are required to ensure that their staff understand its application to their practice. Awareness of any new content/change in process will be through the staff bulletin in the first instance. Where a substantive revision is made then a separate plan for communicating and implementing this change will be devised by the Chief Finance Officer – SIRO or IG Manager.

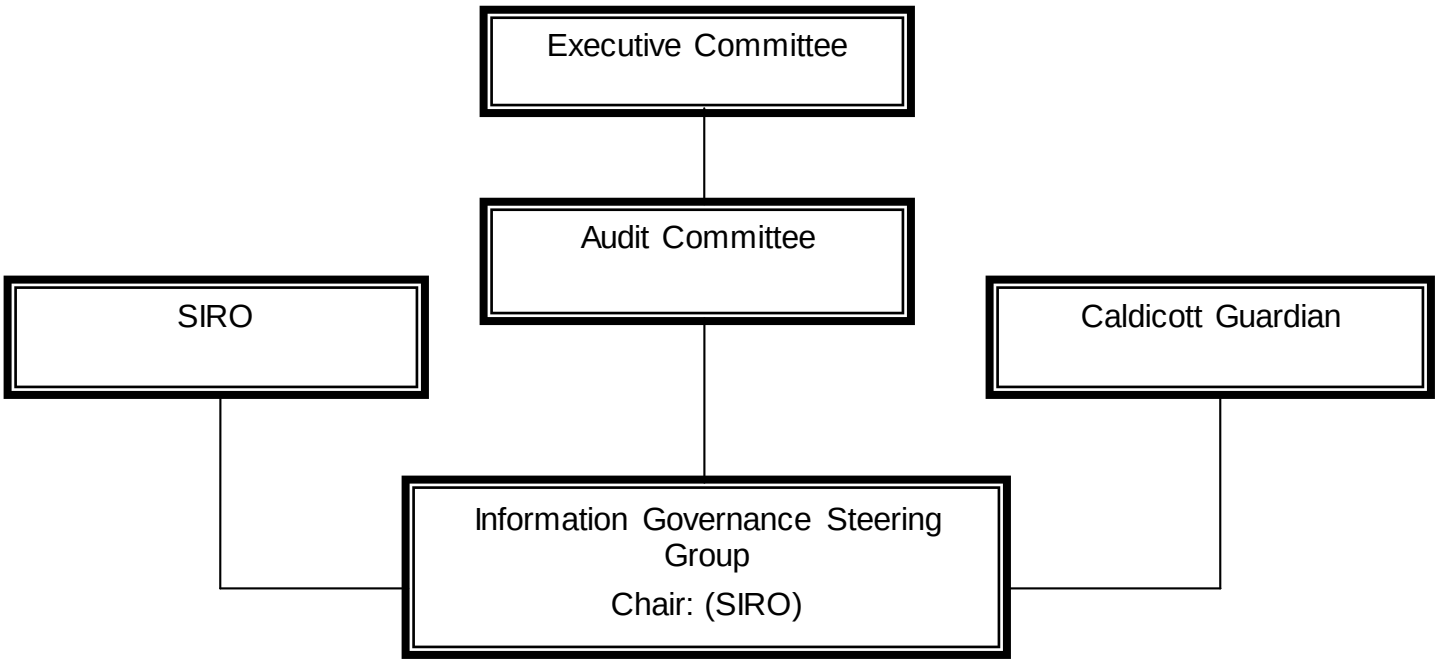
12. Related Documents

The following documentation relates to the management of information and together underpins both CCG's Information Governance Assurance Framework. The Information Governance Framework should be read in conjunction other documents, including, but not limited to:

- Information Governance Policy
- Information Security Policy
- Remote Working Portable Devices Policy
- Subject Access Request Policy
- Data Protection and Confidentiality Policy
- Records Management Policy
- Freedom of Information Policy
- Information Governance and Cyber Security Incident Management and Reporting Procedures

Appendix A: Information Governance Reporting Structure





Appendix B: Information Governance Steering Group - Terms of Reference

1. Purpose

The Information Governance Steering Group (IGSG) is accountable to the CCG Executive Committee and Audit Committee, which in turn report to the CCG Governing Body. The IGSG will oversee the Information Governance processes, systems and practice across the CCG and ultimately provide the Committees with assurance that the organisation is compliant with, and managing any risks to that compliance, through these processes.

These Terms of Reference (ToR) sets out the areas of work for which the group is responsible:

- Confidentiality and Consent
- Data Protection
- Data Quality
- Information Management
- Information Disclosure and Sharing
- Information Security
- Records Management
- Registration Authority

2. Main Responsibilities

- To support the Senior Information Risk Owner (SIRO) to develop and improve the management of information governance in the CCG.
- To support the Caldicott Guardian on Confidentiality and Data Protection, to enable information sharing where it is appropriate to share and advise on options for lawful and ethical processing of information.
- To ensure the information governance vision and strategy for the CCG is in place; to oversee its implementation; and to ensure its currency.
- To provide assurance that the necessary capacity and capability is available to enable policies, procedures and processes to be developed and implemented to deliver the strategy.
- To provide assurance that the CCG undertake or commission sufficient reporting, assessments and audits of information governance policies and operations so as to ensure that their implementation and practice both complies with the written policy and that the outcomes are measured to ensure intended benefits are delivered.
- To review and send reports to members of the Audit Committees; to ensure they remain informed of national and CCG's policy changes, and the results of measurement that demonstrates their effectiveness.
- To liaise with other committees, working groups in order to promote Information Governance and Information Security issues.
- To provide assurance that national development in information governance policy and legislation are monitored and acted on
- To establish a Registration Authority for any Smartcard usage and integrated approach to IG, records management and Registration Authority through developing and maintaining robust and effective procedures, policies, systems and processes that ensure IG is embedded across the organisation.
- To provide the main point of reference and escalation for the management of issues and risks related to information governance, and to ensure IG incidents are appropriately reported and investigated.
- To discuss IG incidents, Information Risks and Asset Registers in order to ensure that relevant issues and themes are adequately addressed.

3. Membership

- Chair – Chief Finance Officer – Senior Information Risk Owner

- Caldicott Guardian
- Governing Body Secretary
- Associate Information Governance Officer (SE CSU)
- CCG Information Manager

The Chair of the IGSG may request the presence of other senior managers/members of staff to assist in addressing any issues.

4. Quorum

The IGSG is quorate when at least three members of the group are present. If members are unable to attend they are required to send a nominated deputy.

Frequency of attendance of members (or their nominated deputies) should be no less than 50% of scheduled meetings. When attendance of an individual member falls below this over an annual period, the issue will be raised with the individual by the Chair, and any steps taken to improve attendance will be taken.

5. Chair

The SIRO will chair the Group. In the absence of the SIRO, the Caldicott Guardian, Governing Body Secretary, Head of Governance and Planning or Information Governance Manager should assume the position of the Chair.

6. Frequency of meetings

The Group will meet meet bi-monthly, although the SIRO may request to hold meetings in between and more frequently as necessary. IGSG meetings will take place immediately before the regular Executive Committee meeting convenes.

7. Reporting arrangements and Accountability

The Group is accountable to the CCG Executive Committee and Audit Committee, which in turn report to the CCG Governing Body.

8. Monitoring and Review

- The IGSG performance will be monitored by the CCG Committees. Regular report will be submitted to these Committees.
- The IGSG will review its Terms of Reference annually or when changes in legislations necessitate a review.
- Once ratified, minutes of all meetings will be circulated to all members and the Audit Committee as required.
- The Chair will report any urgent matters to the Audit Committee or Governing Body as necessary.

- The Chair will present an annual report on the work of the IGSG to the CCG Governing Body.
- Caldicott and confidentiality issues will be reported on, within the IGSG and will form part of the IG steering group's standard agenda items.
- Information quality and records management issues will be reported on within this forum.
- All IG related services provided by the CSU will be reported to this forum as a standard agenda item.

9. Confidentiality

The IGSG minutes of meetings (or sub-sections of them), unless deemed exempt as Part 2 Papers under the **Freedom of Information Act 2000**, shall be made available to the public upon request.

10. Key Links to be maintained by the Committee

Internal

- Accountable Officer and Senior Management Team
- GP Membership Board
- Audit Committee
- Risk Management and Incident Reporting process
- Clinical Governance
- Commissioning
- Performance
- Informatics
- ICT Providers
- Locality teams
- Service managers and staff

External

- Commissioned Acute, Mental Health, Foundation and other NHS Trusts
- Commissioned Any Qualified Providers of Healthcare services
- Commissioned Any Qualified Providers of non-Healthcare services
- Department of Health, Information Governance Policy team
- Health and Social Care Information Centre.
- Information Commissioners Office
- Surrey Information Governance Group
- Information Governance Alliance
- NHS England (National and Regional)