South East London CCG

IG Framework

Document revision history

Date	Version	Revision	Comment	Author
14/01/2020	V0.1	Reviewed and tailored for SEL CCG	Draft	IG Compliance Manager
28/01/2020	V0.2	Further review and update	Draft	IG Compliance Manager
12/02/2020	V0.3	Final draft to go to CCG to complete highlighted sections	Draft	IG Compliance Manager
27/02/2020	V0.4	Draft for SRDG approval, comments removed	Draft	IG Compliance Manager
13/03/2020	V1.0	Document finalised	Final	IG Compliance Manager

Document approval

Date	Version	Revision	Role of approver	Approver
26/02/2020	V1.0	Approved subject to final changes	IGSG	IGSG

Table of 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 NHS South East London Clinical Commissioning Group (hereafter referred to as the CCG). The Framework outlines the roles and responsibilities of those who are tasked with overseeing that IG is appropriately supported, that necessary guidance and advice are available in an effective and efficient manner, and the responsibilities of all staff.

The Framework is based upon the legal requirements of the following:

- Data Protection Legislation (Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679 as referenced in this Act);
- Common law duty of confidentiality;
- Human Rights Act 1998;
- NHS Constitution;
- Department of Health, NHS England and NHS Digital Information Governance assurance regimes; and
- NHS Data Security and Protection Toolkit (DSPT).

This Framework will underpin the IG policies, procedures and processes upon which the CCG relies.

The law allows personal confidential data (PCD) to be shared between those offering care directly to patients, but it protects patients' confidentiality when data about them is used for other purposes. These "secondary uses" of data are essential if we are to run a safe, efficient, and equitable health service. They include:

- reviewing and improving the quality of care provided;
- researching which treatments work best;
- commissioning clinical services; and
- planning of public health services.

People within the healthcare system using data for secondary purposes must only use data that does not identify individual patients unless they have the consent of the patient themselves, or another identified legal basis for the sharing. This may include a lawful basis identified in Articles 6 and 9 of the General Data Protection Regulation, and/or a NHS Act 2006 section 251 exemption.

2. Key Principles

The IG Framework is based on the following key principles:

The CCG will take a privacy (and data protection) by design and default approach to IG using a risk-based methodology for decision making and delivery. The intent and outcomes of the CCG's IG decision

making, and delivery approach shall be to ensure that the benefits to be derived by stakeholders and individuals is greater than the risks the CCG will accept and tolerate. As a commissioner of services, the CCG:

- is 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 IG obligations; and
- ensure any new staff are supported in undertaking relevant and appropriate IG training.

3. Key workstreams overseen by the Information Governance Steering Group

3.1 General IG Work Plan

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 DSPT and any other assurance model, should it be required, for example, for 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;
- Data Security and Protection Toolkit audit exercises for the CCG;
- IG incident reporting and action plan implementation review;
- Governance review; and
- Annual statement of assurance from Information Asset Owners to the SIRO.

These will be quality assured and supported by the IG function in place to support the CCG.

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

3.2 Data Protection Work Programme

The key elements of the CCG's Data Protection Work Programme are to:

- Ensure compliance with all aspects of the Data Protection Act 2018 and related provisions and provide reports, including undertaking audits, to the relevant governance body of the CCG;
- Ensure compliance with the IG 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 input into governance reviews and resulting direct decisions to implement;
- Advise patient and public involvement fairness and transparency strategies;

- Promote data protection awareness throughout the CCG 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 individuals are provided with information on their rights under data protection legislation;
- Assist with investigations into complaints about breaches of the Act; and
- If required, develop and deliver a data protection audit, proportionate and appropriate to the current and evolving requirements of the CCG.

3.3 Data Protection Impact Assessment (DPIA)

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 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 individuals 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.

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.

3.4 Privacy by Design and Default

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

Security areas that should be considered when creating bespoke technology or engaging existing technology are set out in the Information Commissioner's Office (ICO) guidance on Privacy by Design.

3.5 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 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 IG function for the CCG.

3.6 Information and Informatics IG Work Programme

The CCG 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).

3.7 Information and Communications Technology (ICT) IG Work Programme

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

The Director of ICT & IG will lead on the following areas for the CCG:

- Information Security Risk Management and Assurance Plan/Strategy (see section 6.4 below);
- Outline the requirements for assurance, scrutiny and performance monitoring in conjunction with the CCG;
- Lead on key IG schemes to deliver assurance or effect information;
- Identify and report information risks related to information security as part of the ICT Risk register and Information Risk register; and
- Lead on cyber security.

3.8 Change Control

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

3.9 Assurance from Commissioned Services

The CCG will develop an IG assurance framework for its commissioned services in line with expectations from the Department of Health and Social Care and relevant contracts.

Healthcare Providers

Where IG assurance frameworks are not in place, the CCG will negotiate with healthcare providers to ensure that contracts or informal agreements require the healthcare providers to:

- undertake relevant assurance framework (such as the DSPT and CQC Regulations);
- ensure self-assessments are independently audited;
- have any audit report scruntinised by the IG Steering Group; and
- ensure any IG incidents or data losses are escalated to the CCG as commissioner, and provide assurance on the appropriate handling of these issues.

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

Non-Healthcare Providers

For providers of non-healthcare services, the CCG 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 authorities shall be asked to complete an IG 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 CCG.

4. Accountability and Governance Structure

4.1 Overview

Senior management ownership and understanding of information risk management is vital and provides a clear link to the overall risk management approach of the CCG. Senior management involvement and leadership demonstrates the CCG's commitment to ensure compliance with IG requirements and understanding resource implications.

4.2 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) for the CCG is the Chief Operating Officer.

The SIRO is expected to understand how the strategic business goals of the CCG may be impacted by information risks and will report on these to the Integrated Governance and Performance Committee and Governing Body of the CCG, as appropriate.

The SIRO acts as an advocate for the appropriate management of information risks for the Governing Body and in internal discussions, and will provide written advice to the Accountable Officer on the content of the Annual Governance Statement in regard to information risks.

The SIRO provides an essential role in ensuring that information risks are identified and actions taken to address them. They must also ensure that a framework for managing information incidents and risk are in place, used and understood. They will provide leadership and guidance to the organisation's Information Asset Owners (IAOs).

The key responsibilities of the SIRO are to:

- Ensure the issue of information risk, governance and management are represented at the CCG Governing Body and are taken into account when setting strategic objectives;
- Ensure the Integrated Governance and Performance Committee and Governing Body are adequately briefed on information risk issues;
- Provide updates to the Integrated Governance and Performance Committee, Governing Body and Accountable Officer on the management of information in the CCG, potential risks, and outlines the potential impacts on strategic goals;
- Provide a written overview of the CCG's information risks and issues to the Accountable Officer, which is to be included in the CCG's Annual Governance Statement where required;
- Oversee the development of an information risk-related policy as an integral part of the CCG's integrated governance arrangements, and a risk-based strategy for implementing the information risk issues within the CCG;
- Take ownership of the risk assessment process for information risks, including review of an annual information risk assessment to support and inform the Annual Governance Statement;
- Ensure that the CCG's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff;
- To have oversight of and agree on action for identified information risks, providing a focal point for the resolution and/or discussion of information risk issues;
- To fulfil responsibilities as outlined in the current Information Governance Policy, Information Security Policy, Information Quality and Information Management Policy;
- Review and oversee the information risk assessment process, which contributes to the submission of the DSPT, or relevant equivalent;
- Ensure regular updates to the Information Asset Register from the appointed Information Asset Owners;
- Ensure key information risks are analysed and incorporated into the IG Risk Register at SEL CCG level as appropriate; borough level risks to be maintained locally as appropriate in collaboration with the local IG Lead and the IG SMEs.
- Require annual information risk assurance statements from all Information Asset Owners on the identification and management of the information risks of assets within their remit; and
- Ensure that the CCG's use of special categories of personal (confidential) data for secondary use purposes is de-identified or pseudonymised, meets legal requirements and that controlled environments are in place with appropriate technical and organisational controls.

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

- Undertake annual SIRO training;

- Ensure that the CCG's IG related policies, as part of the overall integrated governance arrangements, meet requirements, and are embedded in the working practices of the CCG;
- Fulfil the functions required of the SIRO in any current Data Security and Protection Toolkit or equivalent assurance model, as agreed by the CCG's Governing Body;
- Ensure that Information Asset Owners 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 CCG to endorse and promote best practice; and
- Consult with CCG colleagues, where required, to ensure the appropriate management of IG risks and any incidents, including the engagement of GP members of CCG to endorse and promote best practice.

The SIRO's input and sign off is required on:

- Information/data sharing/handling agreements or protocols;
- Proposed routine transfers of personal data outside of the UK;
- Data protection impact assessments, governance and risk review decision making;
- Project, programme 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 controller/processors or sub-processor organisation;
- Procurement or decommissioning of all systems that hold special categories of personal (confidential) data in any format; and
- Where required, within the Data Security and Protection Toolkit, and on the overall annual submission of the Toolkit.

4.3 Caldicott Guardian

Overview

The Caldicott Guardian must ensure a harmonised approach to information management and the protection of patient confidentiality within the CCG.

The Caldicott Guardian plays a key role in ensuring that the CCG satisfies the highest practical standards for managing special categories of personal data, commonly referred to as personal confidential data (PCD). The post holder acts as the conscience of the CCG, actively supporting work to enable information sharing where it is appropriate to share and advises 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 CCG's overall integrated risk management framework. This role is particularly

important in relation to the implementation of evolving NHS and NHS Digital Standards for PCD management in the CCG and the development of integrated care systems and processes with social care.

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

Responsibilities

The CCG has appointed the Chief Nurse as Caldicott Guardian to oversee the arrangements and sharing of PCD with other bodies. They shall lead the data protection and confidentiality assurance agenda within the CCG.

The Caldicott Guardian shall:

- Undertake annual Caldicott Guardian training as required and, where possible, attend relevant events;
- Ensure that the CCG's data protection and confidentiality assurance model is fit for purpose and is reflected in the strategic objectives of the CCG;
- Fulfil the functions required of the Caldicott Guardian in any current Data Security and Protection Toolkit or equivalent assurance model as agreed by the CCG's Governing Body; and
- Advise and set the scope and specifications for confidentiality audits, governance reviews and data protection impact assessments and consequent decision making that will be proportionate and appropriate for the CCG.

The Caldicott Guardian input and sign off responsibilities shall include:

- Information/data sharing/handling agreements or protocols;
- Proposed routine transfers of patient or staff information outside of the UK;
- Data protection impact assessment and governance review decision making;
- Projects, programmes or work-streams that impact on data relating to individuals;
- Contracts or service level agreements where personal data is being transferred to another CCG or commercial supplier; and
- Several requirements within the Data Security and Protection Toolkit and on the overall annual submission of the Toolkit.

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;
- Provide routine reports to the relevant governance body on confidentiality and data protection issues.

4.4 Data Protection Officer

The Data Protection Officer (DPO) reports to the SIRO and the highest level of management. This ensures the DPO can act independently and without a conflict of interest.

The DPO is responsible for ensuring that the CCG and its constituent business areas remain compliant at all times with data protection legislation, Privacy & Electronic Communications Regulations, Freedom of Information Act and the Environmental Information Regulations (information rights legislation).

The DPO shall:

- Lead on the provision of expert advice to the organisation on all matters concerning the information rights law, compliance, best practice and setting and maintaining standards; and
- Provide a central point of contact for the information rights legislation both internally and with external stakeholders (including the office of the Information Commissioner).

The CCG must ensure that the DPO is consulted on:

- Whether or not to carry out a data protection impact assessment and associated methodology;
- What safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects;
- Whether or not the data protection impact assessment has been correctly carried out and whether its conclusions are in compliance with the GDPR; and
- Data breaches.

4.5 Information Asset Owners (IAO)

All senior management staff i.e. at director level, are required to act as Information Asset Owners (IAO) for the information assets within their remit. They are directly accountable to the SIRO and will provide assurance that information risk is managed effectively for the information assets identified as within their remit.

IAOs are required to identify Information Asset Administrators from among team leaders or managers who have day-to-day responsibility for the use of information assets to support them in this role.

Ownership of information assets shall be 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.

Information Asset Owners shall:

- 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 information flow map is maintained and reviewed on a regular basis for all information assets within their remit;
- Identify, manage and escalate all information security (for example, 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; and
- Provide an annual statement to the SIRO providing assurance and details of usage of the asset.

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

- Data protection registration;
- Information provided to individuals; and
- Managing privacy risks – corporate and individual.

IAOs shall support the Data Security and Protection Toolkit assessment, or other relevant 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.

These IAO functions can be delegated and co-ordinated with Information Asset Administrators identified for each asset where they are identified and appointed.

4.6 Information Asset Administrators

Information Asset Administrators are operational managers, staff and teams who use information assets to do the work of the CCG. They produce the procedures for using them, control access to them and understand their limitations. Each information asset needs at least one administrator which can be either an individual or multiple post-holders.

The Information Asset Administrators for the CCG will be identified depending on the operational roles and responsibilities undertaken on behalf of the CCG.

The Information Asset Administrator shall be:

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

Information Asset Administrators shall:

- Support the IG Workplan and colleagues in recording and risk assessment of the flows of information internally and externally for their work areas;
- Help identify any information asset - system, spread sheet or database that holds special categories of personal data and record on the information asset register;
- Provide the risk context about these assets to help assess risks, dependencies and mitigating controls;
- Ensure that access to information assets are appropriately controlled and that there are regular reviews to ensure that appropriate access, procedures and working practice are in place; and
- Develop and maintain the system level security policies of information assets within their operational control.

4.7 Information Governance Lead

The IG Leads will support the SIRO/Caldicott Guardian and IAOs in delivering assurance on the IG agenda.

Key responsibilities are to:

- 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 coordinate 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;
- Support the development and decision making regarding data protection impact assessment, governance reviews and other related risk-based IG endeavours;
- Support the management and control of IG related incidents;
- Support the development and delivery of fairness and transparency related strategies and actions;

- 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; and
- 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 role from NEL, and the IG Support Officer role, both of which provide the IG service for the CCG.

4.8 All Staff

All those working for the CCG have legal obligations, under data protection legislation, the common law duty of confidentiality, and professional obligations, for example, the Confidentiality NHS Code of Practice and professional codes of conduct. These are in addition to their contractual obligations of adherence to policy, confidentiality clauses in their contract.

All staff are responsible for the maintenance of confidentiality, the protection and appropriate use of special categories of personal data in accordance with data protection legislation. These details are outlined in the contract that all staff are required to sign and adhere to.

4.9 Those Working on the CCG's Behalf:

The same responsibilities in relation to confidentiality and IG apply to those working on behalf of the CCG whether they are volunteers, students, work placements, contractors or temporary employees. Those working on behalf of the CCG are required to sign a third party agreement outlining their duties and obligations**.**

4.10 Clinical Commissioning Group Governing Body

The Governing Body is accountable for ensuring that the CCG has an effective an programme for IG and assurance. Verification of the effectiveness of IG and delivery against objectives is provided by the receipt of minutes and, when required, assurance reports from the IG Steering Group of the CCG and other relevant working groups, as appropriate. The Governing Body receives details of each Data Security and Protection Toolkit submission, which identifies key areas of weakness and strengths to be addressed in the ongoing work plans across the IG agenda.

In addition, the Governing Body is accountable for data protection, confidentiality, the registration authority, records management and information lifecycle management across the CCG. It must seek assurance that the required standards are being maintained and that information is managed across the CCG 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 CCG supporting this work. This is in addition to monitoring the delivery of key performance indicators.

The Governing Body will look for assurance on IG from the CCG IG Steering Group through the Integrated Governance and Performance Committee of the CCG.

4.11 Integrated Governance and Performance Committee

The Integrated Governance and Performance Committee shall have the following duties:

- Ensure a coordinated approach to the information agenda is developed for, and adhered to, throughout the CCG and with contracted service providers;
- Ensure that an 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 IG;
- Scrutinise the effectiveness of strategy and consider and approve policies and procedures across the IG agenda;
- Sign off approved strategies, policies and procedures on behalf of the CCG;
- 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 Integrated Governance and Performance Committee.

4.12 Information Governance Steering Group (IGSG)

The IGSG of the CCG will at agreed intervals submit its minutes, workplan and action points to the Integrated Governance and Performance Committee once approved.

The IGSG provides assurance to the Integrated Governance and Performance Committee on variance and risk around all of these agendas. It will do so 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 Integrated Governance and Performance Committee.

The IGSG will have delegated authority from the CCG Governing Body through the CCG Integrated Governance and Performance Committee to oversee operational work and workplans across the IG agenda. The IGSG of the CCG will act as a focus point for the reporting, investigation and response to information incidents. It is responsible for supporting the Caldicott function within the CCG, and acts as the Records and Information management group.

The IGSG will be chaired by the Senior Information Risk Owner or an appropriate Director of the CCG. The IGSG has delegated authority to form working groups to deal with particular IG issues or work streams.

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

5. Information Incident Reporting

All information incidents (whether involving PCD or not) must be reported to the Senior Information Risk Owner and the CCG IG Leads. Contact details can be found in Annex A. This should happen as soon as the issue is detected.

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.

The report should detail:

- The nature of the incident;
- The information affected and the number of records;
- The behavioural factors that contributed to the incident;
- The potential or actual risk of harm (damage or distress) that is a consequence of the incident;
- The nominated investigating manager and contact point; and
- The learning from the incident.

Incidents should be investigated in accordance with the CCG's Incident Policy and procedure.

5.1. Management of Incidents

Incidents will be managed in accordance with the CCG'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 IG Leads for the CCG will provide guidance and support to the investigation manager.

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

5.2. Investigation of Incidents

In addition to the requirements of the standard investigation procedure, it is vital to identify whether PCD has been or may be affected in any incident or suspected incident. It is important to quickly identify what data may have been lost or breached, in order to ensure that the investigation and response is comprehensive and can address the CCG's obligations under data protection legislation.

Key questions that need to be addressed as part of any investigation, whether this involves PCD or not, are:

- What happened? Did something go wrong? What things went well?
- How did it affect the patient, you, and the business or healthcare process?

- Could it have been avoided?
- Can it be stopped from happening again? What action needs to be taken by whom and when?
- What learning or development need has this highlighted for you (to put into your personal development plan)?
- What learning or personal development need has it highlighted for others?

5.3. Incident Conclusion

Any report on the incident will be provided to the IGSG and escalated as appropriate. These reports will be based on the standard 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 HR.

6. ICT Information Security

6.1. 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.

For technical information security issues, operational and strategic authority rests with the CCG's ICT providers. The CCG has three ICT providers to support the ICT infrastructure across South East London;

- Bexley ICT support services
- Bromley Healthcare CIC IT support service IT
- NEL Commissioning Support Unit

The CCG's ICT providers shall have a nominated Information Security Manager with appropriate duties and resources as follows:

- Bexley ICT support services – Assistant Director of ICT & IG
- Bromley Healthcare CIC IT support service IT - Head of IT for Bromley Healthcare and NHS Bromley CCG
- NEL Commissioning Support Unit – NEL Customer Relationship Manager

The three ICT providers shall work together in a unified approach for ICT services within SE London CCG. The designated Information Security Managers from each of the ICT service provider services will occupy a key role in the delivery of IG activities, and the responsible individual will 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 Manager are to:

- Draft and/or maintain the currency of the appropriate Information Security Policy;
- Ensure security accreditation of information systems in line with the CCG's approved definitions of risk;
- Ensure compliance with the information security components of the Data Security and Protection Toolkit, contributing to the annual assessment;
- Ensure all arrangements for managing information security are effective and aligned with the CCG's Information Security and Risk Policies;
- Provide reports to the senior member of management (e.g. a SIRO/Caldicott Guardian/IAO or equivalent) who has responsibility for IG;
- Provide regular information security risk assurance reports to the information risk lead (SIRO) and, depending upon the supporting structure established, to IAOs and the IGSG (or nominated committee);
- 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;
- Co-ordinate the necessary response and resolution activities following a suspected or actual security incident or breach. Keeping the SIRO and IAOs informed of security incidents, impacts and causes, resulting actions and learning outcomes;
- Assist in the drafting and maintenance of system level security policies;
- Assist in the development of business continuity management arrangements for key information assets;
- Advise in the development of a network security policy 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;
- Assist in designing and configuring access controls for key systems;
- Assist in developing the CCG's information asset register; and
- Develop and document an action plan for the delivery of all specific activities involving information security; and
- Manage the registration and access controls required for Registration Authority services to ensure that individuals who are authorised access to NHS Care Record Services or any of the NHS spine compliant services are done so in line with the National Registration Authority Policy.

The Registration Authority services for South East London CCG will be managed by the SE London ICT Provider (Bexley). RA services for GP practices, optometrist, pharmacist and other specified provider services will continued to be managed by the three ICT providers for their nominated boroughs.

- Bexley (Bexley/Greenwich)
- Bromley Healthcare (Bromley)
- NEL CSU (Lambeth, Southward and Lewisham)

6.2. ICT Information Security Incidents and Events

All information security incidents should be reported to the designated ICT provider service desk upon detection. These should be highlighted to the nominated information security officer for the relevant provider organisation and, where appropriate, to the IG management of the ICT provider organisation. ICT Information Security Incidents include:

- Viruses;
- Inappropriate access to files or folders;
- Use or suspected use of another member of staff's login (for email, network or system) or smartcard;
- Suspected or known disclosure of a smartcard;
- Accidental or intentional damage to the accuracy of data;
- When applications are running slowly;
- Media/advertising Pop-Ups;
- Use of unencrypted laptops, USB sticks;
- Leaving smartcards unattended;
- Unattended IT Assets (laptops, USB sticks, etc.); and
- Accidental or deliberate inappropriate disclosure of confidential information through any means, electronic or hard copy.

The helpdesk will advise of any additional steps that are required, including initiating policy and procedure as outlined in the relevant Serious Incident and Investigation Policy and Procedure.

6.3. Management of IT Information Security Incidents and Events

The management of information security incidents will follow the CCG's ICT provider helpdesk procedures for issue resolution and escalation as necessary. The nominated Information Security Officer will advise the IG Leads or SIRO as appropriate for further guidance.

6.4. ICT Information Security Risk Management and Assurance Plan / Strategy

To ensure that there is effective implementation of information risk processes, the CCG'S ICT providers will work together to 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 CCG. Each risk will be clearly scoped, systematic and seek to identify, quantify and prioritise the information risks to the CCG's business functions. Consideration should also be given to information risks that may affect the CCG's 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 engage a Plan, Do, Check and Act cycle as follows:

- Risk Identification;
- Risk Analysis;
- Risk Treatment; and
- Risk Review.

7. Staff Awareness and Training

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

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

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

7.1 Training

All staff, including volunteers, students, contractors and temporary employees are required to complete and pass IG 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 IG training programme will be provided, which is mandatory for all staff.

The online IG 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 IG assurance framework as outlined by the Department of Health and Social Care, NHS England and NHS Digital.

7.2 Training Needs Assessment

A full IG Training Needs Assessment will be reviewed and approved by the IGSG of the CCG. This will address the expected training for staff at all levels of the CCG and those that are working within particular specialities.

7.3 Resources

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

8. Monitoring and Compliance

This framework and the associated controls; policies, protocols, procedures; will be monitored through the risk management system for the CCG. The IG 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 IG workplan.

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.

9. 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.

10. Implementation and dissemination of document

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 also be published on the CCG's intranet.

11. Further Reading / References

CCG

Suite of Information Governance policies

Subject Access Request procedure

Incident Reporting procedure

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 R//esearch 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

The Data Protection Act 2018

Contact Details for Key Post Holders: As of [insert date]

Role	Post Holder	Email	Telephone
CCG Information Governance Lead	Director of ICT & Information Governance	nisha.wheeler@nhs.net	0208 658 6195
Information Governance Lead (NEL team)	Xx	xx	xx
Information Governance Lead (Bexley)	Alison Pryor	alison.pryor@nhs.net	020 8298 6008
Senior Information Risk Owner (SIRO)	Christina Windle	christina.windle@nhs.net	
Caldicott Guardian	Kate Moriarty-Baker	kate.moriarty-baker@nhs.net	
Data Protection Officer	NEL Head of IG	nelcsu.dpo@nhs.net	03000 428438

Current NEL Key Post Holders

Role	Post Holder	Email	Telephone
Senior Information Risk Owner (SIRO)	Richard Wells	richard.wells2@nhs.net	
Caldicott Guardian	Anna Dorothy	annadorothy@nhs.net	
Data Protection Officer	NEL Head of IG	nelcsu.dpo@nhs.net	03000 428438