NHS
Merton
Clinical Commissioning Group

Report to the Merton Clinical Commissioning Group Governing Body

Date of Meeting: 23rd January 2014

Agenda No: 7.5 **Attachment:** 18

Title of Document: Information Governance Framework	**Purpose of Report:** To receive and note
Report Author: Andrew Bromley – CSU/ MurraeTolson	**Lead Director:** Cynthia Cardozo
Contact details: Murrae.tolson@mertonccg.nhs.uk	
Executive Summary: The information governance framework provides a solid basis upon which Information Governance (IG) and all its component parts will be implemented throughout the MCCG. The framework outlines the roles and responsibilities of those who are tasked with over-seeing 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, Common Law Duty of Confidentiality and Human Rights Act and the Department of Health's (DH) assurance regime; the information governance toolkit (IGT). This framework will underpin the organisation's IG policies, protocols and procedures upon which the organisation relies in its duties to provide and support the business of MCCG.	
Key sections for particular note (paragraph/page), areas of concern etc: Whole document	
Recommendation(s): Note whole document	
Committees which have previously discussed/agreed the report: Information Governance Steering Committee and Audit Governance Committee	
Financial Implications: Data breaches could result in a fine of £1m or more.	
Other Implications: (including patient and public involvement/Legal/Governance/ Risk/ Diversity/ Staffing) N/A	
Equality Analysis: N/A	
Information Privacy Issues: N/A	
Communication Plan: (including any implications under the Freedom of Information Act or NHS Constitution) To be added to intranet and is currently part of IG training staff are receiving.	

Information Governance Framework

Document control

Document Information

Document Name:	Information Governance Framework		
Location:			
Consultation:	SIRO and Merton CCG EMT		
Approved by:	Merton CCG	Date:	
Supersedes:	DRAFT 0.2		
Description:	Information Governance Framework noting assurance model, roles and responsibilities.		
Audience:	All Merton CCG staff		
Contact details:			

Change History

Version	Date	Author	Approver	Reason
0.1	4.02.13	Glyn Jones		
0.2	17.9.13	Murrae Tolson	Cynthia Cardozo	Revisions
0.2.1	11.10.13	Andi Scott - SLCSU		Revisions
0.2.2	14.01.13	Andrew Bromley - SLCSU		Revisions

Contents

1.0 Introduction

Merton Clinical Commissioning Group (MCCG) has prepared this information governance framework document for the purpose of supporting Information Governance (IG) within the organisation and for all staff working in, or on behalf of, the organisation.

The information governance framework provides a solid basis upon which IG and all its component parts will be implemented throughout the MCCG. The framework outlines the roles and responsibilities of those who are tasked with over-seeing 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, Common Law Duty of Confidentiality and Human Rights Act and the Department of Health's (DH) assurance regime; the information governance toolkit (IGT).

This framework will underpin the organisation's IG policies, protocols and procedures upon which the organisation relies in its duties to provide and support the business of MCCG.

Key Principles

The following key principles are reflected in this paper:

- Any staff appointed will be required and be supported to undertake 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 Clinical Commissioning Group must seek assurance that these organisations are meeting their IG obligations.

2.0 Roles and Responsibilities

2.1. Senior Information Risk Owner (SIRO)

1.1.1. 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 agenda of the Executive Management Team (EMT) and that resource requirements needed to support this agenda are understood.

The Senior Information Risk Owner (SIRO) for the organisation is the Chief Finance Officer.

1.1.2. Responsibilities

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 EMT and the Governing Body.

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

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

The key responsibilities of the SIRO are to:

- Ensure the issues of information risk, governance and management are represented at the Governing body and are taken into account when setting strategic objectives.
- Ensure the EMT and Governing Body is adequately briefed on information risk issues.
- Provide updates to the EMT, Governing Body and Accountable Officer on the management of information in the organisation, potential risks and outlines the potential impacts on strategic goals.
- Provide a written overview on the organisation's information risks and issues to the Accountable Officer which is included in the annual Internal Audit Control Assurance 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 IG 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.
- To have oversight of, and agree action for, identified information risks, providing a focal point for the resolution and/or discussion of information risk issues.
- To fulfil the role as outlined in the current IG Policy, Information Security Policy and Risk Management Strategy.
- Review and oversee the information risk assessment process, which contributes to the submission of the IG Toolkit, or relevant equivalent.
- Ensure regular updates on the Information Asset Register from the appointed Information Asset Owners.
- Ensure Key risks are analysed and incorporated into the Information Risk Register or Risk Register by the staff of the organisation.
- Require annual assurance statements from all Information Asset Owners on the identification and management of Assets within their remit.
- Ensuring that secondary use of patient identifiable data is de-identified or pseudonymised or meets legal requirements, that new safe havens are in place with appropriate process and procedure.

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

- Undertake and complete annual strategic information risk management training.
- Undertake 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 Clinical Commissioning Group.
- Fulfil the functions required of the SIRO in the current Information Governance Toolkit or equivalent assurance model, as agreed by the organisation'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.
- 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.

Sign off responsibilities include:

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

- Information sharing agreements, or protocols.
- Proposed routine transfers of patient or staff information outside of the UK.
- 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 organisation or commercial supplier.
- The SIRO must sign off the procurement or decommissioning of all systems that hold Personal Confidential Data (PCD) in any format.
- Sign off is required from the SIRO on several requirements within the IGT and on the overall annual submission.

2.2. Caldicott Guardian

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

2.2.1. Overview

The Caldicott Guardian plays a key role in ensuring that the organisation satisfies the highest practical standards for managing patient data, particularly Patient Identifiable Data (PID) or PCD. The post holder acts as the conscience of the organisation and actively supports 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 organisation's overall governance framework. This role is particularly important in relation to the implementation of the National Programme for IT 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. Responsibilities

The organisation has appointed the Director of Quality as the Caldicott Guardian to oversee the arrangements and sharing of PCD with other bodies. They are expected to lead the data protection and confidentiality assurance agenda within the Clinical Commissioning Group.

The Caldicott Guardian is expected to:

- Undertake and complete 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.
- Fulfil the functions required of the Caldicott Guardian in the current IGT or equivalent assurance model as agreed by the CCG's Governing Body.
- Ensure the scope and specifications for a confidentiality audit that is proportionate and appropriate for the organisation has been agreed
- Ensure that Information Asset Owners fulfil their responsibilities and provide assurance on information assets, information flows, information risks and provisions of service; that involve PCD.

Sign off responsibilities include:

- Information sharing agreements, or protocols.
- 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 the overall annual submission of the Toolkit.

2.3. Information Asset Owners (IAO)

All senior staff at Director, Executive or Head of department level are required to act as Information Asset Owners 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 may appoint an Information Champion to assist them in fulfilling this obligation. IAOs are required to identify Information Asset Administrators (IAA) 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 assets is related to the position held and remit, rather than an individual. Any hand-over of responsibilities should be accompanied by a formal hand over of information assets, all relevant information, protocols and procedures.

Information Asset Owners must:

- 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 an annual 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.
- 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 Information Asset Administrators 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 must ensure all new processes, services, information systems and other relevant information assets are developed and implemented in a secure and structured manner. The Information Assets should comply with IG security accreditation, information quality, 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. Information Asset Administrators (IAO)

IAOs are senior managers and teams who use information assets to do the work of the organisation. They produce the procedures for using the assets, control access to them and understand their limitations. Each Information Asset needs an administrator which can be either an individual post-holder or a team.

The Information Asset Administrator should be:

- A senior user of the system or asset
- Understand what it allows the business to do
- Understand how it works and how it is used

Information Asset Administrators will:

- Support the IG Work plan and colleagues in recording the flows of information internally and externally to the team.
- Help identify any system, spread sheet 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. Information Governance Lead

The IG lead will support the SIRO/Caldicott Guardian and IAOs 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 Governing Body or EMT 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 description of the designated IG Manager from South London Commissioning Support Unit, which provides the IG service for MCCG.

3.0 IG Work Programme

3.1. General IG Work plan

In order to provide 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 are:

- Data Flows (mapped and reviewed)
- Information Asset Register (review)
- Information Risks
- Confidentiality Audit and Staff Survey
- Review
- Annual statement of assurance from Information Asset Owners to the SIRO

These will be quality assured by the Information Governance Function and will be subject to audit in line with expected standard.

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 seek to maintain a quarterly review cycle to ensure appropriate scrutiny.

3.2. Specific IG Work programmes

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.

3.3. Caldicott Function work programme

This work programme will:

- Ensure the confidentiality and data protection work programme is successfully co-ordinated and implemented.
- Ensure that assurance on confidentiality is developed and delivered including an appropriate and proportionate confidentiality audit.
- Ensure compliance with the principles contained within “Confidentiality: NHS Code of Practice” and subsequent 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 Information Governance Toolkit, contributing to the annual assessment.
- Provide routine reports to the relevant governance body on Confidentiality and Data Protection issues.

3.4. Data Protection Work Programme

The key elements of the Data Protection Work Programme are:

- Ensure compliance with all aspects of the Data Protection Act and related provisions and provide reports, including undertaking audits, to the relevant governance body of the organisation.
- Draft and/or maintain the currency of the Data Protection policy.

- Promote data protection awareness throughout the organisation 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.
- 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 organisation.

3.5. Information and Informatics IG Work Programme

The Clinical Commissioning Group will appoint or ask, where appropriate, the provider of 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 on, as appropriate, the use of pseudonymisation on and anonymisation techniques
- Identify and report Information Risks related to the secondary use of patient data for key business functions (such as commissioning, performance and informatics).

3.6. Information and Communications Technology (ICT) IG Work Programme

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

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

- Information Security Assurance and appropriate work-plan
- Outline the requirements for assurance, scrutiny and performance monitoring in conjunction with the CCG
- Lead on key IG schemes to deliver assurance for effect information security.
- Identify and report Information Risks related to information security as part of the ICT Risk register and Information Risk register

3.7. Change Control

In addition to the IG related to these functions, IG will ensure that its requirements are included within the change control processes and systems within the organisation and those that provide services to it.

3.8. Assurance from commissioned services

The CCG will develop an assurance framework from commissioned services in line with expectations from the Department of Health and relevant contracts. Where not in place, the CCG will negotiate to ensure:

3.8.1. Healthcare Providers

For healthcare providers, the CCG will look to ensure that contracts or informal agreements ensure that:

- The Healthcare provider undertakes relevant assurance model (such as the IGT and CQC Regulations)
- Any self-assessment is independently audited
- That the audit report is scrutinized by the EMT
- That any incidents, near misses or data losses are escalated to the CCG as commissioner and assurance is sought 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

3.8.2. 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 or tools, such as the CSU, will be asked to complete an Information Governance Assurance model, such as the IGT.

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 an organisation 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.

4.0 Key Policies

- The following written controls will be provided for staff working for the Clinical Commissioning Group.
- Information Governance strategy
- Information Governance policy
- Data Protection Protocol
- Confidentiality Code of Conduct
- Information Security Policy
- Information Management Policy
- Freedom of Information Protocol
- Corporate Governance Protocol
- Risk Management Strategy and protocol

4.1. Policy, Protocol and Procedure Distribution

All policies, protocols and procedures will be made available on the Clinical Commissioning Group intranet or equivalent system and will be highlighted in the staff briefing and via briefings to teams provided by the IG team.

Knowledge of the key details will be tested through the use of the online IG training tool (https://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm), with the use of staff surveys to test knowledge in particular areas and other training methods (e.g. face-to-face sessions etc.)

5.0 Clinical Commissioning Group Governing Body

The Governing Body is accountable for ensuring that, as a statutory body, the CCG has an effective 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 EMT and the other relevant working groups, as appropriate. The Governing Body receives details of each IGT submission, which identifies key areas of weakness and strengths to be addressed in the on-going work plans across the IG agenda.

In addition, the Governing Body is accountable for data protection, confidentiality, the Registration Authority (RA – provision and control of Smartcards,) 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 the IG 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. It is recommended that the EMT appointments a Records Management champion from amongst its members to supplement the work of the SIRO and Caldicott Guardian and to lead on this agenda.

The IG Steering Group (IGSG) will, at agreed intervals, submit its minutes, work plan and action points to the Governing Body once approved. It provides assurance to the Governing Body on variance and risk around all of these agendas. Its terms of reference and work plan are signed off by the Governing Body.

The IGSG has delegated authority from the Governing Body to oversee operational work and work plans across the IG agenda. The IGSG acts as a focal 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 who receives all papers and can chair or convene additional meetings as required. 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 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 organisation.

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

- Information Assets
- Data Flow mapping
- Provision of services involving PID or PCD
- Information and Data Quality
- IG assurance from Projects (including Privacy Impact Assessments)
- Information Sharing Agreements and Protocols
- Information Security (both technical and non-technical)
- Data Protection Notification and Registration
- Consent, confidentiality
- Investigations into information incidents
- Information Risks identified through incidents and/or associated with assets or as part of a review

The IGSG forms the assurance and scrutiny group for the following and can convene separate working groups.

- Caldicott and confidentiality issues
- Data Protection
- Information sharing and processing
- Registration Authority
- Records Management

Key Work streams overseen by the Information Governance Steering Group

The steering group will oversee the following key work streams in IG Assurance. They include:

- To establish an active and integrated approach to IG, records management and Registration Authority through developing and maintaining robust and effective procedures, protocols, and systems that ensure IG is embedded across the organisation.
- To co-ordinate the organisation's response to the IGT or other assurance model, to meet the relevant deadlines.
- Set out mandatory and non-mandatory IG training requirements and ensure that they are implemented and adhered to.
- Ensure that the statutory bodies comply with law, statute and other IG requirements, such as those identified and set by the DH.
- Support the work of the SIRO and Caldicott Guardian, as well as Information Asset Owners, Information Governance Lead and Information Asset Administrators.
- Provide a forum for the scrutiny of the IG framework and assurance model across the CCG as statutory body and its key services providers.
- Review information incidents and information security incidents and report output to the EMT. These include information and data quality, as well as records management and record-keeping.
- Support Records Management and Records Standards within the Clinical Commissioning Group.

The IGSG will also provide a forum for all hosted and partner organisations as necessary.

6.0 Information Incidents

6.1. Reporting Information Incidents

All information incidents must be reported to the Caldicott Guardian and the Information Governance Lead. Contact details can be found in Annexe A. This should happen as soon as practical after 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.)
- Patient Identifiable Data sent to the wrong individual.

The report should detail:

- The nature of the incident.
- The information affected and the number of records.
- The nominated investigating manager and contact point.

The incident should be investigated in accordance with the relevant Serious Incident and Investigation protocol and procedures.

6.2. Information Security Incidents and Events

All information security incidents should be reported to the relevant ICT Helpdesk upon detection. These should be highlighted to the nominated information security officer for the relevant organisation and, where appropriate, to the Information Governance Manager.

Information Security Incidents include (this is not an exhaustive list):

- Viruses.
- Inappropriate access to files or folders.
- Use, or suspected use, of other member of staff's login (for email, network or system) or smartcard.
- Suspected or known disclosure of your smartcard PIN.
- Accidental or intentional damage to the accuracy of data.
- Slow computers.
- Pop-Ups.
- Use of unencrypted laptops and USB sticks.
- Leaving smartcards unattended.
- Unattended IT Assets (laptops, USB sticks, etc.)

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 Incidents

Incidents will be managed in accordance with the Incident and Investigation Protocol and Procedures. All information incidents will be investigated by the relevant manager or, if not appropriate, by a manager nominated by the nominated Director or Information Champion. The Information Governance Lead will provide guidance and support to the investigation manager.

Categorisation of the incident will be undertaken in accordance with the standard protocol and procedure.

6.4. Management of Information Security Incidents and Events

The management of Information Security incidents will follow 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. Incidents of theft and burglary are to be reported through the same Incident Policy protocols and procedures.

6.5. Investigation of Incidents

In addition to the requirements of the standard Investigation Procedures, it is vital to identify what personal identifiable 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 Data Protection Act.

Key Questions that need to be addressed as part of the investigation:

- 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?

6.6. 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.

7.0 Information Security

7.1. Responsibility for 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 South London Commissioning Support Unit as the ICT provider. The provider has a nominated Information Security Manager with appropriate duties and resources.

The Information Security Manager occupies a key role in the delivery of IG activities and the responsible individual 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 organisation's information security.

The key responsibilities of the Information Security Manager are to:

- Draft and/or maintain the currency of the appropriate Information Security Protocols;
- 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 IGT, 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 Protocols;
- Provide regular information security risk assurance reports to the SIRO) and to Information Asset Owners (IAOs) for use by the Information Governance Steering Group;
- 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 protocol 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 organisation's Information Asset Register;
- Develop and document an action plan for the delivery of all specific activities involving the Information Security agenda.

7.2. Information Security Assurance Plan and Strategy

To ensure that there is effective implementation of Information Risk processes, the organisation will provide a comprehensively scoped and formally documented plan and programme. This 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, e.g. care, the protection of personal data 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 organisation. Each risk will be clearly scoped, systematic and seek to identify, quantify and prioritise the information risks to the organisation's business functions. Consideration should also be given to information risks that may affect the organisation's business partners. Where appropriate, controls (counter measures) should 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:

- Risk Analysis
- Risk Treatment

8.0 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.

9.0 Responsibility and Accountability

9.1. All staff

All those working for the CCG have legal obligations, under the Data Protection Act, common law of confidentiality; and professional obligations, for example the Confidentiality NHS Code of Practice and professional codes of conduct.

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

9.2. Those working on behalf of MCCG

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

10.0 Training

All staff are required to complete and pass appropriate IG training on an annual basis. This can be achieved by passing the DH provided online IG Training Tool (IGTT) or by face-to-face sessions. Staff with specific roles, such as the SIRO and Caldicott Guardian, are required to undertake annual training specifically aimed at these roles.

The current training requirements are outlined as follows, and will be updated when there are changes to the IG assurance framework outlined by the DH. Managers are required to ensure staff have provided them with proof that they have passed their training and are asked to ensure a copy of the relevant certificate is kept on the member of staff's personnel file.

10.1. Training Needs Assessment

A full IG Training Needs Assessment will be reviewed and approved by the IGSG. This will address the expected training for staff at all levels of the organisation and those that are dealing with particular issues.

11.0 Intranet and Communications

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
- Records Management

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

12.0 Annexes

Annexe A - Key Post Holders

Annexe B – Key Legislation and Guidance

Annexe A – Key Post Holders

Contact Details for Key Post Holders

As of 01/10/2013

Role	Post Holder	Email	Telephone
Governing Body IG Lead	Cynthia Cardozo	Cynthia.Cardozo@mertonccg.nhs.uk	
Senior Information Risk Owner (SIRO)	Cynthia Cardozo	Cynthia Cardozo@mertonccg.nhs.uk	
Caldicott Guardian	Jenny Kay	Jenny.Kay@mertonccg.nhs.uk	

Current South London Commissioning Support Unit

Role	Post Holder	Email	Telephone
Senior Information Risk Owner (SIRO)	Debbie Turner	debbie.turner9@nhs.net	07918703062
Caldicott Guardian	Dr Bruce Websdale	bruce.websdale@nhs.net	020 8812 7700
Information Governance Lead	David Stone (Interim Head of IG)	david.stone5@nhs.net	07947052704

Annexe B – Key Legislation and Guidance

Legislation

Access to Health Records Act 1990

Computer Misuse Act 1990

Data Protection Act 1998

Fraud Act 2006

Freedom of Information Act 2000

Human Rights Act 1998

NHS Act 2006

Health and Social Care Act 2012 (https://www.gov.uk/government/publications/health-and-social-care-act-2012-fact-sheets)

Regulation of Investigatory Powers Act 2000

Common Law Duty of Confidence

NHS Guidance

NHS Codes of Practice

Confidentiality (2003)

Information Security

Records Management

NHS Care Record Guarantee

NHS Constitution

Other Guidance

Information Commissioners Office (www.ico.org.uk)

British Medical Association (www.bma.org.uk)

Industry Standards

ISO 27001 Information Security Management Systems