South West London CCG
Information Security Policy

Document revision history

Date	Version	Revision	Comment	Author/Editor
03/10/2018	V0.1	Draft GDPR compliant document created	Draft	Head of Information Governance
25/10/18	V0.1	Review of changes	Final	Senior IG Hub Manager
03/01/2020	V1.0	Review and tailor for SWL CCG	Draft	IG Compliance Manager
30/01/2020	V1.1	Reviewed and updated following further review	Draft	IG Compliance Manager

Document approval

Date	Version	Revision	Role of approver	Approver

Contents

1.0 Introduction

This policy sets out the intentions of NHS South West London Clinical Commissioning Group (hereafter referred to as 'the CCG') to manage all the information within its remit to the standards required by law and regulation. In doing so, it supports high quality commissioning and healthcare, through accurate, accessible and appropriately governed information. The CCG has put this policy in place to ensure staff are fully aware of their information security responsibilities.

This document uses definitions provided by the Cabinet Office. The Cabinet Office defines data as 'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation' and information as 'output of some process that summarises interprets or otherwise represents data to convey meaning'. This definition will be used throughout this document. All references to information in this document encompass information and data. This includes information which is personal, financial or falls within any other category. The CCG uses information to support the commissioning and management of commissioning of healthcare for patients. Information is also used to support the administration of the NHS. In addition to these functions are requirements of NHS England and NHS Digital (NHSD) which form the wider governance structure that the CCG operates within.

This policy will set out the objectives and framework for the management of information within the CCG to ensure its security, maintaining its confidentiality, integrity and availability. This includes meeting our obligations under Data Protection Legislation (Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679 as referenced in this Act – identified in this documentation as the Data Protection Legislation) to those we hold information about, supporting the ongoing development of the organisation and ensuring that innovation supports our organisation's development without undermining the security of the information we hold. The NHS and the administration of the NHS is dependent on the appropriate use of Personal Data; the management of secondary use of this data and business sensitive data.

The CCG recognises that effective information management is fundamental to good administration and operational effectiveness, and is an enabler to the achievement of strategic goals.

This policy is part of the suite related to Information Governance which set out the expected standards and controls around its use. They are: Information Governance, Information Quality, Information Management and Information Security. The overarching document which sets out the CCG's approach to Information Governance is the Information Governance Framework. The concepts and standards are interrelated. It is important to consider all our obligations and intentions across the suite of policies.

This policy is intended to identify the CCG's intentions related to the organisational implications of information security, policies related to operational and technical implementation of Information Security requirements are documented in the suite of ICT policies for the CCG.

2.0 Scope

This policy is applicable to:

- All information held and processed by the CCG. All information must be managed and held within a controlled environment and to a standard of accuracy and completeness. This includes personal

data of patients and staff, patient level data (non-identifiable) as well as corporate information. It applies to records, information and data regardless of format, in addition to legacy data held by the organisation;

- All information processed by NEL, provider of the CCG's commissioning support services including ICT and IG services;
- The standards expected from services commissioned by our organisation for healthcare and non-healthcare purposes;
- All permanent, contract or temporary staff of the CCG and all third parties who have access to the CCG premises, systems or information. Any reference to staff within this document also refers to those working on behalf of the organisation on a temporary, contractual or voluntary basis;
- Information systems, data sets, computer systems, networks, software and information created, held or processed on these systems, together with printed output from these systems; and
- All means of communicating information, both within and outside the organisation and both paper and electronic, including data and voice transmissions, emails, post, fax, voice and video conferencing. The CCG also believes that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of information governance as a designated corporate function.

3.0 Purpose

This document defines the information security principles and objectives for the CCG. It outlines the systems that ensure current information security obligations are met, how changes, performance and incidents are governed. This document sets the policy, stating the required standard.

Information is an asset that, like other important business assets, is essential to business and needs to be suitably protected. Its security must be maintained to the standards expected in law, regulations and contracts. The standard for the public sector is mandated by the Cabinet Office. It supports the confidentiality, integrity and availability of the information held, processed and the responsibility of the organisation. It is supported by an assurance process that demonstrates the ongoing management of the security of information, the associated risk and the process of change to ensure the correct controls are in place.

ISO/IEC 27002:2013 describes information security and information in the following terms, which set the remit and principles behind this policy and related controls:

"Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities."

The CCG will achieve information security by the implementation, monitoring and improvement of suitable controls.

The CCG is responsible for driving improvements in Information Governance from these services and monitoring their management of risks associated with information security and any failures to maintain standards of information security. This ensures an efficient, effective and accountable service supporting high quality healthcare and appropriate clinical decision making. In those instances where we appropriately share or publish information we must ensure that this is done in a lawful and secure manner.

3.1 Objectives

This policy sets out the CCG's objectives and principles for ensuring the security of information within its remit and identifies the risks, priorities and resources required to ensure information security management is carried out to the appropriate standard.

The CCGs key objectives in relation to information security are to maintain and improve:

- Confidentiality - Access to Information is confined to those with appropriate authority and a legitimate relationship to it.
- Integrity – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- Availability - Information shall be available and delivered to the right person, at the time when it is needed.
- Accountability – Users are held responsible for their use of information.

To achieve this, the policy sets out:

- The organisation's information security obligations;
- The key areas of control and management of risk for information security across the organisation;
- How the organisation will assess where information security impacts on business processes and how assurance is provided;
- The expectation on the management of Information Assets, ICT systems and information to deliver information security and assurance; and
- The responsibilities of staff in maintaining Information Security

The primary aims of information security are to:

- Ensure the confidentiality, integrity and availability of information within SWL CCG
- To reduce the risk of a security breach, data loss or breach of confidentiality
- To understand where risks to information security originate, what issues that arise and the management of those risks
- To protect information assets from threats, both internal and external.

4.0 Definitions

See Annexe A for definitions not defined at the point of use.

5.0 Responsibilities

The Information Governance Framework sets out the core roles and responsibilities of individuals within the CCG. The responsibilities outlined below are specifically in relation to Information Security.

ICT Security Manager
The ICT Security Manager is responsible for the implementation of information security, this role includes:

- monitoring and reporting to the effectiveness of information security;
- ensuring compliance with legislation, including the review and update of this policy;
- review and update of all ICT security policies, protocols and procedures;
- ensuring that relevant staff are aware of their security responsibilities;
- Ensuring that a log of security incidents is maintained and reported to the Information Governance Group.

6.0 Information Security Assurance

6.1 Objectives

Several key Information Services are commissioned from NEL which play a crucial part in maintaining information security for the CCG. This includes Information and Communications Technology ("ICT"), Business Intelligence, Information Governance as well as physical security requirements for our equipment on our premises. NEL is contracted to provide the required standards of security, including assurance and the ongoing management of associated risks.

The CCG works within a framework of written controls, risk management and systems to monitor and provide assurance. Scrutiny of these functions will be undertaken by the CCG as detailed in the relevant service specific policies, procedures and contracts in line with the Accountability and Responsibility detailed within this policy. It is expected that routine reports and evidence of the controls in place will be provided to our customers, in a timely and appropriate manner. This will need to be in line with relevant assurance processes such as audit, the requirements of the Data Protection and Security Toolkit and risk management.

6.2 Overview

The CCG uses several mechanisms to manage information security. These are detailed below and in the relevant written controls. The ICT service maintains a list of information security issues, risks and mitigations for routine discussion with the SIRO, organisational controls are monitored via the Information Governance risk register linked to ICT risks. The ICT service also meets on a regular basis to review trends in cyber security field and ensure appropriate counter measures are taken to protect the CCG infrastructure

and information. This includes information that is held on-site and with current networks, as well as that held off-site and off-line, including appropriate disposal and destruction processes to the required standard.

6.3 Management of Information Risk

In order to appropriately manage Information Risk and prioritise the Information Security Assurance, it is important to identify and quantify risk through the routine work of the organisation and those providing key services, such as ICT. This risk needs to account for the value of the asset, the potential severity of any impact and the likelihood of an occurrence.

Risks are captured in the relevant Departmental Risk Register and will be reviewed on at least a monthly basis. Risk Registers will be maintained for each ICT Network and contribute to the overall Corporate Risk Register through escalation via the IG Steering Group (IGSG) for inclusion on the corporate register. These are reviewed on a regular basis in accordance with the terms of reference for the IGSG.

6.4 Forensic readiness

- Protect the CCG, staff and clinical systems through the availability of reliable digital evidence gathered from its systems and processes;
- Allow consistent, rapid investigation of major events or incidents with minimum disruption to CCG business;
- Enable the pro-active and comprehensive planning, gathering and storage of evidence in advance of that evidence actually being required;
- Demonstrate due diligence and good governance of the CCG information assets.

6.5 System Level Security Policies

Each Key Information System is required to have a system level security policy that details, where appropriate:

- Access control requirement specifications (such as whether two-part authentication is required and is in place);
- Authorisation process for access to the system (user registration and deregistration);
- Assignment of responsibilities for the system (access, maintain and issue resolution);
- Details on system design and dependencies, including encryption;
- Provisions for reports generated by system utilities on use and audit logs;
- What system documentation is in place;
- Login controls - threshold of failed logins;
- Password controls:

- Must not be based on your username.
- Must contain characters from three of the following four categories:
- Uppercase alphabetic characters (A-Z).
- Lowercase alphabetic characters (a-z).
- Arabic numerals (0-9).
- Non-alphanumeric characters, for example: ! $ # %
- Must not repeat any of your last 4 passwords.
- Passwords must be changed once every 90 days;

- Backup requirements;
- Back-up data testing arrangements;
- Business Continuity or Back-up plans for system data and software applications;
- Details of UPS technologies or other system continuity support;
- Schedules of tests;
- Input data validation;
- Risk Assessment for the System on key areas.

The policy must detail what security reports are available and who can provide them for the following issues, where appropriate:

- Access log files generated by the system
- Current User overview
- Account Monitoring (unused accounts etc.)
- Forensic Readiness assessment

Each system level policy will be reviewed on at least an annual basis.

6.6 Definition of a key Information System

Key Information Systems (Assets) are defined as:

- Systems which other business critical assets are dependent upon (e.g. Network)

6.7 Information Security Incidents

All information Security Incidents must be recorded and reported to the Information Governance team and the ICT service desk. Information Security Incidents or suspected Information Security Incidents must be reported immediately. The Information Governance team will carry out an assessment of the severity of the incident using Data Security and Protection Incident Reporting tool to determine whether the incident is reportable.

If the incident compromises Personal Data it must be reported to the Information Commissioners Office and via the Data Security and Protection Toolkit within 72 hours. This is a requirement of Data Protection Legislation.

Prior to reporting, the Information Governance team will escalate to the SIRO and the Data Protection Officer for advice.

The Information Governance Team will provide a report to the SIRO on a routine basis in line with the standard procedures. The report will note which issues were resolved, which have been escalated as risks and the associated action plan for the management or mitigation of the risk.

6.8 Information Sharing and Transmission

Where information is shared or transmitted, maintaining the security, confidentiality and integrity of the data is a legal requirement, in addition to ensuring an appropriate lawful basis. No Personal Confidential Data should be shared, transmitted or published without the appropriate approval of the Information Governance team or reference to the relevant process, such as legal disclosure or disclosure under Data Protection Legislation or Access to Health Care provisions.

Only encrypted USB memory devices, encrypted Laptops or other authorised mobile device (e.g. blackberry or other smart phone) owned by the CCG are permitted for the transportation of personal identifiable information and/or business sensitive information. Staff with an approved business need to use a mobile device should gain authorisation from their manager, before transferring any information to a mobile device. Such devices are encrypted following the ICT encryption protocol.

6.9 Performance of Information Systems

The performance of Information systems and dependencies will be provided to the SIRO and Director with responsibility for ICT, where applicable, on at least a quarterly basis. Any risks resulting from performance will be added to the relevant Risk Register in line with the Risk Management and Assurance Framework.

Information Systems consist of but are not limited to:

- Network
- Servers
- Key databases and datasets
- Email systems
- Portable devices (such as laptops, memory sticks)
- Cloud based platforms

Performance reports will provide details of, where appropriate (for the reporting period):

- The level of performance for different teams and services (for example Network, Voice and Mobile Working)
- Change Control management
- Information Security priorities and actions

- Network capacity, trends and management
- Server capacity, trends and management
- The number of helpdesk calls received, resolved and open
- Number of User authorised User accounts
- Number of User accounts activated
- Number of User accounts deactivated
- Number of Information Security Incidents, Events or Near Misses
- Lessons Learnt from Information Security Incidents
- Compliance Monitoring
- Audit findings and reports
- Review Meetings
- Changes to Controls and system policies
- System intrusion reports
- Virus software effectiveness
- User Surveys

6.10 Change Management

The SIRO will authorise, either personally or via pre-arranged criteria set to enable the Information Governance lead for internal assurance to give authorisation, the Change Management process for each Network and Key Information Asset and will be advised on any changes that impact on Information Security. A Data Protection Impact Assessment and Information Security Risk assessment will be provided along with an outline of the proposed change. This will include details of the nominated Senior Responsible Officer for the change and Project Board where possible, as well as the reporting line to the CCG.

It is expected that Information Security Assurance will be provided to the SIRO as part of the process of routine management and in good time to effect change.

All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and will comply with Information Management, Quality, Governance and Security accreditation. They will account for data quality, confidentiality and data protection requirements.

It is a legal requirement that the impact of any change is assessed and signed off before the change process is initiated. This change will include:

- A data protection impact assessment for changes impacting on data subject privacy, rights and freedoms.
- A security assessment for changes impact on ICT security (network, telephony) or physical security.
- A risk assessment on the potential risks of the change incorporating any risks to the delivery of the change. This risk assessment must balance the benefits of undertaking the change against the risks, and those risks of not undertaking the change.

A procurement and contract review requirement for any use of third parties for the provision of services impacting on information management or security.

6.10.1 Change Management that requires Caldicott Guardian sign off

Where the following criteria apply the Caldicott Guardian, for the ICT providers and the CCG will be required before any change can commence:

- Where patient records (regardless of format) are impacted.
- Where a data protection impact assessment has indicated a significant change or threat to privacy.

6.11 Mandatory Controls

Assurance is sought on the mandatory controls in place for Information Assets through several measures. It is expected to be part of routine ICT performance reports, for the assets within their control, part of the review and risk assessment of Information Risk Owners and a deliverable of the change management process.

6.12 Information Risk/Asset Owner Review

Information Risk/Asset Owners are required to provide an annual update to the Senior Information Risk Owner on the management of information risks related to the information assets utilised within their remit. This includes a review of the controls and their effectiveness, on a least an annual basis.

7.0 Information Security Principles

7.1 Access Control

Access Control is required for the management of appropriate access to all information assets. Access will be restricted to any sensitive, confidential or personal confidential data. Access control requirements will be elaborated in more detail for information assets and within System Level Policies, as required.

Access Control will be routinely monitored, audited and removed promptly once a legitimate basis for access no longer exists for a member of staff. Access will be provided in line with the training and awareness provided to staff.

Appropriate authentication of users is required for both information and physical systems, the standards required will be outlined in the relevant system requirements.

7.2 Responsibility for Equipment

Any equipment issued to staff is for the purposes of conducting the business of the organisation and is required to be used in an appropriate and professional manner. Staff are responsible for the equipment issued to them and following the appropriate protocols and procedures for working off site, working remotely and for the return of any equipment no longer required by the staff member.

8.0 Information Security Incidents and Events

8.1 Identifying and managing Information Security Incidents

All information Security Incidents must be recorded and reported to the Information Governance on Nelcsu.information-governance@nhs.net and the ICT service desk. Information Security Incidents or suspected Information Security Incidents must be reported immediately.

These will be highlighted to the nominated Information Security Officer via the ICT service desk. . Examples of incidents are on the intranet and in procedures for incident management.

The Information Governance Team will carry out an assessment of the severity of the incident using Data Security and Protection Incident Reporting tool to determine whether the incident is reportable via the Data Security and Protection Toolkit.

If the incident compromises Personal Data it must be reported to the Information Commissioners Office and via the Data Security and Protection Toolkit within 72 hours. This is a requirement of Data Protection Legislation. Prior to reporting, the Information Governance Team will escalate to the SIRO and the Data Protection Officer for approval of the report.

The Information Governance Team will provide a report to the SIRO on a routine basis in line with the standard procedures. The report will note which issues were resolved, which have been escalated as risks and the associated action plan for the management or mitigation of the risk.

9.0 Training

All staff will be made aware of their responsibilities for information security through generic and specific training programmes and guidance. Training requirements will be publicised via the Communications Department and workforce system where applicable.

The ICT Security Manager is responsible for ensuring ICT security awareness and training for all staff.

10.0 Monitoring and compliance

This policy and the associated controls will be monitored through the Risk Management system for the CCG. The Risk Register will be reviewed on a monthly basis and additionally in response to any Information Security Incident or enforcement action by the Information Commissioner's Office. Information Risk Management is a key component of wider assurance and control in setting the priorities for the information governance work plan.

Information Risk Owners, assisted by Information Risk 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.

Further monitoring will be undertaken through the change control process.

Table 1: Control Audit and Monitoring Table

Monitoring requirements 'What in this document do we have to	The management of information risks (Information Risk Management) Compliance with the law

monitor'	Compliance with the Data Protection and Security Toolkit(DPST) Incidents related to the breach of this policy
Monitoring Method	Information Risks will be monitored through the Risk management system. Compliance with law will be monitored through audit, work directed by the Data Protection and Security Toolkit and as directed by the Internal Assurance Group and Information Governance Steering Group In addition, the DPST will be audited by the organisation's internal audit function before the annual submission. Incident reporting and management requirements
Monitoring prepared by	Information Governance Team Incident reports will be produced by the nominated investigation officer
Monitoring presented to	Information Governance Steering Group Senior Information Risk Owner Caldicott Guardian Highlight report for escalation to the Finance and Performance Committee, where required
Frequency of Review	Monthly updates will be provided to the SIRO and the CG Quarterly reports will be provided to the Information Governance Steering Group The internal audit report on IGT performance will be provided to the Information Governance Steering Group Incident Reports will be reviewed on a monthly/quarterly/annual basis and as directed by the seriousness of the incident

10.1 Non-Compliance

Failure to comply with the standards and appropriate governance of information as detailed in this policy, supporting protocols and procedures can result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance that as individuals they are responsible for. Failure to maintain these standards can result in criminal proceedings against the individual. These include but are not limited to:

- Common law duty of confidentiality
- Computer Misuse Act 1990
- Data Protection Act 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Public Records Act 1958
- Health and Social Care Act 2012
- Care Act 2014
- General Data Protection Regulation (EU) 2016/679

11.0 Review

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

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

12.0 Statement of evidence/references

The following is a list of the Key legislative and regulatory framework

- Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Common law duty of confidentiality
- Human Rights Act 1998
- Health and Social Care Act 2012
- Care Act 2014
- NHS Constitution
- Information Commissioner Offices guidance, passim.
- Care Quality Commission Requirements (for commissioned healthcare services)
- General Data Protection Regulation (EU) 2016/679

Other relevant policies are:

- Information Governance
- Information Quality
- Information Management
- ICT security policies

13.0 Implementation and dissemination of document

The Policy, once approved will be shared with all staff through the all staff email, updated on the CCG intranet page, included in staff briefings and placed in the policy register. A team and management briefing will be provided to support this dissemination.

In addition to the monitoring detailed above, awareness of the policy will be checked through a staff survey and spot checks on at least an annual basis.

Appendix A: Definitions

Term	Definition	Source
Data	Data is used to describe 'qualitative or quantitative statements or numbers that are assumed to be factual, and not the product of analysis or interpretation.'	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)[1] based on the Cabinet Office definition
Information	Information is the 'output of some process that summarises interprets or otherwise represents data to convey meaning.'	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)
Personal Confidential Data or PCD	This term describes personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this review 'personal' includes the Data Protection Act definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)
information security	The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved	ISO/IEC 17799:2005
Information Security Management System - ISMS	That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security NOTE: The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.	ISO/IEC27001:2005 ISO/IEC27002:2005, 2013 ISO/IEC27005:2008

[1] See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf, p. 24