South East London CCG
Information Governance Policy

Document revision

14/01/2020	0.1	Reviewed and tailored for SEL CCG	Draft	IG Compliance Manager
28/01/2020	0.2	Further review and update	Draft	IG Compliance Manager
12/03/2020	1.0	Document finalised	Final	IG Compliance Manager

Document approval

Date	Version	Revision	Role of approver	Approver
26/02/2020	1.0	Document approved, caveat of final additions.	IGSG	IGSG

Contents

1.0 Introduction

The role of NHS South East London Clinical Commissioning Group (CCG) is to commission healthcare, so that valuable public resources secure the best possible outcomes for patients. In doing so, the CCG will seek to meet the objectives prescribed in the Mandate and to uphold the NHS Constitution. This policy is important because it will help the people who work for the CCG understand how to look after the information they need to do their jobs, and to protect this information on behalf of individuals.

This policy sets out the intentions of the CCG to manage the information governance agenda within its remit to the standards required by law and regulations; specifically, the 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). In doing so, this supports high-quality commissioning and healthcare, through accurate, accessible and appropriately governed information.

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 applied throughout this document. All references to information in this document encompass information and data. This includes information that 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 and service users. Information is also used to support the administration of the NHS. In addition to these functions are the requirements of NHS England and NHS Digital (NHSD), which form the wider governance structure that the CCG operates within.

The NHS and the administration of the NHS are dependent on the appropriate use of personal data, and the management of secondary uses of this data and business sensitive data.

The aims of this policy are;

- To maximise the value of organisational assets by ensuring that data is:
    - Held securely and confidentially;
    - Obtained fairly and lawfully;
    - Recorded accurately and reliably;
    - Used effectively and ethically; and
    - Shared and disclosed appropriately and lawfully.
- To protect the organisation's information assets from all threats, whether internal or external, deliberate or accidental. The CCG will ensure:
    - Information will be protected against unauthorised access;
    - Confidentiality of information will be assured;
    - Integrity of information will be maintained;
    - Information will be supported by the highest quality data;

    - Regulatory and legislative requirements will be met;
    - Business continuity plans will be produced, maintained and tested;
    - Information security training will be available to all staff; and
    - All breaches of information security, actual or suspected, will be reported to, and investigated by the Information Governance Team.

The CCG recognises that effective information management is fundamental to proper administration and operational effectiveness, and is an enabler to the achievement of our strategic goals. These are:

- Mapping and implementing future plans;
- Further integration of health and social care where appropriate;
- Delivering improved health outcomes and reduced health inequalities;
- Improving service quality and patient safety;
- Delivering sustainable finances;
- Ensuring robust governance;
- Organisational competence; and
- Underpinning our business with patient and public engagement.

This policy is part of the collection related to information governance that set out the expected standards and controls around the use of information. The policies are:

- Information Governance;
- Information Quality;
- Information Management;
- Information Security; and
- Confidentiality.

The concepts and standards within these policies are interrelated. Obligations and intentions are considered across the suite of policies. The policies sit under an overarching Information Governance Framework, which sets out roles and responsibilities and information governance related work plans.

2.0 Scope

This policy applies to:

- All information and data held and processed by the CCG, which must be managed and held within a controlled environment, including the personal data of individuals, as well as corporate information. It applies to information, regardless of format, and includes legacy data held by the organisation;

- All permanent, contract or temporary staff of the CCG and any 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 outputs from these systems, and

- All means of communicating information, both within and outside the CCG in both paper and electronic format, including data and voice transmissions, emails, post, voice and video conferencing.

The CCG believes that its internal management processes will be improved by the greater availability of information that will grow by the recognition of information governance as a designated corporate function.

3.0 Purpose

Information governance ensures processes, confidentiality and security controls are in place and sets standards of quality and ethical use of personal data. Corporate records must also be managed appropriately and, where possible, provided to the public under the appropriate legislation (Freedom of Information Act 2000 and Environmental Information Regulations 2004) to ensure transparency and accountability.

Information forms a key component of the National Data Guardian's Review of Data Security, Consent and Opt-Outs. This reaffirms the NHS intention to ensure effective decision making, inform and, empower patients through the provision of accurate, accessible and coherent information.

The CCG must manage its statutory and organisational responsibilities. All staff are responsible and contribute towards effective and responsible governance of information in line with the organisation's aims and objectives.

3.1 Objectives

The CCG's Governing Body is committed to ensuring that all:

- Information that relates to individuals is processed, protected and disclosed appropriately to provide improved healthcare and decisions for patients; and

- Information related to its functions, activities and decisions must be managed to the appropriate standards.

The right information, in the right format, to the right people at the right time.

The CCG's aims for the management of information and associated risk includes:

- Effective and efficient management of information for the care of service users and the management of the care service;

- Active advancement of the management of information to improve the provision of services, information and care of patients;

- Engagement with partner organisations and, where appropriate and lawful, share information to support care and the public interest;
- Discharge of its obligations to disclose information in response to lawful requests with due regard to its duties of confidence by following clear and systematic processes;
- Ensuring that systems and processes are effective to ensure the confidentiality and security of personal and other sensitive information;
- Ensuring that all information and data processed, held and managed is of the highest quality in terms of completeness, accuracy, relevance, accessibility and timeliness;
- Ensuring that all information and data is held in a consistent and systematic manner that ensures its accessibility, accuracy and integrity throughout its lifecycle;
- Active provision of information in line with the Freedom of Information Act 2000 and other regulatory or organisational requirements;
- Ensuring that those working on behalf of the CCG are informed, trained and active in the appropriate management of information; and
- Ensuring that change is undertaken in a structured and systematic manner that ensures information governance issues are dealt with in a timely, proportionate and appropriate way.

4.0 The Use of Information

All information must be created, used and managed in a professional manner, as described in the Information Management Policy. It must be accessible to the organisation on a long-term basis and must be stored in a systematic and consistent manner.

Access to information systems, such as to emails, the internet or network, and records of the organisation are provided to staff for business purposes and remain the property of the CCG. All access to, and use must be appropriate and in line with the discharge of their duties.

As staff create information, they are doing so on behalf of the organisation, for example when sending emails, and are accountable for the information they create, for its appropriateness and accessibility.

4.1 Use of Personal Data

Personal data can relate to information about patients, service users and members of staff and describe an identifiable person. It does not have to include particular demographic information, such as name and address but can consist of a combination of factors that would make it possible to identify the person. Information provided to the NHS is done so on the expectation of confidentiality and often in a healthcare setting. If personal data is also subject to a duty of confidentiality, for example because it relates to a patient, we refer to this as personal confidential data. It is important for staff and working practice to account for this and to ensure that any secondary use of personal confidential data, for non-care purposes, is done in accordance with legal and organisational requirements.

The CCG has a suite of privacy notices published on its website, which detail what personal data is held and processed, for what purpose it is used, who it is shared with, and what governs that process. Each service within the organisation must provide a clear statement for their area of responsibility.

4.2 Use of Information to Improve Performance

The organisation will actively seek opportunities to improve the performance of the NHS across its customer base by the better use of information and data. This includes:

- Use of anonymised or de-identified patient data to inform better health care decisions for individuals and the community;
- To review processes and functions within the organisation to ensure efficient and effective data processing; and
- To engage with partner organisations to identify appropriate information sharing, which ensures that the patient and public can exercise choice and are kept informed.

All change processes must follow the standard required, as set out in the Change Management Policy, including completion of a Data Protection Impact Assessment (DPIA). All staff managing change must ensure that they identify any potential information governance requirements when scoping the business case for any change.

5.0 Data Quality

In order to support effective commissioning and to support efficiency, all systems and standard working practice involved in the processing of information must ensure the accuracy and quality of information.

Data quality as per in the Information Quality Policy requires:

- **Accessibility** – information can be accessed quickly and efficiently through the use of systematic and constituent filing.
- **Accuracy** – information is accurate, with systems that support this work through guidance.
- **Completeness** – the relevant information required is identified and working practice ensures it is routinely captured.
- **Relevance –** information is kept relevant to the issues rather than for convenience with appropriate management and structure.
- **Timeliness** – information is recorded as close to possible to being gathered and can be accessed quickly and efficiently.

6.0 Disclosure and Sharing Information

As a public body, the constituent parts of the CCG can only share personal confidential data when it is legally permissible.

This includes adherence to:

- The common law duty of confidence, which extends after death; and
- Data protection legislation.

Any basis of disclosure and sharing needs to be understood and clearly stated before it is undertaken. This decision must demonstrate that the disclosure or sharing is done:

- Reasonably and in good faith for a clear intention;
- Lawfully and is relevant to the purpose intended;
- With grounds that are in the public interest.

Data sharing in the NHS is also governed by the Caldicott Principles, which support the legal framework.

Disclosure or sharing of personal confidential datamust be done so in accordance with the law.:

6.1 Public Rights of Disclosure

All staff are reminded that there are several pieces of legislation that require information to be released to the public, the Freedom of Information Act 2000, Environmental Information Regulations 2004), the subject of personal data (Data Protection Legislation), or those with a claim to the estate of the deceased or lawful right (Access to Health Records 1990).

Freedom of Information Act 2000 and Environmental Information Regulations 2004 apply to information in all formats; this includes emails, voice recordings and images.

To meet this responsibility, all staff are responsible for ensuring that the contents of records are:

- **Accessible** – ensuring that they can be found within a systematic and consistent filing structure.
- **Appropriate** and **relevant** – this includes a professional and appropriate tone.
- Have **Integrity** or completeness – so that they can be used in an ongoing basis.
- **Confidential** – appropriately safeguarded to ensure confidentially with a clear statement of who was provided access to the information.
- **Identified** – systems and staff should ensure that personal identifiable, sensitive, confidential and corporate information is clearly stored and marked as such.

Details of the CCG’s policy on active disclosure and compliance with the Freedom of Information Act is outlined in the organisation’s Public Access to Information Policy and associated protocols and procedures.

7.0 Transferring of Information

All transfers of information within and outside the CCG must be managed, comply with the information security requirements and follow clear process. All teams must have a clear statement of their inward and outward flows of personal data and personal confidential data.

This process must identify:

- The appropriate method and inherent risks of the transfer;
- The contact point and details to which the information is routinely transferred. All contact points should identify a team and position, rather than an individual to which the information is being transferred; and

- How the transfer is confirmed and completed.

In addition, where the transfer of information involves personal or identifiable data, the process must identify:

- The purpose and justification for transferring the information;
- The security standards of the method of transfer;
- The appropriate safeguards in place for the protection of information transferred outside the European Economic Area.

It is expected that most transfers of information will be routine and follow an identified process.

The transfers of information within the CCG and between external organisations must be managed in an appropriate manner and by secure methods with any risks identified and managed.

The CCG does not support the use of physical fax machines. Staff must make every effort to encourage those they communicate with to use secure email and/or software with secure and controlled access to communicate sensitive information.

8.0 Information Security

The purpose of information security is to ensure business continuity in order to minimise the impact of security-related incidents and to ensure the integrity of the information and data processed by the CCG, as described in the Information Security Policy.

Information security enables information to be processed and shared with appropriate safeguards in place. It ensures the protection of information and assets as well as identifying and acting on threats to security.

Information security is both the technical and physical. It ranges from the security of networks, to the use of appropriate passwords by staff and storage of confidential information in secure environments.

All staff contribute towards the security of information and Information Asset Owners are required to have a clear statement on the information security and risks in place for the assets within their remit.

Information security has four basic components:

- **Confidentiality**: ensuring that sensitive information or data is accessible to only authorised individuals and is not disclosed to unauthorised individuals or the public.
- **Integrity**: safeguarding the accuracy and completeness of information and software, and protecting it from improper modification.
- **Availability**: ensuring that information, systems, networks and applications, as well as paper records, are available when required to departments, groups or users that have a valid reason and authority to access them.
- **Accountability –** Users are held responsible for their use of information.

Further information is detailed in the CCG's Information Security Policy.

9.0 Monitoring and Compliance

This framework and the associated controls: policies, protocols and procedures will be monitored through the risk management system for the CCG. The information governance risk register will be reviewed on a regular basis and additionally in response to any information incident or enforcement action by the Information Commissioner's Office. Information risk management is a key component of wider assurance and control in setting the priorities for the information governance work plan.

Information Asset Owners, assisted by Information Asset Administrators, will be required to routinely review the risks and information flows associated with the information assets utilised to fulfil the business functions and activities within their remit.

Furthermore, the organisation's compliance with this policy will be measured by the annual completion and subsequent audit of the Data Security and Protection Toolkit.

9.1 Non-Compliance

Failure to comply with the standards and appropriate governance of information as detailed in this policy, supporting protocols and procedures may result in disciplinary action. All staff are reminded that this policy covers several aspects of legal compliance that as individuals they are responsible. Failure to maintain these standards can result in criminal proceedings against the individual.

10.0 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.

11.0 Implementation and Dissemination

The updated policy, once approved by the Integrated Governance and Performance Committee, will be shared with all staff through an emailed and physical staff briefing to support this dissemination and updated on the intranet.

Awareness of the policy will be checked through a staff survey and spot checks on at least an annual basis.