South West London CCG
Information Quality Policy

Document revision history

Date	Version	Revision	Comment	Author/Editor
03/01/2020	V1.0	Reviewed and tailored for SWL CCG	Draft	IG Compliance Manager

Document approval

Date	Version	Revision	Role of approver	Approver

Contents

1.0 Introduction

Information quality is a requirement for appropriate decision making, governance and the ongoing commissioning of high-quality healthcare. The concept applies to the records, information and data that our organisation creates, maintains and utilises. 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'.* All reference to information in this document encompasses information and data which is personal, financial or falls within any other category.

Information quality is a legal requirement for the organisation under the Data Protection legislation (Data Protection Act 2018 and General Data Protection Regulation (EU) 2016/679– identified in this documentation as the Data Protection legislation) and Public Records Act 1958. It is a regulatory as well as an organisational requirement under government policy and standards.

This policy sets out the standards expected in our processes, systems and working practice to ensure good quality information is at the heart of all of our organisation's functions. It aims to ensure that we create and perpetuate a culture of information quality throughout NHS South West London Clinical Commissioning Group (hereafter referred to as the CCG) and with those that work in partnership with us and who are commissioned to provide services. This includes standards of quality across Information and Data, as outlined by the Cabinet Office and referenced below. In addition, the policy sets out the principles of how we evaluate and mitigate errors in data.

The policy sets out: our statement of intent for information quality**,** the principles that inform the relevant standard, who is accountable for the requirements within this policy, where responsibility sits and the method for their measurement, reporting and delivery.

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

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

2.0 Scope

This policy is applicable to:

- All records, information and data held and processed by the CCG. All information must be managed and held within a controlled environment and to a high standard of accuracy and completeness. This includes personal data of patients and staff, patient level data (non-identifiable – with exceptions) as well as corporate information. It applies to records, information and data regardless of format, in addition to legacy data held by the organisation, in accordance with the approved retention standards;

- The standards expected from services commissioned by our customers for healthcare and non-healthcare purposes;
- Patient level data must be in non-identifiable format (anonymised or pseudonymised) except where held for direct care purposes or permitted via an NHS Act 2006 s.251 approved use;
- Patient level data held in identifiable format must only be held and processed with the appropriate consent or other legal gateway with security and access control requirements in place which meet Data Protection standards;
- All permanent, contract or temporary staff of the CCG and all third parties who have access to our 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.

There are different levels and ranges of data that support the commissioning and contracting of services, from Personal Confidential Data (or "PCD" see definitions for further clarification) also known as special categories of personal data, to Board Level performance data.

3.0 Purpose

As a Controller of personal data we require good quality information to be created, managed and utilised. We have a responsibility to drive improvements in Information Governance from the services we commission. This ensures an efficient, effective and accountable service. This includes ensuring that contractual requirements and monitoring of performance include information quality on a routine basis. In those instances where we appropriately share or publish information we must ensure that this information is accurate and complete.

Without high standards of information quality, supported by systematic processes and practice, we cannot support the delivery of high quality healthcare and improve services.

Objectives

This organisation is committed to ensuring that all information within its responsibility or that it commissions, is created, processed and held to a high standard of quality in a manner which ensures accurate and appropriate decision making.

The right information, to the right people at the right time

This policy sets out our intentions for the creation and maintenance of high-quality information and the management of the associated risks.

- To be of value, information quality must be accurate and complete. The provenance of the information (where it came from) and its timeliness (when it was collected or altered) should be captured where necessary and where possible;
- Information Systems must incorporate methods (or controls) to support the capture of accurate and complete information, this includes validation checks and reporting to identify errors, outliers and issues that require investigation;
- Procedures must incorporate appropriate steps for the validation of information to ensure that it is accurate and complete throughout its lifecycle (from creation through use, to disposal);
- Working Practice supported by training must deliver methods to check and confirm that accurate information is collected, maintained and shared. Those working with information need their training needs and requirements for improving skills and knowledge around information quality assessed and supported;
- Contracts with commissioned services (healthcare and non-healthcare) must incorporate provisions for information quality. These must be supported by methods for monitoring, escalating and resolving issues around information quality for our customers;
- Information must fulfil all of the purposes required of it and must be used in a lawful and appropriate manner.
- When reporting, sharing or publishing information, processes must include appropriate checks (including validation where possible) to ensure that accurate information is provided;
- Concerns around the quality of information will be assessed to capture any associated risks and issues arising, to ensure appropriate mitigation, management and risk reduction over time.

4.0 Equality Analysis

This document demonstrates the organisation's commitment to create a positive culture of respect for all individuals, including staff, patients, their families and carers as well as community partners. The intention is, as required by the Equality Act 2010, to identify, remove or minimise discriminatory practice in the nine named protected characteristics of age, disability, sex, gender reassignment, pregnancy and maternity, race, sexual orientation, religion or belief, and marriage and civil partnership. It is also intended to use the Human Rights Act 1998 and to promote positive practice and value the diversity of all individuals and communities.

5.0 Definitions

See Appendix A for definitions.

6.0 Responsibilities

Key responsibilities, accountability and governance arrangements are outlined within the Information Governance Framework

7.0 Principles of Information Quality

Accessibility

Information can be accessed quickly and efficiently through the use of systematic and consistent management in electronic and physical formats. Access must be appropriate so that only those with a lawful basis and legitimate relationship to information can view, create or modify it.

Accuracy

Information is accurate and supported by appropriate systems, processes, guidance and practices. This is a legal requirement of the Data Protection Legislation 'personal data shall be accurate, and where necessary, kept up-to-date'. Ideally, systems will capture data once and ensure that accuracy is maintained and checked through process.

Any limitations on accuracy of data must be made clear to its users and effective margins of error built into calculations.

Completeness

The relevant information required is identified. Systems, processes and working practices ensure it is routinely captured. The specification of what data is required for the defined need will be incorporated into processes, collection and validation.

Evaluation of information quality must include checks for missing, incomplete or invalid information and consider the causes for this and any associated risks.

Relevance

Information is kept relevant to the issues rather than for convenience, with appropriate management and structure.

Reliability

Information must reflect a stable, systematic and consistent approach to collection, management and use. Methods of collection, use and analysis must ensure consistency in the data and variations in these methods must be considered for their potential impact on the quality or content of the information.

Timeliness

Information is recorded as close as possible to being gathered and can be accessed quickly and efficiently. This is a requirement of the Data Protection Legislation 'personal data shall be accurate, and where necessary, kept up-to-date'.

Validity

Information must be collected, recorded and used to the standard set by relevant requirements or controls. Validity is supported by consistency over time, systems and measures. Any information collection, use or analysis process should incorporate a proportionate validation method or tool to ensure that the standards and principles outlined above are met. Validation tools and processes will support routine data entry and analysis, as well as support the identification and control of duplicate records and errors.

National data standards

The use of national data standards, such as Information Standards Notices, will be incorporated where it supports the appropriate sharing, exchange and monitoring of information. Systems and processes are evaluated to consider what national data standards are relevant and how they will be incorporated. Any risks from not using these standards will be considered, recorded and appropriately managed.

NHS Number

The NHS Number is the unique identifier within the National Health Service. Where appropriate and legal to be used, it must be incorporated into all correspondence with patients and relevant information systems to ensure that the correct individual is identified.

Services that are commissioned are contracted to the use of NHS Number, where appropriate, and to ensure it is incorporated into routine data collection, data management and working practice. Appropriate mitigation is required from commissioned services in clinical and commissioning systems for the absence of an NHS number for an individual.

8.0 Quality of Information and Quality of Data

As noted above this policy uses the terms data and information as defined by the Cabinet Office. However, issues of quality impact upon Information and Data differently due to the separate contexts and it is therefore important to draw distinctions between the two. The principles outlined in this policy apply to both, but the following sections outlines issues around the individual context.

Quality of Information

Information is defined as 'the output of some process that summarises interprets or otherwise represents data to convey meaning'. In terms of this policy, the principles of information quality apply to information but are exercised through the process of interpretation or representation. These processes must ensure the information is complete, accurate and support validation. Any errors are identified through the process and the appropriate mitigation undertaken.

Quality of Data

The principles of information quality apply to data and are evaluated before, during and after analysis and interpretation. Processes to ensure the principles in this policy are used but data will be subject to broader analysis for duplication, error and results that sit outside expected ranges.

9.0 Errors in Information and Data

Key Principles

It is understood that errors and inaccuracies will occur in Information. Systems, process and analysis during the lifecycle of the information need to identify the causes of any errors, the relevant margin of error introduced into any subsequent use of the Information and the appropriate action taken.

This includes understanding the context of any Information or Data Set, to ensure that “outliers”, results that fall outside expected ranges, are investigated to determine if there are any resulting information quality concerns. It is important to determine and maintain a view of expected ranges of information to support the principles of information quality.

Mitigations

Where errors are identified, appropriate mitigation is required. This includes correction or annotation, where relevant, analysis of process and appropriate action, and ongoing monitoring. Understanding the cause of error and its likely consequence are a key component of improving information quality or managing issues that cannot be addressed through appropriate controls.

10.0 Specific Requirements

System Level Policies and Controls

Key Information Assets that utilise information, usually referred to as Information Systems are required to have a System Level Policy that sets out their principles of operation and controls. Within these policies the approach to information quality against the principles outlined in this policy are detailed.

These systems must consider the requirements of relevant legislation, legal gateways and national data standards; the policy outlines how they are incorporated and the relevant controls. Routine audits of controls on data and validation programmes are incorporated into system level policies and working practice.

Regular reviews of current controls and working practice are required to ensure that any developments of national standards and guidance. The standard and frequency for reviews will be outlined in the relevant System Level policy.

Information Collection

Any process that involves information collection must incorporate information quality requirements into the relevant protocol and procedures to ensure the quality of information/data collected is sufficient for the intended purpose(s)

Transcription

Transcribing data from one form to another, either manually or by computer, may increase costs or reduce the quality and usefulness of that data**.** Organisations collecting confidential information should design collection systems which avoid requirements for transcribing data.

Commissioning

Any commissioning of service (healthcare and non-healthcare) must include appropriate contractual and monitoring for information quality. It is important to set out the requirements for any information to be gathered in the course of the contract and ensure it is appropriate, lawful and meets the required standards for the duration of the contract and at its cessation.

Reports provided by commissioned services will be monitored for Information Quality requirements against the expected standards with the actions taken by the commissioned service monitored as part of ongoing contract management.

New Systems and Change Control

Any new system or change control, must incorporate an assessment of the impact on information quality and relevant controls to support. Accountability for this assessment will be clearly defined and incorporated.

11.0 Monitoring and compliance

This policy and the associated controls will be monitored through the Information Risk Management system for the organisation. The Information Governance Risk Register will be reviewed on a regular basis by the SIRO 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 central in setting the priorities for the information governance work plan for information quality.

Further assurance will be provided through completion of the Data Security and Protection Toolkit (DSPT) and the associated audit. Reviews of the current controls and their operation will be undertaken in line with a quarterly timescale, as a minimum, in line with the expectations of the DSPT. It is noted that the Toolkit may require supplementary work to ensure broader assurance.

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 provides more details

Table 1 Control Audit

Control Audit and Monitoring Table	
Monitoring requirements 'What in this document do we have to monitor'	The management of information risks (Information Risk Management) Compliance with the law Compliance with the Data Security and Protection Toolkit (DSPT) Incidents related to the breach of this policy

Monitoring Method	Information Risks will be monitored through the Information Governance Risk Register and management system. Compliance with law will be monitored through audit, work directed by the DSPT and as directed by Information Risk Management The Information DSPT will be monitored by assessment of evidence against the objective of the relevant requirement. 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 Function and Information Governance Steering Group Incident reports will be produced by the nominated investigation officer
Monitoring presented to	Information Governance Steering Group Senior Information Risk Owner Caldicott Guardian Governing Body and Accountable Officer
Frequency of Review	Regular updates will be provided to the IG Steering Group, the SIRO and the Caldicott Guardian Relevant Information Risks will be added to the Corporate Risk Register and reported in line with Risk Management system Annual (as a minimum) updates to the Governing Body will be provided. The internal audit report on DSPT performance will be provided to the Governing Body or delegated sub-committee. Incident Reports will be reviewed on an annual basis and as directed by the seriousness of the incident

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
- General Data Protection Regulation 2018 (GDPR)
- Freedom of Information Act 2000
- Human Rights Act 1998
- Public Records Act 1958
- Health and Social Care Act 2012
- Care Act 2014

12.0 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.

13.0 Statement of evidence / references

Key Legislative and Regulatory Environment

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

- Data Protection Act 2018
- General Data Protection Regulation 2018 (GDPR)
- 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
- Care Quality Commission Requirements (for commissioned healthcare services)

- Records Management Code of Practice for Health and Social Care 2016
- Code of Practice on Confidential Information 2014

Other References

Other relevant policies are:

- Information Governance
- Information Management
- Information Security
- Confidentiality Policy

A list of related protocols and procedures will be maintained in the Information Governance Framework.

14.0 Implementation and dissemination of document

The Policy, once approved will be shared with all staff through the all staff email, updated on the intranet, included in staff briefings and place 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) based on Cabinet Office definition.
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 'special categories' as defined in the Data Protection Act.	Definition taken from The Information Governance Review, Mar 2013 (Gateway Ref: 2900774)

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