# IG/05

# Surrey Heartlands' CCGs' Information Quality Policy

**Policy applicable to:**

| | |
|---|---|
| NHS Guildford and Waverley CCG | ✓ |
| NHS North West Surrey CCG | ✓ |
| NHS Surrey Downs CCG | ✓ |

| | |
|---|---|
| Policy number | IG/05 |
| Version | 1.0 |
| Approved by | CCG Senior Information Risk Owners |
| Name of originator/ author | Daniel Lo Russo, Head of Information Governance / Data Protection Officer |
| Owner | CCG Senior Information Risk Owners / ICS Directors |
| Date of last approval | March 2019 |
| Next approval due | March 2020 |

## Version control sheet

| Version | Date | Author | Status | Comments / changes since last version |
|---|---|---|---|---|
| 0.1 | 23/02/2019 | Head of IG | Initial Draft | Reviewed by Data Protection Officer |
| 0.2 | 15/03/2019 | Head of IG | Approved by CCG IG Sub Committees | Minor amendments to formatting etc. |
| 1.0 | 19/07/19 | Head of IG | Final | Ratified by Audit Committees |

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 via the CCGs' websites at link:

- NHS Guildford and Waverley Clinical Commissioning Group
- NHS North West Surrey Clinical Commissioning Group
- NHS Surrey Downs Clinical Commissioning Group

## Equality statement

The Surrey Heartlands' CCGs aim to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. We take into account the Human Rights Act 1998 and promote equal opportunities for all. This document has been assessed to ensure that no employee receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the member of staff has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

We embrace the four staff pledges in the NHS Constitution. This policy is consistent with these pledges.

See next page for an Equality Analysis of this policy.

## Equality analysis

Equality analysis is a way of considering the effect on different groups protected from discrimination by the Equality Act, such as people of different ages. There are two reasons for this:

- to consider if there are any unintended consequences for some groups; and
- to consider if the policy will be fully effective for all target groups.

| | | |
|---|---|---|
| **Name of Policy:**<br>Information Quality Policy | **Policy Ref:**<br>IG/05 | Is this<br>New? [✓] |
| **Assessment conducted by:**<br>Daniel Lo Russo, Head of IG / DPO | | **Date of Analysis:**<br>15/03/2019 |
| **Directorate:**<br>Corporate Affairs and Governance | **Director's signature:**<br>Elaine Newton | |

| | |
|---|---|
| 1. | Who is intended to *follow* this policy? Explain the aim of the policy as applied to this group.<br>All individuals with access to CCG confidential / personal data or ICT systems which the CCGs are responsible for are required to comply fully with the requirements of this policy. |
| 2. | Who is intended to *benefit from* this policy? Explain the aim of the policy as applied to this group.<br>All CCG staff and users of CCG supplied or commissioned services will benefit from the CCGs complying with applicable legislation. |
| 3. | **Evidence considered.** What data or other information have you used to evaluate if this policy is likely to have a positive or an adverse impact upon protected groups when implemented?<br>Best practice and guidance shared via local and national networks has been utilised as well as learning from historical complaints made to CCGs. |
| a) | **Consultation.** Have you consulted people from protected groups? What were their views?<br>We have not directly consulted CCG people from protected groups.<br>During 2019/20 the CCGs will establish a Patient Data Panel that will include people from protected groups and which will review IG related policies, procedures, data protection impact assessments, and information sharing agreements. |
| b) | **Promoting equality.** Does this policy have a positive impact on equality? What evidence is there to support this? Could it do more?<br>Policy represents best practice. |

| | |
|---|---|
| c) | **Identifying the adverse impact of policies.** Identify any issues in the policy where equality characteristics require consideration for either those abiding by the policy or those the policy is aimed to benefit, based upon your research.<br>Not applicable – reasonable adjustments will be made where required. |
| | i) People from different age groups:<br>No adverse impact identified. |
| | ii) Disabled people:<br>Adverse impact identified – reasonable adjustments will be made where required (e.g. CCG will support people to make written requests for access to information or support for disabled staff members to access e-learning).<br>Information supplied by the CCGs will meet the Accessible Information Standard. |
| | iii) Women and men:<br>No adverse impact identified |
| | iv) Religious people or those with strongly help philosophical beliefs:<br>No adverse impact identified |
| | v) Black and minority ethnic (BME) people:<br>Potential adverse impact identified (people who do not have English as their first language) – reasonable adjustments will be made where required (e.g. CCG will support people to make written requests via translators etc). |
| | vi) Transgender people:<br>No adverse impact identified. |
| | vii) Lesbians, gay men and bisexual people:<br>No adverse impact identified. |
| | viii) Women who are pregnant or on maternity leave:<br>No adverse impact identified. |
| | ix) People who are married or in a civil partnership:<br>No adverse impact identified. |
| 4. | **Monitoring.** How will you monitor the impact of the policy on protected groups?<br>The CCGs have in place established processes to gather complaints, compliments, and feedback from service users – relevant feedback to be reviewed by CCG Head of IG in liaison with Head of Engagement, Diversity & Inclusion and IG Sub Committees |

## Contents

# 1. Introduction and Policy Objective

## 1.1 Background

1.1.1 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 the Surrey Heartlands' CCGs' and our staff create, maintain and utilise.

1.1.2 Information quality is a legal requirement for the organisation under the Data Protection legislation and the Public Records Act 1958. It is a regulatory as well as an organisational requirement under government policy and standards.

1.1.3 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 organisations' functions. It aims to ensure that we create and perpetuate a culture of information quality throughout the Surrey Heartlands' CCGs and with those that work in partnership with us and who we commission to provide services.

1.1.4 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.

1.1.5 The purpose of this policy is to assist individuals undertaking work on behalf of the CCGs to conduct activity in a way that takes into account the applicable legislation, regulatory requirements, and best practice. This will support delivery of the CCGs' Strategic and Corporate Objectives (available at link).

1.1.6 This is one of a suite of policies, procedures, and guidance material that link to the CCGs' Information Governance Management Framework. This policy should be read alongside the CCGs' Records Management Policy in particular.

1.1.7 The policy reflects the current capacity, capability, and structure of CCGs and will be regularly reviewed to ensure that it remains aligned with these and fit for purpose.

1.1.8 This policy supersedes the following CCG specific policies:

| CCG | Policy |
|---|---|
| NHS Guildford & Waverley CCG | N/A |
| NHS North West Surrey CCG | Information Quality Policy (IG 3) |
| NHS Surrey Downs CCG | N/A |

# 2. Legislative Framework / Core Standards

## 2.1 Relevant Legislation

2.1.1 The policy reflects the requirements of the following key laws and legislation with which the CCGs are required to comply:

- The **Data Protection Act 2018** (DPA18) sets out six principles regarding how personal data should be used. The Fourth Principle requires that personal data be accurate and kept up to date.
- The **Public Records Act 1958** (PRA58) details specific requirements relating to public authorities and confirms that employees of these authorities are responsible for any records that they create or use in the course of their duties.

## 2.2 Health & Social Care Specific Requirements

2.2.1 The policy also reflects the following health and social care sector specific statutory guidance with which the CCGs are required to comply:

- The Records Management Code of Practice for Health and Social Care 2016, issued by the Information Governance Alliance, sets out what people working with or in NHS organisations in England need to do to manage records correctly. It's based on current legal requirements and professional best practice.
- All organisations that have access to NHS patient data and systems must use the **NHS Data Security and Protection Toolkit** (available at link) to provide assurance that they are practicing good data security and that personal information is handled correctly. This includes specific requirements relating to data quality.

# 3. Scope

## 3.1 Who this policy applies to

3.1.1 This policy applies to the Surrey Heartlands' CCGs, which includes:

- NHS Guildford and Waverley Clinical Commissioning Group;
- NHS North West Surrey Clinical Commissioning Group; and
- NHS Surrey Downs Clinical Commissioning Group.

3.1.2 This policy applies to all permanent, contract or temporary staff of the CCGs and any third parties who have access to the CCGs' premises, systems or information.

3.1.3 Any reference to staff within this document also refers to those working on behalf of the organisation on a temporary, contractual, honorary, or voluntary basis.

### 3.2 What this policy applies to

3.2.1 This policy applies to:

- all information and data held and processed by the CCGs which must be managed and held within a controlled environment; including the personal data of patients and staff, as well as corporate information. It applies to information, regardless of format, and includes legacy data held by the organisation;
- 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 CCGs in both paper and electronic format, including data and voice transmissions, emails, post, fax, voice and video conferencing.

## 4. Definitions

### 4.1 Key Definitions

4.1.1 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’.

4.1.2 All reference to information in this document encompasses information and data which is personal, financial or falls within any other category.

### 4.2 List of acronyms used in this policy

4.2.1 A list of abbreviations used within this document are included in the table below:

| Term | Explanation |
|---|---|
| DPA18 | The Data Protection Act 2018 |
| DPIA | Data Protection Impact Assessment |
| DPO | Data Protection Officer |
| GDPR | The General Data Protection Regulation 2018 |
| IAA | Information Asset Administrator |
| IAO | Information Asset Owner |
| IG | Information Governance |
| IGSCs | Information Governance Sub Committees |
| IGMF | Information Governance Management Framework |
| IQ | Information Quality |
| SIRO | Senior Information Risk Owner |

## 5. Roles and Responsibilities

Details of the key IG related roles within the Surrey Heartlands' CCGs and their respective responsibilities are included within the CCGs' Information Governance Management Framework (available at link). Specific roles and responsibilities with respect to this policy are detailed below:

### 5.1 The Governing Bodies

5.1.1 The Governing Bodies are accountable for ensuring that the CCGs have an effective programme for managing information quality in place.

### 5.2 The Audit Committees

5.2.1 The Audit Committees of the CCGs are the Governing Bodies' Committees with oversight for information governance related matters, including information quality. They therefore have responsibilities with respect to:

- being assured that this policy is, and remains, fit for purpose;
- the ratification of approval of this policy and associated work programmes; and
- considering regular summary assurance reports regarding the CCGs' compliance with the requirements of the policy.

## 5.3 The IG Sub Committees (IGSCs)

5.3.1 Each CCG has a dedicated IG sub-committee to undertake detailed scrutiny of information governance related activities, including those relating to information quality. The IGSCs are a sub-committee of the Audit Committee.

5.3.2 The key roles and responsibilities of the IG Sub Committees of the CCGs are included within the Information Governance Management Framework.

5.3.3 The IG Sub Committees have the following specific roles and responsibilities with respect to this policy:

- reviewing the policy and providing provisional approval of the policy and subsequent amendments to this for Audit Committee ratification;
- ensuring that appropriate information quality related activities are included within the CCGs' annual IG Work & Improvement Programme;
- reviewing regular progress reporting with respect to the completion of information quality related activities;
- setting and monitoring Key Performance Indicators with respect to information quality; and
- receiving reports regarding the CCGs' overall level of compliance with the requirements of this policy.

## 5.4 Joint Accountable Officer

5.4.1 The Joint Accountable Officer is ultimately responsible for ensuring that the Surrey Heartlands' CCGs comply with legislative requirements relating to information quality.

## 5.5 Senior Information Risk Owner

5.5.1 The CCGs' Senior Information Risk Owners (SIROs) are the ICS Directors (secondment). Details of the key roles and responsibilities of the CCGs SIROs are detailed within the Information Governance Management Framework. Deputy SIRO's will be appointed and may fulfil the roles and responsibilities when the CCG's SIRO is unavailable.

5.5.2 SIROs / Deputy SIROs have the following specific roles and responsibilities with respect to this policy:

- delegated responsibility for ensuring that the Surrey Heartlands' CCGs comply with legislation relating to information quality;
- identified owner of the policy;
- approve any procedures related to this policy and changes to these;
- approve submission of the CCGs' Data Security and Protection Toolkits; and

- receive and review reports regarding the outcomes of reviews and audits of information quality undertaken for their CCG.

## 5.6 The Caldicott Guardian

5.6.1 Each CCG has a Caldicott Guardian and their key roles and responsibilities are detailed within the Information Governance Management Framework. Caldicott Guardians provide advice and guidance regarding information quality issues relating to patient data utilised by the CCGs and commissioned services.

## 5.7 Information Asset Owners

5.7.1 The CCGs' have identified Information Asset Owners (IAOs) for all CCG Departments and Teams. IAOs are senior managers (e.g. 'Head of' or above) and details of the key roles and responsibilities of the CCGs SIROs are included within the Information Governance Management Framework.

5.7.2 They also have the following specific roles and responsibilities with respect to this policy:

- ensure that information quality requirements for the information assets they are responsible for are detailed within System Level Security Policies;
- ensure that information quality requirements are taken into account during the completion of Data Protection Impact Assessments that are completed for any new activities that they are responsible for and which require the processing personal data or changes to existing activities and associated business processes;
- ensure that reviews of information quality for the information assets they are responsible for are regularly undertaken;
- Where errors are identified, ensure that appropriate mitigation is undertaken; and
- provide assurance to the SIRO regarding information quality for the information assets they are responsible for.

## 5.8 Information Asset Administrators

5.8.1 CCGs' also have Information Asset Administrators (IAAs) who assist the IAOs to meet the responsibilities detailed above. IAAs may support information quality related reviews and audits undertaken within the CCGs.

## 5.9 The Data Protection Officer

5.9.1 The CCGs are required to have a Data Protection Officer (DPO) and within the CCGs this is the Head of Information Governance & Freedom of Information. The key roles and responsibilities of the DPO are included within the Information Governance Management Framework (available at link). The DPO will provide advice and guidance regarding information quality issues relating to personal data utilised by the CCGs or which is processed other organisations as part of the delivery of CCG commissioned services, projects and contracts.

## 5.10 The Surrey Heartlands' CCGs' IG Team

5.10.1 The key roles and responsibilities of the CCGs' IG Team are included within the Information Governance Management Framework available at link) - they also have the following specific responsibilities with respect to this policy:

- management of the process of ensuring that this policy and related procedures are kept up to date and aligned with the current capacity, capability, and structure of CCGs;
- supporting IAOs to develop System Level Security Policies which detail applicable information quality requirements;
- providing advice and guidance regarding information quality for personal data and confidential business data;
- supporting internal and external reviews and audits of information quality; and
- undertaking checks of compliance with the requirements of this policy by individuals undertaking work on behalf of the CCGs and provide reports regarding these to the CCGs' SIROs and IG Sub Committees.

## 5.11 Directors and Managers

5.11.1 Directors and Managers of CCG Teams have the following specific responsibilities with respect to this policy:

- ensuring that all individuals undertaking work on behalf of their directorate / team comply fully with the requirements of this policy and related procedures;
- responsibility for the quality of the information, data and records that their team create and use;
- ensuring that information quality requirements are taken into account during completion of Data Protection Impact Assessments that are completed for any new activities that they are responsible for and which require the processing personal data or changes to existing activities and associated business processes;
- ensuring that suitable contracts or other agreements containing appropriate clauses relating to information quality are in place with all individuals / organisations engaged to undertake work on behalf of the CCG and commissioned services etc.;

- receiving and considering reports regarding the quality of data and records that their team create and use; and
- Where errors are identified, ensuring that appropriate mitigation is undertaken.

### 5.12 All staff and other individuals undertaking work on behalf of the CCGs

5.12.1 All staff and other individuals undertaking work on behalf of the CCGs are responsible for any records that they create or use in the course of their duties. They are therefore required to:

- read this policy and understand how it relates to their role;
- comply fully with the requirements of this policy and related procedures;
- assist fully with any reviews or audits of information quality undertaken
- Where errors are identified with records they have created or used, assist with the delivery of any mitigation activities undertaken; and
- report any information quality issues to the appropriate Information Asset Owner / Senior Manager and also via the CCGs IG Incident Reporting process.

## 6. Policy specific information

### 6.1 Policy Statement

6.1.1 The Surrey Heartlands' CCGs require good quality information to be created, managed, and utilised. The CCGs also have a responsibility to drive improvements in Information Governance and information quality within the services we commission. This ensures an efficient, effective and accountable healthcare service is provided for patients. CCG responsiblities include ensuring that contractual requirements and monitoring of performance include information quality on a routine basis. In instances where we appropriately share or publish information we must ensure that this information is accurate and complete.

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

### 6.2 Objectives

6.2.1 Surrey Heartlands' CCGs are committed to ensuring that all information within their responsibility or the services that they commission, is created, processed and held to a high standard of quality in a manner which ensures accurate and appropriate decision making.

6.2.2 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 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; and
- 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.

## 6.3 Principles of Information Quality

6.3.1 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.

6.3.2 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.

6.3.3 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.

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

6.3.5 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.

6.3.6 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'.

6.3.7 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.

## 6.4 National data standards

6.4.1 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.

## 6.5 NHS Number

6.5.1 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.

6.5.2 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.

## 6.6 Quality of Information & Quality of Data

6.6.1 As noted above within the definitions section 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.

6.6.2 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.

6.6.3 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.

## 6.7 Errors in Information and Data

6.7.1 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.

6.7.2 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.

## 6.8 Mitigations

6.8.1 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.

## 6.9 System Level Security Policies and Controls

6.9.1 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.

6.9.2 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.

6.9.3 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.

## 6.10 Information Collection

6.10.1 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).

## 6.11 Transcription

6.11.1 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.

## 6.12 Commissioning

6.12.1 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.

6.12.2 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.

### 6.13 New Systems and Change Control

6.13.1 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.

## 7. Procedural requirements relating to this policy

### 7.1 Dissemination and Implementation

7.1.1 This policy and any subsequently approved versions will be distributed to staff via the CCG newsletter and placed on the CCG intranet. This policy will also be publicly available via the CCG websites.

7.1.2 All individuals undertaking work on behalf of the CCGs will be made aware of this policy during the induction process.

### 7.2 Process for Monitoring Compliance

7.2.1 The activities described in the CCGs' IG Work and Improvement Programme and supporting assurance plans will be used to monitor compliance with the requirements of this policy.

7.2.2 Individuals should be aware that failure to comply with the CCGs' IG Management Framework and/or supporting policies may be dealt with as:

- a disciplinary matter in accordance with the CCGs' Human Resources related policies; or
- a breach of NHS Standard Terms and Conditions for the Supply of Services or other contract / agreement.

7.2.3 Serious non-compliance may also result in criminal proceedings being taken against the individual(s) involved.

### 7.3 Review Date

7.3.1 Review of this policy will take place on the first anniversary of adoption and subsequently every two years until rescinded or superseded. The review will be undertaken by the CCGs' Data Protection Officer.

## 8. Bibliography

### 8.1 Sources of information:

- NELCSU template CCG IG related policies
- NHS Data Security & Protection Toolkit available at link
- Previous CCG Policies

- Records Management Code of Practice for Health and Social Care 2016
- UK legislation at link

## 9. Appendix 1 – Related Documents

This policy links to the following key documents:

### 9.1 Related policies

Other Surrey Heartlands' CCG IG related policies as detailed below;

- Information Governance Management Framework;
- Confidentiality & Data Protection Policy;
- Information & Cyber Security Policy;
- Records Management Policy; and
- Public Access to Information and Re-Use Policy.

### 9.2 IG related procedures

This policy links to the following key IG related procedures:

- Meeting individuals' information related rights (See Appendix 3 of Confidentiality and Data Protection policy);
- IG Incident Reporting (See Appendix 4 of Confidentiality and Data Protection policy);
- Data Protection Impact Assessment procedure (See Appendix 5 of Confidentiality and Data Protection policy); and
- Secure transfers of data (See Section 7.34 of the Information and Cyber Security Policy).

### 9.3 Guidance Documents

Further guidance is also available via the information governance team:

- What you need to know about IG;
- Information Asset Owners Handbook; and
- The CCGs' IG Team Mailbox.

## 10. Appendix 2 - Procedural Document Checklist for Approval

| **Title of document being reviewed:** | | **Yes/No/ Unsure** | **Comments/Details** |
|---|---|---|---|
| **A** | **Is there a sponsoring director?** | Yes | ICS Director of Corporate Affairs and Governance |
| **1.** | **Title** | | |
| | Is the title clear and unambiguous? | Yes | |
| | Is it clear whether the document is a guideline, policy, protocol or standard? | Yes | Policy |
| **2.** | **Rationale** | | |
| | Are reasons for development of the document stated? | Yes | Comply legislation and DSPT |
| **3.** | **Development Process** | | |
| | Do you feel a reasonable attempt has been made to ensure relevant expertise has been used? | Yes | |
| | Is there evidence of consultation with stakeholders and users? | Yes | Reflects best practice |
| **4.** | **Content** | | |
| | Is the objective of the document clear? | Yes | |
| | Is the target group clear and unambiguous? | Yes | |
| | Are the intended outcomes described? | Yes | |
| **5.** | **Evidence Base** | | |
| | Is the type of evidence to support the document identified explicitly? | Yes | |
| | Are key references cited? | Yes | |
| **6.** | **Approval** | | |
| | Does the document identify which committee/group will approve it? | Yes | |
| **7.** | **Dissemination and Implementation** | | |
| | Is there an outline/plan to identify how the document will be disseminated and implemented amongst the target group? Please provide details. | Yes | |
| **8.** | **Process for Monitoring Compliance** | | |
| | Have specific, measurable, achievable, realistic and time-specific standards been detailed to monitor compliance with the document? Complete Compliance & Audit Table. | Yes | |
| **9.** | **Review Date** | | |
| | Is the review date identified? | Yes | |

| Title of document being reviewed: | | Yes/No/<br>Unsure | Comments/Details |
|---|---|---|---|
| **10.** | **Overall Responsibility for the Document** | | |
| | Is it clear who will be responsible for implementing and reviewing the documentation i.e. who is the document owner? | Yes | |

| | | | |
|---|---|---|---|
| **Director Approval** | | | |
| On approval, please sign and date it and forward to the chair of the committee/group where it will receive final approval. | | | |
| Name | Vicky Stobbart | Date | 15/03/19 |
| Signature | | | |
| Name | Karen Thorburn | Date | 15/03/19 |
| Signature | | | |
| Name | Colin Thompson | Date | 15/03/19 |
| Signature | | | |
| **Audit Committee Approval** | | | |
| On approval, Chair to sign and date. | | | |
| Name | Jacqui Burke | Date | 19/07/19 |
| Signature | | | |

## 11. Appendix 3 – Compliance and Audit Table

| Criteria | Measurable | Frequency | Reporting to | Action Plan/ Monitoring |
|---|---|---|---|---|
| IQ related activities included within IG Work & Improvement Programme | Number of activities included | Annual | Audit Committees and IG Sub Committees | Progress reports and key performance indicators |
| IQ related activities completed | Status activities included (open / complete) | Quarterly | Audit Committees and IG Sub Committees | Progress reports and key performance indicators |
| System level security policies for Information Assets include IQ requirements | If IQ requirements included | Annual | Audit Committees and IG Sub Committees | Reviews of system level security policies (SLSPs) |
| Data protection impact assessments include IQ requirements | If IQ requirements included | Annual | Audit Committees and IG Sub Committees | Reviews of data protection impact assessments (DPIAs) |
| Reviews and audits of compliance with IQ requirements identified in SLSPs and DPIAs | If controls in place and complied with | As required | Audit Committees and IG Sub Committees | Reviews and audits by IG Team and independent auditors |