

Surrey Heartlands CCGs' Information Governance Management Framework

Policy applicable to:

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

Policy number	N/A
Version	1.1
Approved by	Audit Committees
Name of originator/ author	Daniel Lo Russo, Head of Information Governance, & Freedom of Information and Data Protection Officer for the Surrey Heartlands CCGs
Owner (director)	Joint Executive Team
Date of last approval	05/09/18
Next approval due	February 2020

Executive Summary

The IG Management Framework provides a summary of our approach to handling personal data and confidential business data. This is aligned with, and supports delivery of, the CCGs' Strategic and Corporate Objectives. These are available via the Surrey Heartlands CCGs' websites.

It reflects that the CCGs are committed to the Data Protection Principles of:

- Accountability
- Lawfulness
- Fairness
- Transparency

The IG Management Framework also details how we will provide service users and other stakeholders with assurance regarding the way in which we handle information.

To support the best possible use of public funds and effective collaborative working, a common IG Management Framework will be in place across the Surrey Heartlands CCGs. This is underpinned by a robust governance framework, policies and procedures, training, and supporting guidance.

To ensure that it reflects the current capacity and capability of the organisations the IG Management Framework will be reviewed annually by the Data Protection Officer and the Joint Executive Team

Version control sheet

Version	Date	Who	Status	Comments / changes since last version
0.1 – 0.4	09/08/18 – 05/09/18	Dan Lo Russo	Review	Initial draft reflecting legislation and available supporting guidance
0.5	05/09/18	CCGs' Senior Information Risk Owners	Review	Added role of Deputy SIRO Recommendation to approve to JET provided
0.6	21/09/18	Joint Executive Team	Approved	
1.0	15/02/19	Audit Committees	Approved	
1.1	16/10/19	IG Sub Committees	Approved	IG Sub Committees approved extension of review date to February 2020.

Contents

1. Introduction and Policy Objective.....	5
2. Principles	5
3. References	6
4. Definitions	7
5. Purpose and Scope	8
6. Roles and Responsibilities/ Duties.....	8
7. The IG Management Framework	13
8. Target Audience.....	16
9. Monitoring Compliance	16
10. Document Control including archiving arrangements.....	17
11. Associated Documentation	17
12. Appendix 1: Information Governance Sub-Committee- Terms of Reference	18

Introduction and Policy Objective

- 1.1 All organisations within the UK that handle personal data are required to ensure that they can demonstrate an appropriate level of compliance with the requirements of the:
 - European General Data Protection Regulation 2018;
 - UK Data Protection Act 2018;
 - UK Common Law Duty of Confidentiality.
- 1.2 Additionally, NHS organisations, and those that deliver NHS services, must also demonstrate they have a satisfactory level of compliance with the relevant NHS Data Security & Protection Toolkit, and that they are working towards achieving full compliance with this.
- 1.3 To support the CCGs to demonstrate that they are complying with data protection related legislation and applicable NHS requirements, the Joint Executive Team have approved that the IG Management Framework detailed in this document be implemented during 2018/19.
- 1.4 This document includes summary information regarding the IG Management Framework, including:
 - the underlying principles;
 - the key roles and responsibilities;
 - the key governance committees involved; and
 - related assurance processes.

Principles

The CCGs' IG Management Framework reflects the underlying principles of:

1.5 Accountability

- We recognise that we are **responsible** for complying with applicable data protection legislation and that we must be able to **demonstrate** our compliance with this.
- We will therefore put in place technical and organisational measures to ensure, and demonstrate, our compliance with applicable data protection legislation. These measures will be appropriate, risk-based, and proportionate.
- We also recognise that our accountability obligations are ongoing - we will therefore regularly review and, where necessary, update the measures we put in place.

1.6 Lawfulness

- We will ensure that we have identified an appropriate lawful basis (or bases) for collecting and using personal data.
- If we are processing special category data (e.g. health data) or criminal offence data we will ensure that we have also identified a condition for processing this type of data.
- We will not do anything unlawful with the personal data we hold.

1.7 Fairness

- We will use personal data in a way that is fair.
- We will only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.
- We will consider how our processing may affect the individuals concerned and can justify any adverse impact.
- We will not process people's data in a way that is unduly detrimental to the individuals concerned.
- We do not deceive or mislead people when we collect their personal data.

1.8 Transparency

- We will be clear with people from the start about how we will use their personal data.
- We are open and honest, and comply with the transparency obligations of the right to be informed.

References

1.9 Information included within this document has been taken from the following sources:

1.10 **Information Governance Alliance – GDPR Related Guidance** available at [link](#)

1.10.1 Including the following specific guidance:

- [Changes to data protection legislation: why this matters to you](#) (CEO briefing on GDPR and accountability for data protection);
- [Frequently asked questions;](#)
- [GDPR: what's new;](#)
- [GDPR: implementation checklist;](#)
- [GDPR: guidance on the Data Protection Officer; and](#)

- [GDPR: guidance on accountability and organisational priorities](#)

1.11 **NHS Digital Website - [link](#)**

1.11.1 Including the following specific guidance on the role of:

- [Caldicott Guardian](#);
- [Senior Information Risk Owner](#); and
- [Information Asset Owner](#).

1.12 Information Commissioner’s Office (ICO) Website – GDPR Guidance on Accountability & Governance for Organisations available at [link](#)

1.13 The UK Caldicott Guardian Council Website – [link](#)

1.14 The NHS Data Security & Protection Toolkit for Small Organisations - [link](#)

Definitions

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

Term	Explanation
CSU	Commissioning Support Unit
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
ICO	Information Commissioner’s Office
IG	Information Governance
IGSCs	Information Governance Sub Committees
IGMF	Information Governance Management Framework
IM&T	Information Management & Technology
PDP	Patient Data Panel
SIRO	Senior Information Risk Owner

Purpose and Scope

- 1.16 This document details the IG Management Framework that will be in place across the Surrey Heartlands Clinical Commissioning Groups (CCGs) which comprises of:
- NHS Guildford and Waverley CCG
 - NHS North West Surrey CCG
 - NHS Surrey Downs CCG
- 1.17 It supports the CCGs' to demonstrate compliance with applicable data protection legislation and NHS data security requirements.
- 1.18 This IG Management Framework is applicable to:
- substantively employed staff, whether part time or full time;
 - non-employed resource; including Governing Bodies' Members, contractors, and other individuals undertaking work on the CCGs' behalf; and
 - personal data and confidential business data held in all formats, including digital and hardcopy.

Roles and Responsibilities/ Duties

The following have specific roles and responsibilities with respect to the CCGs' Information Governance Management Framework:

1.19 Joint Accountable Officer (JAO)

- 1.19.1 The JAO is ultimately responsible for ensuring that the Surrey Heartlands CCGs comply with Data Protection related legislation and that a robust IG Management Framework is in place.

1.20 Senior Information Risk Owners (SIROs)

- 1.20.1 The CCGs' SIROs are the Managing Directors. They are an Executive Director of the organisation and are accountable and responsible for information risk within their CCG. They ensure that everyone undertaking work for that CCG is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately.
- 1.20.2 Details of the CCGs' SIROs are publicly available via [the SIRO Register](#) included on the NHS Digital website.

1.21 Deputy Senior Information Risk Owners (DSIROs)

1.21.1 The CCGs' DSIROs are the Deputy Managing Directors. They are a Senior Manager of the organisation who will undertake the SIRO roles and responsibilities during periods of SIRO absence or unavailability.

1.22 Caldicott Guardian

1.22.1 The CCGs' Caldicott Guardians are Clinical Governing Body members. They are a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. When making decisions or giving guidance; Caldicott Guardians will often refer to the [Caldicott Principles](#).

1.22.2 Details of the CCGs' Caldicott Guardians are publicly available via the [Caldicott Guardian Register](#) included on the NHS Digital website.

1.23 Data Protection Officer

1.23.1 Data protection legislation requires that public authorities appoint a Data Protection Officer. This is an essential role in facilitating 'accountability' and the CCGs' ability to demonstrate compliance with this legislation.

1.23.2 The DPO provides support, advice and assurance of compliance across the Surrey Heartlands CCGs. The DPO role is independent, free from conflict of interest, and reports directly to the Surrey Heartlands CCGs' Joint Accountable Officer and SIROs in matters relating to data protection assurance and compliance, without prior oversight of their line manager.

1.23.3 The CCGs' DPO must be consulted on all data protection matters at an early stage as part of ensuring a 'privacy by design and default' approach is followed. This includes when planning new activities or changes to existing business processes. They have expert knowledge of data protection law and practices and possess a detailed understanding of the organisation's business and the purposes for which it processes personal data.

1.23.4 The DPO is the first point of contact for members of the public and the Information Commissioner's Office (ICO) and their contact details are included within the Privacy Notices available via the CCGs' websites.

1.24 Head of Information Governance & Freedom of Information (HoIG)

1.24.1 The HoIG acts as DPO and also has additional responsibilities with respect to supporting the Surrey Heartlands CCGs' compliance with

the various requirements included in the NHS Data Security & Protection Toolkit; including those relating to:

- Information Risk Management
- Information and Cyber Security
- Records Management
- Transparency & Freedom of Information.

1.25 Information Asset Owners

1.25.1 Surrey Heartlands CCG teams / departments have assigned Information Asset Owners (IAO). They are a senior member of staff (e.g. Head of function or above) who is the nominated owner for one or more identified information assets of the organisation. The IAOs support the CCG SIROs in their overall information risk management function by ensuring that:

- regular assessment of risks relating to information assets and related flows of personal data are undertaken along with routine reviews of access controls;
- Data Protection Impact Assessments are completed for any new activities involving personal data, or changes to existing business processes;
- Privacy Notices and Records of Processing for their activities are accurate and updated as required; and
- individuals working within their area of the business comply fully with the CCGs' IG Management Framework and complete relevant IG mandatory training.

1.25.2 Details of the allocated CCGs IAOs are included with the Information Asset Register held by the CCG. These are not currently made publicly available via the IAO Register included on the NHS Digital website.

1.25.3 Most Surrey Heartlands CCG teams also have an assigned Information Asset Administrator (IAA) who will support the IAO in effectively discharging their duties.

1.26 Other Roles

1.26.1 The following also have related responsibilities and are involved in ensuring that a robust IG Management Framework is in place:

- Senior Information Governance Manager – provides advice and support to assist compliance with the IGMF

- Information Governance Delivery Managers – undertake assurance activities and check compliance with the IGMF
- NELCSU IG Team – provide ad hoc IG related support during 2018/19
- IM&T Director – provides strategic support and guidance on Information Management & Technology (IM&T) related matters
- Information Security Manager – Information and Cyber Security related operational support provided by South Central & West Commissioning Support Unit
- Internal Auditors (RSM & TIAA) – provide independent review and assurance
- The [Information Commissioner's Office](#) (ICO) – UK's independent authority set up to uphold information rights in the public interest.

1.27 All staff

1.27.1 It is the responsibility of all staff members of the CCGs', and any other individuals undertaking work for us, to comply with the requirements of the CCGs' IG Management Framework and any supporting policies and procedures.

1.28 Joint Executive Team (JET)

1.28.1 Data protection legislation requires that the highest level of management receive regular reports on data protection assurance and compliance. The DPO will therefore provide the JET with regular highlight reports which include:

- advice regarding current or planned CCG activities that may constitute high risks to the information related rights of individuals;
- details of significant data protection compliance related risks or serious IG incidents that relate to confidentiality and/or individuals' information related rights; and
- assessments of the financial and human resources required to maintain and/or improve levels of compliance of Surrey Heartlands CCGs with Data Protection related legislation and the NHS Data Security & Protection Toolkit.

1.29 IG Sub Committees (IGSC)

1.29.1 Each CCG has a separate IG Sub Committee. However, there is provision in the Terms of Reference to meet as a committee in

common to ensure consistency of approach and the best possible use of resources.

1.29.2 The SIROs and Caldicott Guardian are voting members for the CCGs they represent only. The DSIRO also has voting rights for the CCG they represent during periods of SIRO absence or unavailability.

1.29.3 The IGSCs also includes ad hoc additional non-voting representatives from CCG business units and key suppliers as required.

1.29.4 The IGSCs will undertake the following activities:

- approve the annual IG Improvement & Work Programme and receive regular reports regarding the delivery of this;
- agree the Key Performance Indicators for the above and receive regular reports regarding these;
- review and approval of any IG related policies, procedures and supporting guidance;
- approve the outcomes of information asset risk reviews;
- receive regular reports regarding trends in IG related incidents and near misses;
- approve the CCGs' NHS Data Security & Protection Toolkit submissions.

1.30 Audit Committees

1.30.1 Each IGSC is a sub-committee of the CCG Audit Committee. The Audit Committees will therefore receive quarterly highlight reports relating to delivery of the agreed IG Improvement & Work Programme and copies of the minutes of the IGSCs.

1.31 Patient Data Panel

1.31.1 The CCGs will hold a quarterly meeting which includes Caldicott Guardians, Service User, and relevant CCG business unit representation to review:

- Data Protection Impact Assessments and data sharing arrangements;
- Privacy Notices and Fair Processing arrangements; and
- changes to Data Sharing Agreements the CCGs have with NHS Digital.

1.32 Other Committees

- 1.32.1 Ad hoc subject specific reporting to other any other Senior Management or Governing Body Committee/s as required.

The IG Management Framework

- 1.33 The key elements of the CCG's IG Management Framework include:

1.33.1 Overarching IG Strategy for Surrey Heartlands Clinical Care Partnership

- This is to be developed with local partners during 2018/19.

1.33.2 IG Policy for Surrey Heartlands CCGs

- The CCGs will have a single common policy for Surrey Heartlands CCGs that covers the following key areas:
 - Confidentiality & Data Protection;
 - Information & Cyber Security;
 - Records Management; and
 - Incident Management.
- All CCG staff members are required to confirm that they have read the CCGs' IG Policy and understand how the requirements of it relate to their role as part of appraisal and performance review process.
- The CCGs' IG Management Framework and IG Policy also links to other CCG policies; including those relating to Freedom of Information, Human Resources and Procurement.

1.33.3 IG Procedures

- To support staff to comply fully with the IG Policy, the CCGs will publish detailed procedures covering the following:
 - Secure information sharing;
 - Data Protection by Design and Default;
 - Information Asset Management;
 - Respecting Individuals Rights (separate procedures for service user / staff related requests); and
 - IG Incident Reporting.

1.33.4 Supporting Guidance & Tools

- *What you should to know about IG* – a reference guide for all individuals undertaking work for the CCGs which includes regularly updated Frequently Asked Questions (**update in progress**); and
- ad hoc support, advice and guidance provided via IG Team via central mailbox - please email queries to gwccg.informationgovernance@nhs.net.

1.33.5 IG Work & Improvement Programme

- An annual IG Work & Improvement Programme will be developed by the Data Protection Officer for approval by the Joint Executive Team following recommendation from IG Sub Committees.

1.33.6 Key Performance Indicators (KPIs)

- On an annual basis the IGSCs will agree a range of KPIs to assist them to monitor delivery of the IG Work & Improvement Programme; these relate to:
 - overdue / incomplete agreed actions;
 - completion of Data Protection Impact Assessments;
 - Reviews of Privacy Notices and Records of Processing
 - Subject Access or other Individual's Information Rights related requests completed within deadline;
 - incidents (for CCGs and commissioned service providers); and
 - agreed audit actions completed.

1.33.7 IG Assurance Plan

- An annual IG Assurance Plan, which is aligned with the IG Work & Improvement Programme, will be developed by the Data Protection Officer for approval by the IG Sub Committees. Key components of this include:
 - Regular Confidentiality Audits undertaken by the IG Team;
 - assurance from CCG Information Asset Owners / Heads of Departments;
 - assurance from CCG Contract Managers;
 - assurance from CSUs and other contracted support organisations;
 - Service User Reviews (Child and Adult); and

- independent Audits (includes annual Data Security Protection Toolkit related audit and other IG related reviews as required)

1.33.8 Training

- An annual Training Needs Analysis will be developed by the Data Protection Officer for approval by the Senior Information Risk Owners.
- All CCG staff, Governing Bodies and committees members will receive basic IG related training as part of Induction and are required to undertake Data Security Awareness Training on an annual basis.
- Additional suitable accredited training will be provided for key staff with IG related roles; including the DPO, SIRO, DSIRO, and Caldicott Guardians.
- Assurance will be received regarding IG related training completed by others undertaking work on behalf of CCGs; including contractors and those working under Honorary Agreements etc.

1.33.9 Incident Management

- All IG incidents will be managed, investigated and reported in accordance with the NHS Digital Guide to the Notification of Data Security and Protection Incidents.
- Detailed procedures for staff regarding reporting incidents are will be made available via Intranet.
- The Datix system will be used by all CCGs for the reporting of any actual or suspected IG incidents - **TBC**.
- Procedures are will be in place to deal with serious IG incidents reported to the CCGs by commissioned provider organisations as per the NHS Standard Contract, including those reported out of usual working hours to the CCGs' On Call Managers.

1.33.10 Data Sharing

- To support the CCGs to collaborate and to work effectively with each other and our other partners we may enter into data sharing arrangements:
- Data / Information Sharing Agreements will be utilised to provide other organisations with access to personal data for which the CCG is legally responsible (including pseudonymised data provided via NHS Digital)

- Data Processing Deeds will be utilised where CCG staff and other individuals undertaking work on our behalf require access to personal data for which other organisations (e.g. providers, GP practices etc.) are legally responsible.
- The IG Management Framework is designed to support the CCGs in demonstrating their compliance with the following:
 - Common Law Duty of Confidentiality
 - Public Records Act 1958
 - Computer Misuse Act 1990
 - Human Rights Act 1998
 - Freedom of Information Act 2000 & Environmental Information Regulations 2004
 - Records Management Code of Practice for Health and Social Care 2016
 - European General Data Protection Regulation 2018
 - UK Data Protection Act 2018
 - The NHS Data Security & Protection Toolkit

Target Audience

1.34 The target audience for this policy includes all:

- substantively employed staff, whether part time or full time; and
- non-employed resource; including Governing Bodies Members, contractors, and other individuals undertaking work on the CCGs' behalf.

Monitoring Compliance

1.35 The activities described in the CCG's IG Assurance Plan will be used to monitor compliance with the requirements of the IG Management Framework and supporting policies.

1.36 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.

- 1.37** Serious non-compliance (e.g. theft or malicious damage to personal data) may also result in criminal proceedings being taken against the individual(s) involved.

Document Control including archiving arrangements

Document and Version Control	
Name of Document	Surrey Heartlands CCGs' Information Governance Management Framework
Owner	Daniel Lo Russo, Head of Information Governance & Freedom of Information (and Data Protection Officer) for Surrey Heartlands CCGs
Contact Details	Email: Daniel.lorusso@nhs.net Telephone: 07917 093042
Next Review	2 years from date of approval or earlier if there are significant organisational change or changes to the legislative / regulatory framework
GPMS	Not protectively marked
Distribution and Accessibility	This document will be made available to all staff via the Intranet following approval. The CCGs' electronic staff newsletters will be used to make staff aware that this document has been developed and approved. This document will also be made publicly available via the CCGs' websites.

Associated Documentation

- Agreed Terms of Reference for CCG IG Sub Committees (see Appendix 1).
- Surrey Heartlands CCGs Data Protection and Confidentiality Policy (available at [link](#)).

Appendix 1: Information Governance Sub-Committee- Terms of Reference

Information Governance Sub Committees Terms of Reference

Version Control Page

Date	Version no.	Reviewed by	Comments
20/11/18	0_1	Eleanor O'Shaughnessy	For review by Senior IG Manager
03/12/18	0_2	DPO	Recommended for approval
13/02/19	0_3	Eleanor O'Shaughnessy	For ratification by Audit Committees in Common

Committee Chair approval

Reviewed by	Date
Chair of Audit Committees in Common	February 2019

Lead Executive Director approval

Reviewed by	Date
Elaine Newton, Executive Director of Communications and Corporate Affairs for the Surrey Heartlands CCGs	08/02/19

Information Governance Sub Committees

Terms of Reference

1. Introduction

- 1.1 This Terms of Reference relates to the Information Governance Sub Committees of:
- NHS Guildford and Waverley CCG
 - NHS North West Surrey CCG
 - NHS Surrey Downs CCG
- 1.2 The Committees have the provision to meet “in common” with one or more of the other Surrey Heartlands’ CCGs Information Governance Sub Committees.

2. Purpose & Objectives

- 2.1 The Sub Committees’ purpose is to support and drive the broader information governance agendas and provide the Audit Committees in Common and Executive Management Team with assurance that effective information governance is in place within the organisations.

3. Aim

- 3.1 The Information Governance Sub-Committees will help the organisations and their staff to ensure that personal and corporate information is managed legally, securely and efficiently in order to assist in the delivery of the best possible care.
- 3.2 The Information Governance Sub-Committees will ensure the CCGs successfully report on and manage the risk associated with Information Governance.

4. Key Objectives

- 4.1 To provide assurance to the Audit Committees in Common, and through them to the Governing Body of the CCG, that information governance is embedded within the CCG;

Working together as the Surrey Heartlands Clinical Commissioning Groups

Guildford and Waverley CCG | North West Surrey CCG | Surrey Downs CCG

- 4.2 To ensure the establishment of partnerships, corporate standards and consistent and overarching CCG wide views. This will ensure integration of, and compliance with initiatives and legislation which are elements of Information Governance;
- 4.3 To support the provision of high quality care/services by promoting the effective and appropriate use of information;
- 4.4 To develop support arrangements and provide staff with appropriate tools and support to enable them to discharge their responsibilities.

5. Function

- 5.1 To receive, comment and performance manage all related policies and procedures.
- 5.2 To oversee the management of all relevant Information Governance Legislation and Requirements throughout the CCGs including:
- Caldicott2 – The Information Governance Review;
 - NHS Confidentiality Code of Practice;
 - The Data Protection Act 2018;
 - The Freedom of Information Act 2000
 - The Regulation of Investigatory Powers Act 2000;
 - The Human Rights Act 1998;
 - NHS Records Management Code of Practice;
 - Data Security and Protection Toolkit;
 - Information Security (BS7799/IS027001)
 - Health & Social Care Act 2012
 - European General Data Protection Regulations 2016 (GDPR)
 - National Data Guardian recommendations and Data Security Standards
- 5.3 To provide appropriate assurance to the Audit Committees in Common that the CCG is compliant with the requirements of the Data Security and Protection Toolkit.

6. Key Responsibilities

- 6.1 To ensure that an appropriate comprehensive information governance framework and systems are in place throughout the CCGs in line with national standards;
- 6.2 To inform the review of the CCGs' management and accountability arrangements for information governance;
- 6.3 To develop and recommend approval of IG related policies and associated IG implementation strategy and/or maintain the currency of these policies;
- 6.4 To review the annual Data Security and Protection Toolkit assessments for sign off by the SIROs;
- 6.5 To develop the organisations' information governance improvement programmes;
- 6.6 To ensure that the organisations' approach to information handling is communicated to all staff and made available to the public;
- 6.7 To coordinate the activities of staff given data protection, confidentiality, security, information quality, records management and freedom of information responsibilities;
- 6.8 To monitor the effective delivery the CCGs' Caldicott Function and Information Security & Cyber Security Assurance Plans;
- 6.9 To monitor the organisations' information handling activities to ensure compliance with relevant legislation and guidance;
- 6.10 To ensure that training made available by the organisations is taken up by staff as necessary to support their role;
- 6.11 Provide a focal point for the resolution and/or discussion of information governance issues.

7. Management and Accountability

- 7.1 The Chairs/Senior Information Risk Owners will report back to the Audit Committees in Common and Executive Management Team on the Information Governance Sub-Committees' activities.
- 7.2 The accountability route is to go through the Information Governance Sub-Committee, to the CCGs' Audit Committees in Common, and then on to the Governing Body.

7.3 The Joint Accountable Officer for the Surrey Heartlands CCGs has overall accountability for ensuring that the organisations operate in accordance with the law with the support of their subordinates.

8. Accountability/ Delegated Authority

8.1 The Sub Committees are accountable to the Audit Committees in Common.

8.2 The minutes, including details of all actions agreed, and a separate IG progress report, will be submitted to the Audit Committees in Common.

8.3 Where a “Committees in Common” meeting arrangement is used, the minutes will be written as if only the Sub Committee met.

8.4 The Sub Committees are authorised by the Audit Committees in Common to investigate any activity within these terms of reference. It is authorised to seek any information it requires from any member, officer or employee who are directed to co-operate with any request made by the Sub Committees. All CCG employees and contractors are directed to co-operate with any request made by the Information Governance Sub-Committees.

8.5 The Information Governance Sub-Committees are authorised to implement any activity which is in line with the terms of reference, as part of the IG Improvement & Work Programmes, which shall be approved off by the Audit Committees in Common and the Executive Management Team.

8.6 The Sub Committees are authorised by the Audit Committees in Common to obtain outside legal or other independent professional advice and to secure the attendance of other individuals with relevant experience and expertise if it considers necessary.

9. Membership

9.1 The members of the Information Governance Sub-Committees shall be appointed and reviewed annually by the Audit Committees in Common of the CCGs, as part of their review of this Terms of Reference. The current membership can be found in Appendix 1.

9.2 The Chairs shall be the CCGs’ Senior Information Risk Owners (SIROs) and Managing Directors. The Chairs will provide IG challenge within the organisations. For the occasions when the Chairs are unavailable, Vice Chairs will be appointed. The Vice Chairs are the CCGs’ Caldicott Guardians who have strategic roles, which involve representing and championing confidentiality and information sharing requirements and issues at senior management level and, where appropriate, at a range of levels within the organisations’ overall governance framework. These roles are detailed in the membership list included at Appendix 1.

9.3 The members of the Sub Committees shall be appointed with approval from the Audit Committees in Common.

10. Co-opted members / deputies / attendees

10.1 Sub Committee members may nominate a suitable deputy when necessary and subject to the approval of the Chair. All deputies should be fully briefed and the secretariat informed of any agreement to deputise so that quoracy can be maintained.

10.2 No person attending the meeting in one role can additionally act on behalf of another person as their deputy.

10.3 People from a range of areas may be invited to attend based on the needs of the agenda

11. Attendance

11.1 All voting members are required to attend meetings wherever reasonably possible. Non-voting members of the group are required to attend meetings or send appropriate representation in their absence for continuity purposes. The Secretary for the Information Governance Sub-Committees should be notified in advance of the meeting of those people who will be nominated substitutions.

11.2 CCG staff members will be expected to assist in the development of the CCGs' IG Improvement Programmes and IG related policies, which will be reviewed at Information Governance Sub Committee meetings, and may therefore be required to attend meetings where this is relevant to their role and/or the activity they are undertaking.

12. The Convenor – (Committees in Common)

12.1 Where the Committees are using the “Committees in Common” meeting approach, the participating chairs will select from themselves a “Convenor” for the meeting. All the participating committees will then agree to allow the Convenor to chair the committees in common meeting.

12.2 The Convenor will rotate amongst the participating chairs, although there may be occasions when the business will indicate which of the chairs would be most appropriate to be the Convenor.

13. Quorum

13.1 A quorum shall be two Committee members, which must include:

- CCG Managing Director and Senior Information Risk Owner
- CCG Caldicott Guardian

- 13.2 The Convenor will ask each of the participating chairs to decide if the meeting is quorate after any actions have been taken to manage any declared conflicts of interest.
- 13.3 Nominated deputies attending Sub Committee meetings, on behalf of substantive members, will count towards quorum.
- 13.4 If meetings are not quorate, the Convenor may adjourn the meetings to permit the appointment or co-option of additional members if necessary. The Committee Chairs will have the final decision as to their suitability.
- 13.5 Any decisions put to a vote at Sub Committee meetings shall be determined by a majority of the votes of members present (For clarity: members may be physically attending the meetings or participating by an agreed telecommunications link). In the case of an equal vote, the Chairs shall have a second and casting vote. The chairs will declare the result of the vote.

14. Meetings

- 14.1 The Sub Committees will meet on a quarterly basis. It is expected that meetings will generally be of 60 minutes duration and a maximum of 90 minutes.
- 14.2 The committees will meet in private and agendas and papers will be published at least five working days in advance of the meetings.
- 14.3 Meetings may be held by conference call or by electronic means, so long as those present can hear each other and contribute simultaneously to the meetings.
- 14.4 With the agreement of the Chairs and by exception Members of the Committees may participate in meetings in person or virtually by using video or telephone or web link or other live and uninterrupted conferencing facilities.
- 14.5 To call a meeting, members will be given a minimum of **six** weeks' notice where possible. Notification will be given by email.
- 14.6 Extraordinary meetings of the Sub Committee can be called at the request of the committee members.
- 14.7 Members of the Sub Committees have a collective responsibility for the operation of the Sub Committees. They will participate in discussion, review evidence and provide objective expert input to the best of their knowledge and ability, and endeavour to reach a collective view.

15. Agenda and Papers

- 15.1 The meeting agendas and supporting papers will be distributed 5 working days in advance of the meetings. If submission within this timescale is not possible,

then the Chairs will be notified and the reports will be sent out at the earliest opportunity prior to the meeting dates.

- 15.2 All papers will clearly state the agenda reference, the author and the purpose of the papers, together with the action to be taken.

16. Managing Conflicts of Interest

- 16.1 The members of the Sub Committees must comply fully with NHS England Guidance and CCG Policy regarding Conflict of Interests.
- 16.2 The convenor is responsible for managing conflicts of interests at a meeting of the Sub Committees. If the convenor has a conflict of interest then one of the other participating Chairs or another member of the committees is responsible for deciding the appropriate course of action.
- 16.3 At the start of the meetings, the convenors will invite members to declare if they have any conflicts of interest with the business to be conducted, including previously declared interests.
- 16.4 The convenors will decide any necessary course of action to manage a declared conflict of interest as advised by the CCGs' Conflict of Interest Policy.
- 16.5 Any declared conflicts of interest will be recorded in the minutes along with any action taken, in a form as advised by the CCGs' Conflict of Interest Policy. In summary the information recorded is:
- the name of the person noting the interest;
 - the nature of the interest and why it gives rise to the conflict;
 - the item of the agenda to which the interest related;
 - how it was agreed that the conflict should be managed;
 - evidence that the conflict was managed as intended.

17. Decision-making (Committees in Common)

- 17.1 The aim of the Sub Committees is to achieve consensus decision-making wherever possible.
- 17.2 The Sub Committees will have the provision to meet using the "Committees in Common" arrangement with the other Surrey Heartlands' CCGs. When a decision is unanimously agreed by the members present then the decision will be considered to have been made by the Sub Committees.
- 17.3 Each voting member of the Sub Committees shall have one vote.
- 17.4 If there is not a unanimous agreement, a vote will be taken by the Sub Committee members. (The other CCG Sub Committees meeting at the same

time will likewise take a vote.) The vote will be passed with a simple majority the votes of members present. In the case of an equal vote, the Chairs shall have a second and casting vote.

17.5 The result of the vote will be recorded in the minutes and a record will also be made of the outcomes of the voting for the other CCG Sub Committees.

17.6 All decisions taken in good faith at meetings of the Sub Committees shall be valid even if there is any vacancy in membership or, it is discovered subsequently, that there was a defect in the calling of the meetings, or the appointment of a member attending the meetings.

18. Decision-making (Single CCG Issue)

18.1 On occasions, an agenda item at a CIC meeting will be considered that is pertinent to only one CCG. All meeting members may contribute to the discussion. When a decision needs to be made, the convenor will invite Sub Committees not affected by the item to abstain from the decision-making.

18.2 A record of the discussion and decision need only be included in the minutes of the CCG Sub Committees involved in the item.

19. Emergency/ Chair's action

19.1 The Committees will delegate responsibility for emergency powers and urgent decisions to the Chairs and Deputy Chairs of the Sub Committees

19.2 In the event of an urgent decision being required, this shall be taken by the Chairs or the Deputy Chairs of the Sub Committees; who must consult at least one other member of the committees who is also a member of the Audit Committees in Common prior to taking the decision.

19.3 Urgent decisions must be reported to the next Sub Committee meetings following the urgent decision for ratification by the full meetings together with a report detailing the grounds on which it was decided to take the decision on an urgent basis, and the efforts made to contact the relevant other members of the Committees prior to taking the decision.

20. Secretariat

20.1 The Secretariats shall attend to take minutes of the meetings and provide appropriate administrative support to the Convenors, Sub Committee Chairs and Sub Committee members.

20.2 The Secretary will ensure minutes of the Committee will be formally signed off by the Sub Committees at their next meeting.

21. Policy and Best Practice

21.1 The Sub Committees will apply best corporate governance practice in their decision-making processes, covering a clear ethical basis to the business being considered; aligned business goals; effective strategies incorporating stakeholder values; well governed organisations and reporting systems to provide transparency and accountability.

22. Conduct of the Sub Committee

22.1 The CCGs have a code of conduct in place which defines required standards of behaviour for individuals working within the organisations, and those performing or authorising activities or advisory duties on our behalf. The Sub Committees and their membership will conduct themselves in accordance with these standards and principles.

22.2 The CCGs' code of conduct specifically covers an employee/member's responsibility in relation to hospitality and gifts, and has regard to:

- Professional Standards Authority Standards for Members of NHS Boards and Clinical Commissioning Group Governing Bodies in England,
- NHS Business Services Authority Standards of Business Conduct Procedure,
- Nolan seven principles of public life.

23. Performance of the Sub-Committees

23.1 The Sub-Committees shall review their own performance and effectiveness, including their running costs and terms of reference on an annual basis.

24. Review of Terms of Reference

24.1 These terms of reference will be reviewed annually by the Sub Committees' membership. Any proposed significant changes to the ToR and responsibilities will be presented to the CCGs' Audit Committees in Common for approval.

25. Other

25.1 In order to fulfil their remit, the Information Governance Sub-Committees may obtain any professional advice they require and invite, if necessary, external experts and relevant staff representatives to attend meetings. There is no dedicated budget in place for this activity.

26. Appendix 1

The membership of the committees shall consist of:

- **Voting members (or nominated deputies):**

Job Title	Role on Committee
CCGs' Managing Directors and Senior Information Risk Owners (Chairs)	To ensure that the CCGs effectively manage information risk and information assets
CCGs' Deputy Managing Directors and Deputy Senior Information Risk Owners (Chairs)	To undertake the role of the Senior Information Risk Owner during times when then the Managing Director is unavailable
CCGs' Caldicott Guardians (Vice Chairs)	To champion confidentiality issues and support safe sharing of patient data

- **Non-Voting Members:**

Job Title	Role on Committee
Head of Information Governance and FOI and Data Protection Officer (DPO) for the Surrey Heartlands CCGs	Responsible for the CCGs' day to day compliance with IG requirements and providing specialist advice and guidance
Senior Information Governance Manager	Assists with ensuring the CCGs' day to day compliance with IG requirements and provides specialist advice and guidance; Deputy for the Surrey Heartlands CCGs' DPO
Information Governance Delivery Manager	Secretariat to the IG Sub Committees
IM&T Director (as required)	To provide expert knowledge with respect to CCG ICT services
CSU Information Security Lead (as required)	To provide assurance with respect to security of ICT services
Systems Architect & Data Warehousing Lead (as required)	To ensure that the CCGs utilise data and ICT safely and effectively

Job Title	Role on Committee
Other team / department reps (as required)	Facilities Managers Head of Engagement, Diversity & Inclusion, Surrey Heartlands CCGs Deputy Head of Communications, Surrey Heartlands CCGs
Independent Auditors (as required)	To provide independent review and assurance
Local Security Management Specialist etc. (as required)	To provide expert advice on security issues