IG/04

Surrey Heartlands CCGs' Records Management Policy

Policy applicable to:

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

Policy number	IG/04
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
- to consider if the policy will be fully effective for all target groups

Name of Policy: Records Management Policy	**Policy Ref:** IG/04	Is this New? [✓]
Assessment conducted by: Daniel Lo Russo, Head of IG / DPO		**Date of Analysis:** 15/03/2019
Directorate: Corporate Affairs and Governance	**Director's signature:** 	

1.	Who is intended to *follow* this policy? Explain the aim of the policy as applied to this group. See Scope – all individuals with access to the CCGs' 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. 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?: • best practice and guidance shared via local and national networks; and • complaints made to CCGs
a)	**Consultation.** Have you consulted people from protected groups? What were their views? We have not directly consulted CCG staff from protected groups. 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?

	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. Not applicable – reasonable adjustments will be made where required.
	i) People from different age groups: No adverse impact identified.
	ii) Disabled people: 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). Information supplied by the CCGs will meet the Accessible Information Standard.
	iii) Women and men: No adverse impact identified.
	iv) Religious people or those with strongly help philosophical beliefs: No adverse impact identified.
	v) Black and minority ethnic (BME) people: 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: No adverse impact identified.
	vii) Lesbians, gay men and bisexual people: No adverse impact identified.
	viii) Women who are pregnant or on maternity leave: No adverse impact identified.
	ix) People who are married or in a civil partnership: No adverse impact identified.
4.	**Monitoring.** How will you monitor the impact of the policy on protected groups? 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 All public bodies are required to have effective records management systems in place to support delivery of their functions. Effective records management within the Surrey Heartlands CCGs' supports high quality commissioning and healthcare, through accurate, accessible and appropriately governed information.

1.1.2 The overall objective of this policy is to provide a framework for consistent and effective management of corporate and health records within the CCGs that is based on established standards and which is integrated with other information governance activity.

1.1.3 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).

1.1.4 The policy also reflects the underlying principles detailed in the CCGs' Information Governance Management Framework (available at link), which are:

- Accountability
- Lawfulness
- Fairness
- Transparency

1.1.5 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 other Information Governance related policies.

1.1.6 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.

1.1.7 This policy supersedes the following CCG specific policies:

CCG	Policy
NHS Guildford & Waverley CCG	Records Management Policy (49 EC)
NHS North West Surrey CCG	Information Lifecycle Management Protocol (IG 5)
NHS Surrey Downs CCG	Records Management Policy (IG 08)

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:

2.1.2 The purpose of the **Data Protection Act 2018** (DPA18) is to protect the rights and privacy of individuals. The DPA18 sets out six principles regarding how personal data should be used. The following DPA18 principles are particularly relevant to this policy:

- Principle 4 - requirement that personal data be accurate and kept up to date;
- Principle 5 - requirement that personal data be kept for no longer than is necessary.

2.1.3 The Public Records Act 1958 (PRA58) details specific requirements relating to public authorities and confirms that employees of these 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 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. The Code of Practice Alliance describes how different types of records (including those containing personal data) should be stored and details the period of time that they should be retained for.
- 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 A record is defined as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business' (ISO 15489-1:2016).

4.1.2 This definition draws a distinction between a record and a document:

- a **record** is a final version that may be retained; and
- a **document** can be changed and will not normally be retained except for audit trail purposes where necessary.

4.1.3 The purpose of a record is to preserve information in a form that is trustworthy and, once declared, should not be changed. A record is only created when there is a need to remember the details of an event, decision or action. Creation is supported by a process of lodging a document into a record keeping system, including the registration and classification of the

record and assigning metadata to describe the record and place it in context. The life of a record from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either preservation or confidential destruction.

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
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 2016
IAA	Information Asset Administrator
IAO	Information Asset Owner
ICO	Information Commissioner's Office
IG	Information Governance
IGSC	Information Governance Sub Committee
IGMF	Information Governance Management Framework
IM&T	Information Management & Technology
RM	Records Management
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 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 of the CCGs are accountable for ensuring that the CCGs have an effective programme for records management and related assurance in place.

5.2 The Audit Committees

5.2.1 The Audit Committees of the CCGs are the Governing Body Committees with oversight for records management related matters. 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 Information Governance Sub Committees (IGSC)

5.3.1 Each CCG has a dedicated committee to undertake detailed scrutiny of information governance activities, including those relating to records management. The IGSCs are sub-committees of the Audit Committees.

5.3.2 The key roles and responsibilities of the IGSCs of the CCGs are included within the Information Governance Management Framework available at link).

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 Committees ratification;
- ensuring that appropriate records management related activities are included within the CCGs' annual IG Work & Improvement Programme;
- reviewing regular progress reporting with respect to the completion of records management related activities;
- setting and monitoring key performance indicators with respect to records management related activities; 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 records management related legislation and applicable requirements.

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 available at link). 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 legislative requirements relating to records management;
- identified owner of the policy;
- approval of any procedures related to this policy and changes to these;
- reviewing and approving the CCGs' Records of Processing; and
- receiving and reviewing reports regarding the outcomes of records management related reviews and audits undertaken for their CCG.

5.6 The Caldicott Guardian

5.6.1 Each CCG has a Caldicott Guardian. Their key roles and responsibilities are detailed within the Information Governance Management Framework (available at link). The Caldicott Guardians also have the following specific responsibilities with respect to this policy:

- reviewing Privacy Notices and Records of Processing for areas of the CCG which process personal data; and
- providing advice and guidance regarding records management issues relating to heath records of NHS service users.

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 available at link).

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

- ensuring Records of Processing for their activities include details of the relevant retention period;
- ensuring that records management requirements for the information assets they are responsible for are detailed within System Level Security Policies;
- ensuring that records management 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; and
- providing records management related assurance to the SIRO for the information assets they are responsible for.

5.8 Information Asset Administrators

5.8.1 Most CCGs' also have Information Asset Administrators (IAAs) who assist the IAOs to meet the responsibilities detailed above. IAAs may support:

- the development and update of CCG Privacy Notices and Records; and
- activity relating to records management 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 records management issues relating to the 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:

- managing 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;
- managing the process for development and update of CCG Privacy Notices and Records of Processing;
- supporting teams to complete Data Protection Impact Assessments for their activities;
- supporting IAOs to develop System Level Security Policies which detail applicable information quality requirements;
- providing advice and guidance regarding records management;
- undertaking Confidentiality Audits, which include records management related checks, and provide reports regarding the outcomes of these;
- supporting internal and external reviews and audits of information quality;
- managing the CCGs' IG incident reporting process; 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;
- ensuring that records management 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 records management are in place with all individuals / organisations engaged to undertake work on behalf of the CCG and commissioned services etc.;
- recieving and considering reports regarding the management of the records that their team create and use;
- where records management issues are identified for a record they are responsible for, ensuring that appropriate mitigation is undertaken; and
- receiving and considering reports regarding the outcomes of Confidentiality Audits undertaken for their team's activities.

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 records management related reviews or audits of 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 Background

6.1.1 Information is the key resource of the National Health Service (NHS) and the wider health economy; it enables the effective treatment of patients and the

management of the NHS system and the services we commission. Information Management requires the management of information from creation, use all the way through to destruction or archival retention.

6.1.2 Appropriate management of information enables an organisation, to reduce costs, improve efficiency and enhance the ability to monitor the performance of contracts and commissioned services. Understanding the information we hold and the way our organisation uses it helps us to manage our responsibilities under legislation, such as the Data Protection Act.

6.1.3 As a commissioner of services we require information to be appropriately created, managed and utilised by those we commission. The organisations are responsible for driving improvements in Information Governance from these services. This ensures an efficient, effective and accountable service supporting high quality healthcare and appropriate clinical decision making. In those instances where we appropriately share or publish information we must ensure that this done in a lawful and appropriate manner.

6.1.4 This policy sets out the CCG's information management principles, controls and standards in place for each stage of the information's lifecycle. Staff are responsible for maintaining these controls and standards.

6.1.5 The CCGs records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the organisation and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways. The CCGs Executive Management Team has adopted this records management policy and is committed to on-going improvement of its records management functions as it believes that it will gain a number of organisational benefits from so doing. These include:

- improved use of physical and server space;
- improved use of staff time;
- improved control of valuable information resources;
- compliance with legislation and standards; and
- reduction in costs.

6.1.6 The CCGs also believe that its internal management processes will be improved by the greater availability of information that will accrue by the recognition of records management as a designated corporate function.

6.2 Commitments

6.2.1 This policy includes the following records management related commitments which apply to the Surrey Heartlands' CCGs and all individuals undertaking work on our behalf:

- to have awareness of the importance of records management and evidence of responsibility and accountability for this at all levels;
- to maintain a systematic and planned approach to managing records throughout their lifecycle; which ensures that information within the organisation is of the highest quality in terms of completeness, accuracy, relevance, accessibility and timeliness;
- to have in place effective arrangements to ensure the confidentiality, security and quality of personal data and other confidential information both within the CCGs and its commissioned activities;
- to have in place a records management system that supports the CCG's effective compliance with statutory governance requirements and which supports the CCGs in making non-confidential information publicly available in line with responsibilities under the Freedom of Information Act 2000 and the Government's transparency agenda;
- to minimise as far as possible (financial and staff) costs associated with the management and storage of records and to achieve the best possible value for public funds for records management activity; and
- the proactive and appropriate use of information by the organisation and its partner organisations for the commissioning of care and the robust monitoring and evaluation of this activity.

6.3 Records Management Lifecycle

6.3.1 The Records Management Lifecycle is shown in figure 1 below:

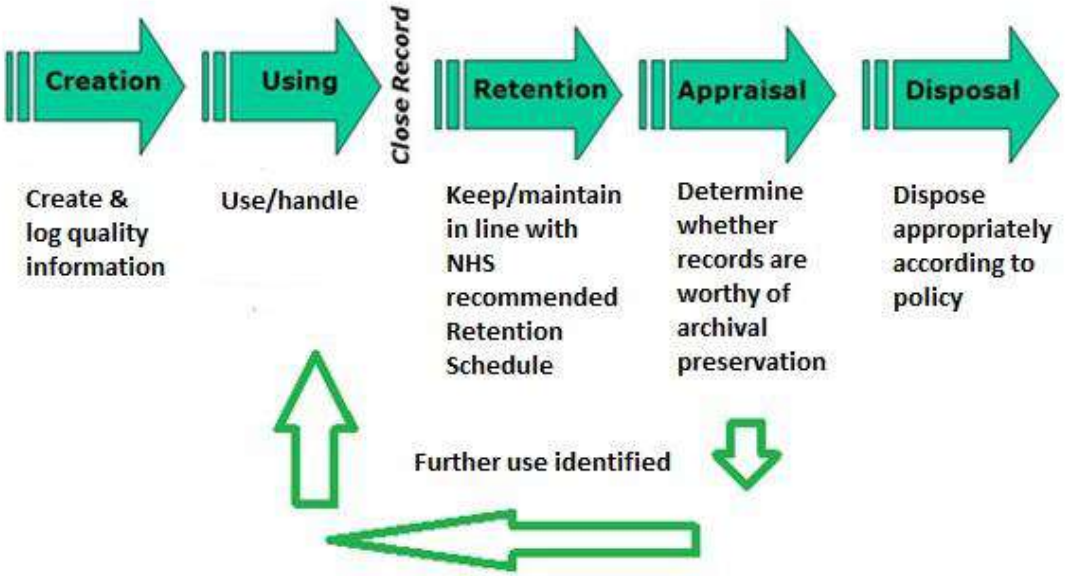

Figure 1: Records/Information Lifecycle published by the Information Governance Alliance, July 2016

6.3.2 Creation - Information when created must be authentic, accurate, accessible, complete, compliant, effective and secure and its integrity must be protected over time. At the point of creation, the relevant metadata (data about the data) needs to be captured to ensure its ongoing value and evidential weight.

6.3.3 Using - All information must be used consistently, only for the intentions for which it was intended and never for an individual employee's personal gain or purpose. If in doubt employees should seek guidance from their line manager and the Information Governance function. Evidential weight relies upon a clear audit trial and the ability to demonstrate that the context and content of information can be relied upon.

6.3.4 The following are key components of use:

- Retrieval – information must be accessible throughout its lifecycle for staff with authorised access and in line with access controls;
- Naming Conventions – a clear, systematic and consistent standard for naming information is required;
- Version Control – a clear, systematic and consistent method of controlling version of information is vital for effective management and efficient working;

- Storage- all information must be stored in systematic and consistent to be of use. Storage must also be Secure; and
- Mapped Information Flows - All Flows of personal confidential data must be in accordance with legal, regulatory and organisational requirements. Flows of information within the organisation and with external bodies will be mapped, ensured as lawful and the risks involved understood.

6.3.5 Retention - All information needs to be maintainable through time. The qualities of availability, accessibility, interpretation and trustworthiness must be maintained for as long as the information is needed, perhaps permanently, despite changes in the format.

6.3.6 Appraisal - Is the process of deciding what do with records when their business use has ceased, no record or series can be automatically destroyed or deleted. There will be one of three outcomes from appraisal:

- destroy / delete;
- to keep for a longer period; and
- to transfer to a place of deposit appointed under the Public Records Act 1958.

6.3.7 Disposal - Disposal is defined as the management intent for a record once it is no longer required for the conduct of current business. Data and information, not classified as a record, may be destroyed once its business value is concluded. There are a number of stages in the disposal phase of a corporate record which will be outlined in the Protocol on Records Management. These include:

- closure - records are made inactive and transferred to secondary storage;
- retention - The retention period varies dependant on the type of information being stored;
- destruction - All information and records must be destroyed appropriately. This applies across all media and to the systems that hold information (such as servers and encrypted memory sticks); and
- archiving - Upon the end of a retention period, information must be assessed for whether it is requires archiving or destroyed;

6.4 Authoritative Records

6.4.1 International Organization for Standardization (ISO) standard 15489-1:2016 relates to records management. This details the characteristics of authoritative records, as detailed in the table below:

Record characteristic	How to evidence
Authentic	• It is what it purports (claims) to be • To have been created or sent by the person purported to have created or sent it and • To have been created or sent at the time purported.
Reliable	• Full and accurate record of the transaction/activity or fact • Created close to the time of transaction/activity • Created by individuals with direct knowledge of the facts or by instruments routinely involved in the transaction /activity.
Integrity	• Complete and unaltered • Protected against unauthorised alteration • Alterations after creation can be identified as can the persons making the changes.
Useable	• Located, retrieved, presented and interpreted • The context can be established through links to other records in the transaction/activity.

6.5 Retention Schedules

6.5.1 Appendix 3 of the Records Management Code of Practice for Health and Social Care 2016 contains detailed retention schedules that set out how long records should be retained, either due to their ongoing administrative value or as a result of statutory requirement. The Surrey Heartlands CCGs will hold records we use for the periods specified in the applicable retention schedule.

6.6 Records of Processing

6.6.1 Data protection related legislation requires that all organisations hold, and can supply on request, detailed information regarding how it uses, shares, and holds personal data to supplement the summary information included within its Privacy Notice – these are known as it's Records of Processing (RoP).

6.6.2 All CCG teams will develop and maintain their own RoP using the standard template in place with the CCGs. Teams RoP will include details of the applicable retention period for the records they use as per the detailed retention schedules included within the Records Management Code of Practice for Health and Social Care 2016

6.7 Records at Contract Changes

6.7.1 Once a contract ends, any service provider still has a liability for the work they have done and as a general rule at any change of contract the records must be retained until the time period for liability has expired.

6.7.2 In the standard NHS contract there is an option to allow the commissioner to direct a transfer of care records to a new provider for continuity of service and this includes third parties and those working under any qualified provider contracts.61 This will usually be to ensure the continuity of service provision upon termination of the contract. It is also the case that after the contract period has ended; the previous provider will remain liable for their work. In this instance there may be a need to make the records available for continuity of care or for professional conduct cases.

6.7.3 Details information can be found at Table 6 - Records at Contract Change Scenarios included within the Records Management Code of Practice for Health and Social Care 2016.

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:

- ISO 15489-1:2016 - Information and documentation - Records management available at link
- 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 at link
- UK legislation at link

9. Appendix 1 Related Documents

This policy links to the following key documents:

Related policies

Other Surrey Heartlands CCG IG related policies as detailed below;

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

IG related procedures

This policy links to the following key IG related procedures:

- Procedure for Handling Information Rights Related Requests;
- Data Protection Impact Assessment Procedure; and
- IG Incident Management Procedure
- Secure Transfers of Data (see section 7.34 of the Information and Cyber Security Policy)

Guidance Documents

Further guidance is also available via the information governance team:

- What you need to know about IG;
- Information Asset Owners Handbook.

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	Audit Committee ratification 19/07/19
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/ 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
RM 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
RM 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 RM requirements	If RM requirements included	Annual	Audit Committees and IG Sub Committees	Reviews of system level security policies (SLSPs)
Data protection impact assessments include IQ requirements	If RM requirements included	Annual	Audit Committees and IG Sub Committees	Reviews of data protection impact assessments (DPIAs)
Reviews and audits of compliance with RM 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