NHS
Herts Valleys
Clinical Commissioning Group

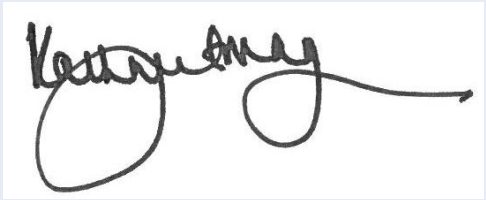
Checklist for the Review and Approval of Procedural Documents

To be completed and attached to any document which guides practices when submitted to the appropriate committee for consideration and approval.

	Yes/No/ Unsure	Comments
Title of Document		Information Lifecycle Management Policy
Could this policy be incorporated within an existing policy?	no	
Does this policy follow the style and format of the agreed template?	Yes	
Has the front sheet been completed?	Yes	
Is there an appropriate review date?	Yes	
Does the contents page reflect the body of the document?	Yes	
Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes	
Are all appendices appropriate and/or applicable?	Yes	
Have all appropriate stakeholders been consulted?	Yes	
Has an Equality Impact Assessment been undertaken?	Yes	
Is there a clear plan for implementation?	n/a	
Has the document control sheet been completed?	Yes	
Are key references cited and supporting documents referenced?	Yes	
Does the document identify which Committee/Group will approve it?	Yes	

Plans for communicating policy to – staff; practice membership; public (as appropriate)		Via weekly staff briefing

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Chief Finance Officer	Date	07/08/17
Signature			

Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	Chief Executive Officer	Date	07/08/17
Signature			

NHS
Herts Valleys
Clinical Commissioning Group

Information Lifecycle Management Policy, Procedure and Strategy

Version Number	V2
Ratified By	Risk Management Group
Date Ratified	**August 2017**
Name of Originator/Author	Information Governance Manager
Responsible Director	Chief Finance Officer
Staff Audience	All Staff
Date Issued	August 2017
Next Review Date	August 2018

DOCUMENT CONTROL

Plan Version	Page	Details of amendment	Date	Author
V2		Annual Review Policy added to new format and general review	Dec 2016	IG Manager
		Approved by Risk Group	08/02/2017	

CONTENTS

Appendices:

1. INTRODUCTION

Information is essential to the delivery of high quality evidence based healthcare and administrative support functions on a daily basis.

NHS bodies must ensure record management policies and procedures are fully complaint with the current UK legislation and NHS requirements as detailed in “Records Management – NHS Code of Practice” and the Information Governance Toolkit. This includes the standards contained with the Data Protection Act 1998 and the Freedom of Information Act 2000.

An organisation wide Lifecycle Policy and Records Management Policy is necessary for identifying the resources needed to ensure records of all types are properly controlled, tracked, accessible and available for use and eventually archived or otherwise disposed of in line with the principles contained within legal requirements and guidelines.

2. PURPOSE

This document sets out the organisation policy regarding all types of records. The CCG will develop appropriate processes and procedures for the management of its records, including the secured destruction of the record.

Many of the CCG’s business activities are subject to legal provisions, regulations and Department of Health standards which specify the way in which information must be recorded and presented e.g. financial records.

These provisions are acknowledged and this document does not direct employees to act otherwise than in accordance with the relevant law, regulations and guidance.

Records for an organisation’s 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 CCG and the rights of staff and members of the public. They support consistency, continuity, efficiency, productivity and help deliver services in consistent and equitable ways.

3. DEFINITIONS

Information Lifecycle Management is the policies, processes, practices, services and tools used by an organisation to manage its information through every phase of its existence, from creation through to destruction and archiving. Record management policies and procedures form part of the organisation's Information Lifecycle Management, together with other processes, such as records inventory, secure storage and records audit.

The main principles of Information Lifecycle Management are:

- That it applies to information in paper and other physical forms e.g. electronic, microfilm, negatives, photographs, audio or video recordings and other assets.
- That it relates to the five distinct phases in the life of information; creation, retention, maintenance, use and disposal.

A record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of NHS employees, examples include:

- Patient health records (electronic paper based)
- Administrative records (e.g. personnel, estates, financial and accounting records; notes associated with complaint handling etc.)
- X-ray and imaging reports, photographs and other images.
- Microfilm (i.e. fiche/film)
- Audio and videotapes, CCTV footage, CD-ROM, DVD etc.
- Computer databases, output portable storage media and all other electronic records
- Emails
- Material intended for shorter more transitory use, including notes and spare copies of documents.

NB This list is not exhaustive.

4. ROLES AND RESPONSIBILITIES

The CCG recognises it has responsibility for ensuring it corporately meets its legal responsibilities and for the adoption of internal and external governance requirements.

4.1 Roles and Responsibilities within the Organisation

Chief Executive

The CE has overall responsibility for records management within the CCG. As Chief Executive they are responsible for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate accurate information is available as required.

Caldicott Guardian
The Caldicott Guardian has responsibility for reflecting patients' interests regarding the use of patient information and is the conscience of the organisation. They are responsible for ensuring patient identifiable data is shared in an appropriate and secure manner.

Senior Information Risk Owner (SIRO)
The SIRO is concerned with identifying and managing the information risks to the organisation with its business partners. This will include oversight of the organisation's information security incident reporting and response arrangements. The SIRO will be supported in their role by one of more Information Asset owners who have assigned responsibility for the information assets of the organisation.

Information Governance Manager
The Information Governance Manager is responsible for the overall development and maintenance of record management practices throughout the organisation; in particular for drawing up guidance for good records management practice and promoting compliance with this policy in such a way to ensure the easy, appropriate and timely retrieval of information.

Risk Management Group
Is the group which will own and report any records management issues to the Audit and Quality & Performance Committees which provide assurance to the Board.

Information Asset Owner (IAO)
The Information Asset Owner is a senior member of staff who is the nominated owner for one or more identified information assets of the organisation. It is a core information governance objective that all information assets of the organisation are identified and that the business importance of those assets is established.

There may be several IAOs within the CCG, whose departmental roles may differ. IAOs will work closely with other IAOs of the CCG to ensure there is a comprehensive asset ownership and clear understanding of responsibilities and accountabilities. This is especially important where information assets are shared by multiple parts of the organisation. IAOs will support the CCG SIRO in their overall risk management function as defined in the organisation's policy.

Information Asset Administrator (IAA)

Responsibilities for the Information Asset Administrator (IAA) duties is aligned with a role and not a person and will pass over as and when the incumbent changes. IAAs will provide support to their IAO to:

- Ensure that policies and procedures are followed
- Recognise potential or actual security incidents
- Consult their IAO on incident management
- Ensure their information asset registers are accurate and maintained and up to date

Specific responsibilities of an IAA include:

- Update the Information Asset Register on an ongoing basis and perform annual review to update or amend as necessary
- Ensure compliance with data sharing agreements for assets that sit on your register
- Ensure information handling procedures are fit for purpose and are properly applied
- Under the direction of the IAO ensure that person identifiable information are wither pseudonymised, anonymised or encrypted and transferred through safe haven channels or by NHS mail.
- Recognise any new information handling requirements e.g. a long used process changes such as local NHS mail accounts or e.g. a new form of information flow is identified and ensures that the responsible IAO is consulted over appropriate procedures.
- Recognise potential or actual security incidents and consult with the responsible IAO or in their absence the SIRO.
- Report to your IAO on the current state of the assets that you are responsible for.
- Under the direction of the IAO ensure that information is securely destroyed when there is no further requirement for it.

An IAO/IAA training course has been developed by the IG Team and is available to CCG staff.

4.2 Consultation and Communication with Stakeholders

This policy will be approved by the Risk Management Group, Senior Leaders Team and Exec.

5. Creation and Registration of Records

All staff

All staff who create, receive and use records have record management responsibilities. In particular all staff must ensure they keep appropriate records of their work and manage those records in keeping with this policy

and any guidance subsequently produced.

Creation and registration of records

Records are created to ensure that information is available within the CCG:

- To protect staff and patients – "if it isn't recorded, it didn't happen"
- To support the care process and continuity of care
- To support the day to day business and administrative processes
- To support sound clinical and administrative decision making
- To ensure sound corporate governance processes are achieved to meet legal requirements
- To assist the performance management and audit processes (clinical and non-clinical)
- To support improvements in clinical effectiveness through research and evidence based care.
- Is there a justified need for information in whatever media in which it is required.

Record registration and record keeping

Each record or file must be registered by having a unique identifier e.g. subject matter, patient identifier etc. Where appropriate, records should be compiled in date order, placed in a suitable folder (manual or electronic), held in an accessible system with details regarding storage location.

Guidance on records management and archiving for the CCG is contained within Appendix 1 of this document.

Person identifiable and sensitive data

Manual or electronic records or record systems (this includes files, indexes, databases, correspondence, lists etc. holding person identifiable information (names, addresses, data of birth, salary etc.) are specifically covered by the requirements of the Data Protection Act 1998. Release or sharing of such data is restricted and all reasonable precautions must be taken to safeguard this type of data.

The CCG is committed to protecting the confidentiality of person identifiable data and meeting the requirements of the Act. Unauthorised release of personal data could result in disciplinary or legal action being taken against the staff involved.

Under no circumstances should person identifiable or sensitive data be left in view e.g. on a computer screen at a vacant desk, on top of a desk, in tray or on view in a vehicle. Records should be stored securely in either a locked cabinet/container or within a secure environment on a computerised system.

Person identifiable data or sensitive data must not be stored on the local hard drove of a computer/laptop.

Staff wishing to record, relocate, transport, share or transport person identifiable data or sensitive data need to contact the IG Team in the first instance.

Transportation of records

Guidance on the secure transfer of electronic and paper files and documents can be obtained from the IG team.

Manual records should be transported in an appropriate sealable container, envelopes, transit pouches or boxes. Lockable Envopak storage bags can be obtained from the IG team. Records should never be left unattended. If being transported in a car they should be locked away in the boot.

Electronic records

The CCG will develop and refine procedures and protocols for the security, access, use (including sharing and transport) auditing, storage and archiving of electronic records incorporating NHS requirements and best practice. Electronic records must not be stored on the hard disk drive of a PC. They should be saved to a dedicated place on the I.T network, with suitable access controls. This will ensure routine security; disaster recovery and business continuity measures are in place to safeguard the records. Highly confidential or sensitive records must have appropriate security, access and business continuity controls applied. Where the possibility exists that records could be used in a legal case, particular standards apply and the advice of the IG team must be sought and applied.

Mobile working and remote access to records

Mobile and remote working is becoming more commonplace. Accessing records using these types of technology requires the use of specific and effective safeguards**.** The Mobile Devices Policy provides procedures for the issue and use of mobile devices.

Retention periods for records

It is a fundamental requirement that all of the organisations records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend upon the type of record and its importance to the organisation's business functions.

The CCG has adopted the retention periods set out in the Information Governance Alliance Record Management: Code of Practice for Health and

Social Care 2016. Where further clarification is required, after thorough research and with approval of the IG team, different timescales may be incorporated.

Archiving of manual records

The Corporate Support team is the first point of contact for any department wishing to archive new records or retrieve records from storage

Dealing with lost or misplaced records

If any record containing person identifiable or sensitive data is lost, every effort must be made to retrieve it. If this proves unsuccessful:

- Inform your line manager
- Contact the IG team and complete an incident form

Confidential Waste/Shredder

The Data Protection Act 1998 states the correct procedures must be taken to protect personal data. All confidential material must be disposed of in a secure way either in a confidential waste bin or by use of a cross shredder. For disposal of electronic media the East and North Hertfordshire CCG HBL ICT Services will arrange safe disposal.

Development Process

As part of IG compliance requirements, the IG team will conduct an annual audit of the CCG's record management policies for compliance with this framework.

The audit will:

- Identify areas of operation covered by the CCG's policies and identify which procedures should comply with the policy
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records and use a subsidiary development plan if there are major changes to be made;
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance and;
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

The results of the audit will be reported to the CCG Risk Group.

6. MONITORING COMPLIANCE

The Policy will be monitored by the IG team and the CCG Risk Group.

It is the responsibility of all CCG staff to ensure compliance with this policy and procedure.

All staff need to protect patient confidentiality and they are reminded they may be subject to disciplinary action if they breach the DPA 1998. The Information Commissioner's office has made it clear they will impose fines on organisations and individuals for serious breaches of the Data Protection Act 1998.

7. EDUCATION AND TRAINING

All staff should undertake annual mandatory information governance training either via www.hscic.gov.uk web portal, via OLM or by contacting the IG team.

8. REFERENCES

NHS Records Management Code of Practice
Records Management Code of Practice for Health and Social Care 2016
Data Protection Act 1998
Freedom of Information Act 2000

9. ASSOCIATED DOCUMENTATION

Information Governance Policy
Safe Haven Policy
Information Security
Data Protection and Confidentiality Policy
Email and Internet Policy

Appendix A - HVCCG Equality & Quality Inclusion Analysis Form

Equality Analysis - Equality Impact Assessment Screening Form

Very occasionally it will be clear that some proposals will not impact on the protected equality groups and health inequalities groups.

Where you can show that there is no impact, positive or negative, on any of the groups please complete this form and include it with any reports/papers used to make a decision on the proposal.

Name of policy / service	Information Lifecycle Policy
What is it that is being proposed?	This organisation wide Lifecycle Policy and Records Management Policy is necessary for identifying the resources needed to ensure records of all types are properly controlled, tracked, accessible and available for use and eventually archived or otherwise disposed of in line with the principles contained within legal requirements and guidelines.
What are the intended outcome(s) of the proposal	That all staff are aware of the process to follow.
Explain why you think a full Equality Impact Assessment is not needed	This is a document to help staff to ensure that the document follows the correct lifecycle management.
On what evidence/information have you based your decision?	That this is guidance for staff to ensure that documents lifecycles follow the correct legislation.
How will you monitor the impact of policy or service?	Via reported data losses/breaches or near misses.
How will you report your findings?	Via the Risk Group meetings/ the SIRO and IG Toolkit (if a level 2 data breach)

Having considered the proposal and sufficient evidence to reach a reasonable decision on actual and/or likely current and/or future impact I have decided that a full Equality Impact Assessment is not required.

Assessors Name and Job title	Ruth Boughton – IG Manager Paul Curry - Equality & Diversity Manager
Date	2nd May 2017