NHS
North East Hampshire and Farnham
Clinical Commissioning Group

Records Management Policy

Document information

Document type:	Operational Policy
Document reference:	
Document title:	NHS North East Hampshire and Farnham Clinical Commissioning Group (CCG) Records Management Policy
Document date:	November 2015
Author:	NHS South, Central and West Commissioning Support Unit, Information Governance Team
Equality Impact Assessment	The content of this policy does not raise any equality and diversity issues in relation to the protected characteristics
Approved by:	Corporate Review Group
Approval date:	11 January 2016
Version:	V2.0
Review date:	November 2017

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1		4	Update staff responsibilities to include temporary or honorary contracts, agency staff and students	November 2015
2		6	Inclusion of data quality guidance	November 2015
3		9	Inclusion of CCG compliance action statement	November 2015
4		Appendix 1 pages 11 & 12	Updated secure folder information, page 11. Update offsite storage information page 12.	November 2015
		Throughout document	References to South CSU removed, replaced with South Central & West CSU	November 2015

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Name of Reviewer	Ratification Process	Notes
2	November 2015	Jackie Thomas, CSU IG Manager		Reviewed at due date

Summary

This Policy is written to give NHS North East Hampshire and Farnham Clinical Commissioning Group (CCG) a clear Records Management framework which includes advice and guidance and to inform staff of their operational and legal responsibilities.

Consultation

The Policy has been considered by the CCG Audit and Risk Committee which includes the Senior Information Risk Officer. Comments have been incorporated as appropriate.

Contents

1. Introduction

1.1 Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through to their lifecycle to their eventual disposal.

1.2 The Records Management: NHS Code of Practice© has been published by the Department of Health as a guide to the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England. It is based on current legal requirements and professional best practice.

1.3 Records within the NHS can be held in paper or electronic form. All NHS organisations will have a duty to ensure that their record systems, policies and procedures comply with the requirements of the Care Record Guarantee.

1.4 The CCG 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.

1.5 In adopting this Policy, the CCG 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:

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

1.6 The CCG also believes 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.

1.7 This document sets out a framework within which the staff responsible for managing the CCG's records can develop specific policies and procedures to ensure that records are managed and controlled effectively, and at best value, commensurate with legal, operational and information needs.

1.8 It is the responsibility of all staff including those on temporary or honorary contracts, agency staff and students to comply with this policy.

2. Scope and Definitions

2.1 This policy relates to all records held in any format by the CCG.

2.2 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, including:

- All administrative records (e.g. personnel, estates, financial and accounting records, records associated with complaints
- All patient health records (for all specialties and including private patients, including x-ray and imaging reports, registers, etc.)
- computer databases, output and disks, and all other electronic records
- material intended for short term or transitory use, including notes and spare copies of documents
- meeting papers, agendas, formal and information meetings including notes taken by individuals in note books and bullet points and emails
- audio, video tapes, cassettes and CD ROMs

This list is not exhaustive.

2.3 Records Management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the CCG and preserving an appropriate historical record. The key components of records management are:

- record creation;
- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and transfer;
- appraisal;
- archiving; and
- Disposal.

2.4 The term **Records Life Cycle** describes 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 confidential disposal or archival preservation.

2.5 In this policy, Records are defined as 'recorded information, in any form, created or received and maintained by the CCG in the transaction of its business or conduct of affairs and kept as evidence of such activity'

2.6 Information is a corporate asset. The CCG's records are important sources of administrative, evidential and historical information. They are vital to the organisation in order to support its current and future operations (including meeting the requirements of Freedom of Information legislation), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

3. Processes/Requirements

3.1 The aims of our Records Management System are to ensure that:

- **records are available when needed** - from which the CCG is able to form a reconstruction of activities or events that have taken place;
- **records can be accessed** - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist;
- **records can be interpreted** - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records;
- **records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;
- **records can be maintained through time** – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format;
- **Records are secure** - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required;
- **records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and
- **Staff are trained** - so that all staff are made aware of their responsibilities for record-keeping and record management.

4.0 Data Quality

4.1 Part of records management involves ensuring records are of a sufficient quality.

To ensure the CCG has good quality data it must be:

- complete (in terms of having been captured in full)
- accurate (the data must be recorded factually, legibly and consistently)
- relevant (the degree to which the data meets current and potential user's needs)
- accessible (available when needed)
- timely (recorded and available as soon after the event as possible)

Good quality data will be used by the CCG to support risk minimisation, clinical and corporate governance and ultimately effective patient care. This will be achieved by setting and meeting the standards contained within this policy and ensuring all staff are aware of their responsibilities regarding data quality.

Data quality issues should be raised via the CCG's incident reporting procedure and regular spot checks should be carried out to ensure records are of a sufficient quality.

To ensure both clinical and corporate records are kept at a high quality they should be audited on an annual basis to identify any areas that need improving.

5. Legal and Professional Obligations

5.1 All NHS records are Public Records under the Public Records Acts. The CCG will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice, in particular:

- The Public Records Act 1958;

- The Data Protection Act 1998;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality; and
- The NHS Confidentiality Code of Practice
- The NHS Care Record Guarantee and
- Any new legislation affecting records management as it arises.

6. Responsibilities

6.1 The CCG has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements

6.2 NHS North East Hampshire and Farnham Clinical Commissioning Group Chief Officer

6.2.1 The CCG Chief Officer has overall responsibility for governance in the CCG. As accountable officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity

6.3 NHS North East Hampshire and Farnham Clinical Commissioning Group Caldicott Guardian

6.3.1 The CCG's Caldicott Guardian has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner.

6.4 NHS North East Hampshire and Farnham Clinical Commissioning Group Senior Information Risk Officer

6.4.1 The CCG Senior Information Risk Officer (SIRO) is responsible for leading on Information Risk. For ensuring the Corporate Risk Management process includes all aspects of Information risk and for ensuring the CCG Audit and Risk Committee is adequately briefed on information risk issues.

6.5 Head of Information Governance – Commissioning Support South, Central & West

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

6.6 NHS North East Hampshire and Farnham Clinical Commissioning Group Managers

6.6.1 The responsibility for local records management is devolved to the relevant directors, directorate managers and department managers. Heads of Departments, other units and business functions within the CCG have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records

controlled within their unit are managed in a way which meets the aims of the CCG's records management policy.

6.7 NHS North East Hampshire and Farnham Clinical Commissioning Group Staff

6.7.1 All CCG staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in the CCG and manage those records in keeping with this policy and with any guidance subsequently produced.

6.8 NHS North East Hampshire and Farnham Clinical Commissioning Group Audit and Risk Committee

6.8.1 The Audit and Risk Committee is responsible for overseeing Information Governance on behalf of the CCG's Governing Body.

6.9 NHS North East Hampshire and Farnham Clinical Commissioning Group Senior Management Team

6.9.1 The CCG's Senior Management Team is responsible for ensuring that this policy is implemented and that the records management system and processes are developed, co-ordinated and monitored.

7. Training

7.1 All CCG staff will be made aware of their responsibilities for record-keeping and record management through generic and specific training programmes and guidance.

8. Retention and Disposal Schedules

8.1 It is a fundamental requirement that all of the CCG's 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 on the type of record and its importance to the CCG's business functions**.**

8.2 The CCG has adopted the retention periods set out in the Records Management: NHS Code of Practice. The retention schedule will be reviewed as appropriate by NHS England.

9. Success criteria

9.1 The Information Governance Action Plan which includes Records Management will be monitored by the CCG Senior Management Team and reported by exception to the Audit and Risk Committee.

9.2 A regular audit of records management functions will be undertaken by Data Custodians.

9.3 The audit will:

- Identify areas of operation that are covered by the CCG's policies and identify which procedures and/or guidance should comply to 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;
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

9.4 The results of audits will be reported to the CCG Audit and Risk Committee.

9.5 Appendix 1 of this Policy can also be used to audit teams.

10. Reference Documentation

- The Public Records Act 1958;
- The Data Protection Act 1998;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality; and
- The NHS Confidentiality Code of Practice

10.1 The CCG will also take action to comply with any new legislation affecting records management as it arises.

11. Equality, diversity and mental capacity

11.1 This policy was assessed against the CCG Impact Needs Requirement Assessment (INRA) tool to ensure that it does not introduce any unexpected or unwarranted equality and diversity disparities. The assessment confirmed that no amendments are required at this time.

11.2 This policy has been assessed and meets the requirements of the Mental Capacity Act 2005.

12. Monitoring and Audit

12.1 This policy will be monitored and reviewed by the Corporate Review Group to ensure any legislative changes that occur before the review date are incorporated. All exceptions will be reported to the CCG Audit and Risk Committee. This policy will also be reviewed every 2 years.

13. Communication and dissemination

13.1 This policy will be communicated and disseminated by means of the CCG Intranet. Additional/alternative dissemination arrangements will be included as they become available.

Appendix 1

Corporate Records Management Guidance

Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through to their lifecycle to their eventual disposal. It is the aims of the organisation to ensure that records are accurate and reliable, can be retrieved swiftly and kept for no longer than necessary.

Corporate Records can be considered records which contain the following:

- all administrative records (e.g. personnel, estates, financial and accounting records, notes associated with complaints);

Records Management will also help Data Custodians with the Information Asset audit and the information flow mapping exercise.

Corporate Records

Records management is crucial to all NHS organisations, especially during a time of transition. If records are not managed effectively, the organisation would not be able to function as required and expected, and to account for what has happened in the past or to make decisions about the future. Records are a fundamental corporate aspect and are required to provide evidence of actions and decisions, enable the organisation to be accountable and transparent, and comply with legal and regulatory obligations such as the Data Protection Act 1998 and the Freedom of Information Act 2000.

Corporate records also support the strategic decision making and enables the organisation to protect the interests of staff, patients, public and other stakeholders.

Corporate Records should:

1. be accurate and complete
2. be relevant and accessible
3. be arranged systematically
4. should be sufficient to enable other members of staff to carry out their tasks
5. Should demonstrate compliance with legal and regulatory requirements

Paper Records

1. A uniform filing system should be implemented to ensure that documents are grouped appropriately and consistently. Records that are frequently used should be stored within secure filing cabinets or secure areas (locked rooms, coded areas). Records that are not frequently or not used at all should be stored in secure rooms or in approved off-site storage facilities. If records are no longer needed and do not need to be kept according to the retention timeframes, the records should be destroyed.
2. The filing system should also be kept simple and easy for all to understand. Operating procedure is a method used to ensure that all staff within your assigned area can follow the same filing procedure.
3. Should you have many categories associated to the same record, cross – referencing is a key element to identify documentation which is connected to the same record.

4. It should also be discussed with line management whether records are to be kept manually or electronically. This will help determine the definitive record.
5. It is best to restrict 'creating folder responsibility' to limited amount of staff. If all members of staff create files, then there is a possibility of duplication, loss of information and more storage space would be required. Should a member of staff require a new folder to be created, they will need to be granted permission from the lead administrator.
6. Paper files should be labeled accurately and helpfully. Labels should be brief, accurate, have a meaningful description of the contents, and intelligible to both current and future members of staff.
7. Where appropriate templates should be used.
8. Version controls should be applied and periodically reviewed.
9. All paper files should be reviewed at the end of every financial year. This will identify if records need to be retained, archived or destroyed. It would be useful to have a tracker card to include who uses the file, location of where the file is situated and also retention review date.
10. Should the file contain personal identifiable or sensitive information, it is important not to add this to the title of the record and should be kept in a secure location. Page numbering confidential files will confirm if pages have been removed or are missing.
11. Permission to access personal identifiable and sensitive information should be restricted to a limited number of staff who requires access.
12. Information Asset audits should be carried out, this will prevent duplication and provide easier access to information readily for requests/enquiries
13. Records should be review on a periodic basis to ensure that destruction rules apply.

14. Electronic Records

1. Name electronic files accurately; they should be simple and easy for all to understand. Operating procedure is a method used to ensure that all staff within your assigned area can follow the same filing procedure.
2. It is best to restrict 'creating or deleting folder responsibility' to limited amount of staff. If all members of staff create files, then there is a possibility of duplication, loss of information and more storage space would be required. Should a member of staff require a new folder to be created, they will need to granted permission from the lead administrator.
3. All electronic files should be reviewed at the end of every financial year. This will identify if records need to be retained, archived (Zipped in secure folder).
4. Each assigned area should compile a list of standard terms and uniform terminology as naming conventions for files and folders.
5. Version controls should be applied and periodically reviewed.
6. Records with personal identifiable and sensitive information should be controlled through the use of logins, password protection and encryption. Please review the organisation Information Security Policy.
7. Once a project is completed, all associated electronic documentation should be contained in a Zipped file, accurately named/dated and stored within a secure folder on the organisation network. This will decrease storage space and will keep all common documentation together.
8. Computers that hold confidential information should be located in rooms that have lockable doors or if not possible should be secured to the desktop. Laptops and portable devices must be encrypted and stored securely out of sight.
9. Consideration should be given to security prior to adopting a filing structure containing personal confidential data. Use secure folders with the minimum number of staff able to access them and avoid the possibility of inappropriate access by attempting to isolate secure folders to enable appropriate authorisation processes for

access. Access to such records should have strict controls in place for staff that have a legitimate purpose to view them.

Record Keeping Audit.

One of the responsibilities of Data Custodians is to conduct a record keeping audit. The information collected from the audit will enable the assigned Data Custodian;

- To understand what records are available within the department
- Assess the staff knowledge of records management
- Identify if the organisation's records management policy and procedures are adhered to by staff and have been implemented within your assigned area.
- Identify any gaps in record management processes
- To help collate information for the information asset register and the information mapping exercise.

Archiving, Retention and Disposal Process including Off-site Storage

To avoid breaches, incidents and information loss, it is important for departments to ensure that retention, retrieval and disposal procedures are followed. One of the responsibilities as Data Custodian is to coordinate this function within your assigned area. By using the outcomes from the audits and the data mapping exercise, Data Custodians will have the knowledge of what type and how long records need to be kept. Members of staff may also ask you to coordinate the archiving and disposal of records.

The CCG currently has offsite storage facilities with PHS Records Management. Should this be required all staff are expected to comply with any process and procedures established for the archiving of CCG information and data. Requests to use the offsite storage facilities should be directed to the CCG Governance Team and CSU IG Lead.

Data Custodians have the responsibility to ensure effective and relevant file management systems are in place for information held within their teams. Following this process will avoid teams duplicating or, mismanaging information therefore ensuring information security.

Each team should have a programme of archiving for records held onsite. The following options should be used when considering records for destruction:

1. **Confidential Shredding.** Teams should ensure all confidential documents are disposed of confidentially. Staff have access to designated shred it confidential waste boxes. Confidential waste is shredded on a regular basis by an approved contractor. Confidential waste should not disposed of within recycling and personal waste bins. Black bin liners should not be used to store or dispose of confidential information.

2. **Destruction of Electronic Equipment**

   All electronic equipment that store personal and sensitive information i.e. CDs, DVD –Roms, USB sticks, computers etc. require specialist destruction. It is important to follow the CCG's hosted IT provider's Information Security destruction process.

Should you have any queries or would like to request destruction of electronic equipment, please contact your IT provider service desk.

What to do in the Event of Missing Health and Corporate Records.

Missing records are a serious risk to the organisation and it is therefore vital that a tracing procedure is undertaken. Should information go 'missing' the following procedures should be followed.

1. Highlight the that a record is 'missing' to the assigned Information Asset Owner (IAO) and work colleagues as soon as this becomes apparent.

2. Undertake a thorough search for the record in the places you would normally expect to find it. Search in the place you would normally expect to see the record but look either side, above and below where it should be filed. If the record is held electronically search in other folders or conduct a 'search' within your files.

3. Should the record remain missing after your search, you will need to contact the CCG IG Team and complete a Risk Incident/Adverse Event form, and follow the Risk management process.

4. Keep a list of all the places that have been searched

5. The Senior Information Risk Owner (SIRO) /Caldicott Guardian should be informed of the loss by the CCG IG Team.

The Information Asset Owner (IAO) and CCG IG team should be informed if the record is found