North West London
Collaboration of
Clinical Commissioning Groups

Corporate Records Management Policy

Document Reference Information

Version	1.1
Status	Approved
Approving Committee	BHH CCGs Federation Operational Committee
Author/Lead	Head of Governance
Date Effective	July 2017
Date of Next Formal Review	March 2019
Version	1.2
Status	Approved
Reviewer	Data Protection Officers (Corporate & GPs)
Approving committee	NWL CCGs Governing Bodies
Date Effective	September 2020
Date of Next Formal Review	June 2021

Version	Description of Change(s)	Reason for Change	Author	Date of revision
1.0	First approved version		Risk and Information Governance Manager	November 2014
1.1	Editorial	The organisation name and logo was changed to reflect the current arrangement. The reference link was also changed to reflect supporting document	IG Manager	July 2017
1.2	Annual Review	Logo changed to NWL, added GDPR 2016 and Data Protection Act 2018 updates	Data Protection Officers (Corporate & GPs)	June 2020
1.2	Review	N/A	SIRO	August 2020

To be read in conjunction with

- Confidentiality Policy
- Information Security Policy
- Incident Reporting and Management Policy
- Subject Access Request Policy
- Freedom of Information Policy
- Acceptable Use of Email Policy
- Policy Development Policy

CONTENTS

1. INTRODUCTION

Records Management is the process by which an organisation manages all aspects of its records, whether internally or externally generated regardless of format or media type, from their creation and throughout 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 The records of CCGs' are its corporate memory, providing evidence and support of managerial actions and decisions taken whilst also representing a vital asset to support daily functions and operations. This approach also serves to protect the interests of CCGs, the rights of patients, staff and members of the public. Accurate records support's consistency, continuity, productivity and assists in the delivery of services in dependable and equitable ways.

1.4 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 standard
- Reduced costs.

1.5 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.

1.6 This document sets out a framework within which staff responsible for managing 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.

2. SCOPE AND DEFINIATIONS

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

- The Public Records Act 1958;
- The General Data Protection Regulation 2016 (GDPR)
- The Data Protection Act 2018;
- The Freedom of Information Act 2000;
- The Common Law Duty of Confidentiality; and
- The NHS Confidentiality Code of Practice.
- And any new legislation affecting records management as it arises.

Since NHS bodies must ensure that records management and keeping policies and procedures are fully compliant with legislation, the CCG has a statutory duty to make arrangements for the management and keeping of their records.

2.2. 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 including:

- Administrative records (e.g. personnel, estates, financial and accounting records; notes associated with complaint-handling)
- Audio and videotapes, cassettes, CD-ROM etc.
- Computer databases, output, and disks etc., and all other electronic records
- Material intended for short term or transitory use, including notes and 'spare copies' of documents

2.3 This policy relates to all non-clinical operational records held in any format and includes but is not limited to: diaries, emails, correspondence, personnel, estates, financial and accounting records, contracts, complaints, records of meetings, policies and procedures.

2.4 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 (see Appendices 1, 2 & 3):

- Record creation;
- Record maintenance (including tracking of record movements);
- Access and disclosure;
- Closure and transfer;
- Appraisal;
- Archiving; and
- Disposal.

2.5 The term **Records Life Cycle** describes the life of a record from its creation/receipt through the period of its 'active' use, a period of 'inactive' retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

2.6 Information is a corporate asset. Records are important sources of administrative, evidential and historical information. They are vital to support the CCG's 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. AIMS OF THE POLICY

3.1 The aims of this policy are to ensure that:

- **Records are available and can be accessed when needed** – records and the information within them can be located and displayed in a way consistent with their use. 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, when this occurred, 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** – records must remain available, and accessible, with the ability to be interpreted and trusted 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 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, in line with NHS Corporate Records Retention guidelines
    - **Staffs are trained** – to be aware of their responsibilities for record-keeping and record management.

4. ROLES AND RESPONSIBILITIES

4.1 Accountable Officer

The AO has overall responsibility for records management.

4.2 Senior Information Risk Owner (SIRO)

The SIRO is responsible for providing advice relating to information risks and incidents and to provide a focal point for the resolution and/or discussion of information risk issues within the CCG.

The SIRO will also ensure that the approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.

4.3 Information Asset Owners (IAOs)

IAOs are responsible for understanding what information is held, added, moved, removed, who has right of access and why. IAOs must ensure that the information held/managed is done so in accordance with policies and legislation.

4.4 Caldicott Guardian

The Caldicott Guardian is responsible for governing and safeguarding recorded patient information in regards to how it is used. This includes responsibility for monitoring and approving the CCGs' guidelines and protocols in respect to the sharing, handling and management of confidential information and to act in an advisory role for staff processing Subject Access Requests.

4.5 Information Governance Lead

The CCG's IG Lead has responsibility for supporting all policies and procedures in relation to information governance agendas and strategies.

4.6 Managers

All managers have overall responsibility for records management in their work areas and are expected to have an up-to-date knowledge of the legal requirements and guidelines concerning record management.

All Managers must maintain standards by:

- Ensuring all staff are aware of this policy in addition to the policies, procedures and best practice guidance contained within the guidance supplied by professional bodies
- Ensuring that all staff complete training relating to confidentiality and information sharing
- Identifying areas where improvements should be made and taking remedial action by way of risk assessment.
- Using the Policy Assurance Form and Audit Tool to manage and monitor the embedding of this policy putting action plans into place where required
- Ensuring that all transportation of records are properly supervised and deemed safe.

4.7 All Staff

All staff working must comply with this policy and are responsible for any records, which they create or use. This includes staff on temporary or honorary contracts, agency staff and students. All staff must annually complete those modules that are mandatory on the NHS Digital Information Governance Training Tool (IGTT).

5. IMPLEMENTATION AND STANDARDS

5.1 The CCG will establish and maintain mechanisms through which departments and other units can register the records they are maintaining. This will be achieved via the annual corporate records audit. The inventory of record collections will facilitate:

- the classification of records into series;
- the recording of the responsibility of individuals creating records; and
- the monitoring of standards across all record keeping systems.

5.2 All CCG's records will be managed in accordance with this policy from its creation/receipt through the period of its 'active' use, then into a period of 'inactive' retention and finally either confidential disposal or archival preservation.

5.3 All staff must ensure that their record keeping systems comply with the minimum standards set out in the following Appendices:

- Appendix 1 Record Creation, Tracking and Retrieval
- Appendix 2 Appraisal & Audit
- Appendix 3 Record Retention, Archiving and Disposal

5.4 The SMST will review the minimum standards on an on-going basis.

6. TRAINING

All managers are responsible for arranging training relevant to staff in records management and keeping and case note handling in accordance with their personal development plans following reviews. Caldicott, Confidentiality, and Security Training is also available for all staff via Electronic Staff Record programme (ESR).

7. SAFE GUARDING AND CONFIDENTIALITY

All staff is obligated to safeguard the confidentiality and security of information relating to patients and other staff.

A breach of confidentiality may be regarded as serious misconduct, which could lead to disciplinary action. If the disclosure of personal information or use of personal information did not meet the requirements of the Data Protection Act 2018 then the CCG and/or employee may be prosecuted as a consequence.

8. MONITORING

The CCG expects all staff to ensure that their record keeping systems comply with the minimum standards set out in the following Appendices:

- Appendix 1 Record Creation, Tracking and Retrieval
- Appendix 2 Appraisal & Audit
- Appendix 3 Record Retention, Archiving and Disposal

An annual corporate records audit will be carried out in accordance with the NHS Digital Data Security & Protection Toolkit to provide information on what information is being held, what is required to be retained and/or archived and what can be destroyed.

9. REFERENCES

The Data Protection Act 2018
http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Access to Health Records Act 1990
http://www.legislation.gov.uk/ukpga/1990/23/introduction

Freedom of Information Act 2000
http://www.legislation.gov.uk/ukpga/2000/36/introduction

Department of Health NHS Records Management Code of Practice 2016 (RMCOP 2016)
https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

Appendix 1 – Records Creation, Tracking & Retrieval

Overview

This Appendix covers the active stages of a records life cycle and provides a basic overview of the standards expected in relation to record keeping and maintenance.

The following standards must be adhered to at all times:

Standards in Records Keeping & Record Maintenance

- **Creation of a Record**
  A record must be kept of all activities carried out and decisions made on behalf of the CCG. Records may serve many purposes; the most important is to have an up-to date record of events and evaluations.

  The ownership (author), version number, and filename should be clearly stated in all documents; preferably in the footer of each page.

- **Date**
  All entries should be dated.

- **Creator of the Record**
  The creator of the record should be clearly identified. Where a signature is required this should be recognisable and the name and designation of the person printed beneath the signature.

- **Abbreviations**
  Abbreviations should be avoided wherever possible. Where used, the full meaning of an abbreviation should be cited the first time it is used.

- **Alterations**
  Do not try to hide errors. Paper records should have errors scored out with a single line and be initialled, dated and timed.

- **Additions**
  If an addition needs to be made to a record it should be prefaced with a comment indicating that this is an additional or late entry and be separately dated and signed. Never try to insert notes, especially after notification of a complaint or claim. Never try to disguise additions to a record. Any amendments made must be recorded in such a way that they may be independently auditable in case of future investigation or review for example, dated, timed and signed.

- **Version Control (see Policy Development Policy)**
  When considering the implications of an historic record it is important that the circumstances surrounding the creation of the record can be understood. For example, when investigating an incident it may be necessary to know which version of a particular policy or procedure was in force at the time of the incident. The version control scheme in the Policy Development Policy should be adopted for documents that are likely to have a number of iterations.

.

  Previous versions of the document must be retained in line with the retention schedule set out within Appendix 3 and made available at all times.

- **Naming of a File**

  The file name should be clear on what information it contains and include a date and version number. Maximum characters for a file name should be 25.

  E.g. topicsubject_v9_01_010112 (Spaces also count as a character) so “topic subject v9 01 010112” is also 25 characters.

  Files or documents should not be saved more than 4 levels down within a directory tree. E.g. S:\department_name\our_files\special_files\Letters In this example the “Letters” directory would be the4th level down within the department directory.

  Your saved file would look like this;
  S:\department_name\our_files\special_files\Letters\topicsubject_v9_01_010112

- **Personal Comments**

  Records should contain factual information or professional opinions. Only include commentary that is relevant and appropriate to the record. Records are not the place to note offensive observations about a person’s character, appearance or habits. Under the Data Protection Act 2018/GDPR, members of the public are allowed to have access and view the content of their records under the Subject Access Request Procedures. Avoid recording offensive, personal, or humorous comments about an individual.

- **Dictated Notes**

  Typed notes must be checked and signed by the professional who dictates them. Responsibility for the accuracy of the record lies with the person who created the record not the typist.

- **Completeness**

  A record needs to be fit for purpose. It should therefore contain information which is adequate, relevant and not excessive for its purpose. Standard request forms, for example, order forms should be completed fully. Insufficient information may lead to serious incidents.

- **Clarity and Legibility**

  Records need to be clear and legible. A hand written record should be written in permanent black ink wherever possible. This will give the records greater clarity and legibility when photocopied. If it is not possible for a person to write legibly the record should be typed. Thermal faxes may fade and should not be included as part of a permanent record. The information should either be transcribed into the record, the original requested or an indelible photocopy made of the fax.

- **Policies**

  All policies must comply with the requirements set out in the “Policy Development Policy”

- **Filing**

  Wherever possible records should be held in a departmentalised central filing system, in electronic form on a central server (s: Drive) to minimise duplication and reduce the costs of storage. Paper records should be held centrally within a Department. Each area

where records are stored should have a clear local record keeping policy and procedure containing:

1. Technical and descriptive documentation to enable the efficient use and support of the system. Including information to provide an administrative context for the record(s);

2. The rules used for referencing, titling, indexing and, where appropriate, the protective marking of records

3. The procedure for tracking records.

All files should be stored in the appropriate filing system when not in use. Filing of documentation is the responsibility of the individual who last made an entry in the record.

- **Indexing**

  The record holder should document a complete list of the files that are held. Such lists should be reviewed on a regular basis for accuracy and completeness.

- **Multiple Documents**

  Multiple documents that constitute a record should be filed together. Paper documents should be securely attached to each other. Where a record constitutes electronic and paper documents it should be kept as a complete document wherever possible. Where this is not possible this should be cross referenced.

- **Email**

  Email is a communication method not a record management system. Where the content of email or attachments forms part of a record it is the responsibility of the user to ensure it is added to, and becomes part of, that record whether held in hard copy or electronic format.

- **Original and Duplicates (Copies)**

  Maintaining multiple duplicate copies of the same document is discouraged. Access controls should be applied to centrally held records to ensure that the integrity of master records is maintained at all times. Copies may be held in circumstances where the original is forwarded outside of the organisation. Anyone having to create a copy of a record must immediately mark the record as a copy to avoid confusion with the original Master copy. Copy records should only be retained for the period of their immediate use after which time they should be destroyed.

- **Tracking a Record**

  Records must be traceable at all times and a system to trace records maintained in each department.

- **Transferring Records**

  The permanent transfer of original records out of a filing system is to be discouraged. Where there is a need to transfer original records out of a filing system (e.g. personnel records), a clear audit trail must exist showing: the date of transfer, reason for transfer, where the record has been transferred to and who actioned/authorised the transfer. Staff who transfer records are responsible for ensuring that appropriate safeguards are in place to ensure safe and secure delivery.

- **Storage and Security**

  All staffs are responsible for the safe custody of records in their use. Personally identifiable information must be handled in accordance with the Data Protection Act 2018. It is important that all staff are aware of their responsibilities in respect to information security and confidentiality. Under no circumstances should personally identifiable information be left unattended and/or visible to those who should not view it, for example, on a computer screen when you are not at your desk, on top of a desk in-tray, in the boot of your car or on a car seat visible to the public. Records should be stored securely in either a locked cabinet or within a secure environment on a computerised system. Where rooms containing notes are unattended, they must be locked.

- **Missing Records**

  If a record cannot be found your line manager must be advised immediately. When all efforts to find the record have been exhausted, an incident form should be completed in accordance with the CCGs' incident reporting procedure.

- **Archiving**

  Records should be archived in line with DH guidance for records retention. The SMST will, with the assistance of the relevant Directorates, assess the financial impact, particular in relation to storage, archiving, training.

Appendix 2: Appraisal & Audit

Overview

This Appendix provides information on how the CCG will ensure that the record systems in use will be monitored, to ensure that they meet minimum requirements. The following minimum standards are to be adhered at all times.

Standards in Appraisal & Audit of Records

- **Appraisal and Audit Process**

  All managers are responsible for regular, localised monitoring of the quality of documentation and adherence to this policy. In particular, managers and senior clerical staff should periodically undertake quality control checks to ensure that the standards, as detailed in this policy, are maintained.

  A corporate records audit of at least 4 areas/departments will be carried out annually.

  Each Directorate/service area should:

  - Identify all records in their work area been recorded;
  - Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures. Serious breaches of the policy should be brought to the immediate attention of the IG Lead;
  - Share the results of the audit within your Directorate;
  - Follow up all areas of concern arising out of the audit to ensure that remedial action has been taken;
  - The IG Lead will report findings of the corporate records audit the SMST.
  - Feed examples of good practice back to the IG Lead for reporting to SMST
  - Set and maintain standards by implementing new procedures including obtaining feedback where the procedures do not match the desired levels of performance.

Appendix 3: Record Retention, Archiving and Disposal

Overview

This Appendix sets out the minimum periods for which the various records created by the CCG or its predecessor bodies should be retained, either due to their on-going administrative value or as a result of statutory requirement. It also provides guidance on dealing with records that have on-going research or historical value and should be selected for permanent preservation as archives and transferred to a Place of Deposit approved by The National Archives.

The Appendix provides information and advice about all records commonly found within NHS Organisations. The retention schedules apply to all the records concerned, irrespective of the format (e.g. paper, databases, e-mails, photographs, CD-ROMs) in which they are created or held.

Interpretation of the Schedules

- **Type of record:**

  An alphabetical list of records created as part of a particular function. The business and corporate records schedule has grouped together records of major functions commonly found in the NHS.

- **Minimum & Maximum retention period:**

  Records are required to be kept for a certain period either because of statutory requirement or because they may be needed for administrative purposes during this time.

  Service Managers may decide that they need to keep records longer than the recommended minimum period. In making this determination consideration must be given to Article 5 (1) (e) of the General Data Protection Regulation (GDPR), that is, that personal data should not be retained longer than is necessary. Minimum retention periods should be calculated from the beginning of the year after the last date on the record. For example, a file in which the first entry is in February 2001 and the last in September 2004, and for which the retention period is seven years, should be kept in its entirety at least until the beginning of 2012. In any event, public records should not ordinarily be kept for longer than 30 years from their creation (calculated from the last date on the file, as described in 'Retention Periods' below) without being transferred to a Place of Deposit.

  Owners of records wanting to retain their records for more than the minimum retention schedule (other than for statutory or active administrative purposes, for example, for research purposes) must contact the IG Lead who will seek advice from the National Archives, other approved local Place of Deposit or other professional body.

- **Derivation**

  Notes the details of legislation, and any other references of relevance, to the recommended minimum retention period.

- **Final action**

  At the end of the relevant minimum retention period, records should be reviewed by the Service Manager who will need to decide if the record should be kept for longer than the minimum retention period. Where the Service Manager considers it appropriate to retain

records beyond the minimum retention period they must make arrangements for the storage of the records in line with the guidance in Appendix 1 - Record Creation, Tracking & Retrieval. It is the responsibility of the individual to ensure the safe and secure destruction of all confidential records. If in doubt they should contact the IG Lead for advice. A record of all documents sent for destruction must be maintained. Service Managers should ensure that arrangements are in place for the destruction of records including confidential waste in line with DH guidance.

- **Corporate (Non-Clinical) Records Retention Schedule**

  This retention schedule details a Minimum Retention Period for each type of non-clinical record. The following types of record are covered by this retention schedule (regardless of the media on which they are held, including paper, electronic, images and sound):

    - Non-Clinical records (including personnel, estates, financial and accounting records, and notes associated with complaint handling or continuing care referrals)
    - Photographs, slides and other images (non-clinical)
    - Microform (i.e. microfiche/microfilm)
    - Audio and video tapes, cassettes, CD-ROMs, etc.
    - E-mails
    - Computerised records
    - Scanned documents

- **Searching for records**

  When requests for information/copy records are received it is imperative that all archived records – both electronic and paper are searched to ensure that an accurate response can be provided.

Appendix 4 Equality Impact Assessment Tool for Policies (Equality Analysis)
To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

		Yes/ No	Comments
1	**Does the policy/guidance disadvantage one group or more than another on the basis of:**		
	• Race (including colour, culture, ethnicity, nationality or national origin and the travelling community)	N	
	• Religion or Belief	N	
	• Sex (e.g. male or female)	N	
	• Marriage or Civil Partnership	N	
	• Sexual Orientation (Lesbian, Gay, Bisexual, Heterosexual)	N	
	• Gender reassignment (e.g. someone who 'is proposing to undergo, is undergoing or has undergone a process (or part of a process) for the purpose of reassigning the person's sex by changing physiological or other attributes of sex.')	N	
	• Disability (e.g. learning disabilities, physical disability, sensory impairment, mental health problems etc.)	N	
	• Pregnancy and Maternity	N	
	• Age (children, young adolescent, older people etc.)	N	
2	**Is the policy/guidance/strategy more favourably towards one group on the basis of:**		
	• Race	N	
	• Religion or Belief	N	
	• Sex	N	
	• Marriage or Civil Partnership	N	
	• Sexual Orientation	N	
	• Gender reassignment	N	

	• Disability (e.g. learning disabilities, physical disability, sensory impairment, mental health problems etc.)	N	
	• Pregnancy and Maternity	N	
	• Age (e.g. children, young adolescent, older people etc.)	N	
3	**If you have identified potential discrimination in the policy/guidance are there any valid, legal and/or justifiable exceptions? Please list any exceptions.**	N/A	
4	**Is the policy/guidance likely to have a negative/adverse impact on any of the above group(s)?**	N/A	
5	**If so, how would you address the impact? Please explain.**	N/A	
6	**What are the associated objectives to the policy/guidance?**		See section 2 of policy

If you have identified a potential discriminatory impact in this document, please refer to the author(s) of the policy/guidance, together with any suggestions required to address the impact.