

Records Management Policy

ICB document reference:	ICB IG 006
Name of originator/author:	NHS AGEM CSU
Date of approval:	March 2024
Name of responsible Committee:	Executive Committee/Audit & Risk Committee
Responsible Director/ICB Officer:	Julie Ellis-Fenwick, Head of Corporate Governance
Category:	Information Governance
EIA undertaken:	
Date issued:	March 2024
Review date:	March 2027
Target audience:	All staff
Distributed via:	Email, Website, Intranet and Board Portal

Document Control Sheet

Document Title	Records Management Policy
Version	0.5
Status	Draft
Authors	NHS AGEM CSU
Date	07/02/2024

Document history			
Version	Date	Author	Comments
0.1	11/01/20	NHS AGEM CSU/Optum Health Systems Support: IG Teams	Updated document based on predecessor Lincolnshire ICB documentation & taking account of the Data Protection Act 2018 and GDPR
0.2	04/03/21	NHS AGEM CSU	Minor amendments to complete the draft version
0.3	14/10/2021	NHS AGEM CSU	No changes, still current.
0.4	27/06/2022	NHS AGEM CSU	Policy review and rebrand for the transition of the ICB to an ICB. Updated linked guidance.
0.5	07/02/2024	NHS AGEM CSU	Minor wording changes, updates to reflect modern working.

CONTENTS

Section		Page
1	Scope and Purpose	4
2	Accountability and Responsibilities	4
3	The Six Phases of the Information Lifecycle	5
4	Equality and Diversity	8
5	Due Regard	8
6	Policy Review and Monitoring	8
7	References	8
8	Extract from Records Management Code of Practice Retention Schedules (Health and Social Care 2016)	9

1 Scope and Purpose

- 1.1 This policy applies to NHS Lincolnshire Integrated Care Board (ICB)
- 1.2 This document covers all information types; clinical, non-clinical, person identifiable or confidential and corporate information irrespective of the media on which they are held.
- 1.3 This policy applies to all employees (permanent, seconded, contractors, management and clinical trainees, apprentices, temporary staff, and volunteers) of the ICB. Third parties with whom the ICB may agree information sharing protocols will be governed by the associated information sharing agreements and will be made aware of this policy.
- 1.4 The Policy has been updated to reflect the Data Protection Act 2018 that incorporates the General Data Protection Regulation (GDPR) into UK law.
- 2.1 This policy supports ensuring that the organisation's information is safely managed through every phase of its lifecycle.
- 2.2 It is supported by separate information governance policies, available on the ICB internet that can be used by staff to ensure that this is effectively implemented in practice.
- 2.3 The records management policy principles apply to any information that may be held whether on paper or any other format e.g. electronic, audio, video etc.
- 2.4 The objective of this policy is to provide an explanation of the phases of records lifecycle to help ensure that the ICB can meet legal and regulatory requirements.

2 Accountability and Responsibilities

- 2.1 It is the responsibility of all ICB employees to adhere to the requirements of this document when handling all types of ICB information.
- 2.2 Training is provided as part of the staff induction process.
- 2.3 Adherence to this policy forms part of the employee's employment contract.
- 2.4 Records created by the ICB are public records and are therefore subject to both legal and professional obligations e.g. Public Records Act, Freedom of Information Act, Data Protection Act.

2.5 The ICB's Corporate Board Secretary leads on Records Management on behalf of the Director of Finance and Contracting in their role as the organisational Senior Information Risk Owner.

3 The Six Phases of a record lifecycle

The Information Lifecycle covers 6 different phases:

- Creation
- Naming
- Filing Structure
- Filing/organisation
- Tracking and tracing
- Retention/disposal

3.1 Creation

- Record creation is one of the most important processes in records management and all staff within the organisation should aim to create good records that can be used in an effective manner
- It is important that records are kept in context and the best way to achieve this is to 'file' or 'classify' them. Records cannot be tracked or used efficiently if they are not classified or have been classified inappropriately
- Records captured or filed in a corporate filing system must be regarded as authentic or reliable
- A common format for the creation of records will ensure that those responsible for record retrieval are able to locate records more easily
- When staff create corporate records, a common format should always be used that as a minimum includes:
 - The difference between a document and a record
 - The referencing to be applied to any new records
 - The version control standards to be followed
 - The agreed naming conventions in use within the ICB
 - Where an original record should be filed
 - To ensure quality and continuity of operational services, all records should be kept accurate and up to date. All ICB staff who are responsible for recording information in both paper and electronic format must ensure they fully understand their responsibilities as set out in this policy and remember that records may be used in a court of law.

3.2 Naming

All staff must ensure that naming conventions:

- Give a unique name to each record
- Give a meaningful name which closely reflects the records content
- Locate the most specific information at the beginning of the name and the most general at the end
- Provide a similarly structured and worded name to all records which are linked e.g. an earlier and a later version

3.3 Filing Structure

- A clear and logical filing structure that aids the retrieval of records must be used
- The filing structure for electronic records must ensure consistency
- Filing of primary corporate records to local drives on PC's is not permitted, these records must be filed on the network within a shared folder that has appropriate access controls
- Final versions of appropriate documents will be circulated or placed onto the local Intranet **or** Internet to ensure that all staff can have access to the approved versions of policies and procedures
- Documents must be given a review date when appropriate. The relevant responsible person or committee for any updates and reviews must also be identified.

3.4 Filing, Storage and Organisation

- A referencing system that meets the needs of the ICB must be used
- Several types of systems may be used e.g. alphanumeric, alphabetical, numeric, keyword etc.
- In some circumstances it may be more feasible to give a unique reference to the file or folder in which the record is kept and identify the record by reference to date and format
- Under no circumstances should personal confidential information be left unattended e.g. on a desk or on a computer screen or in the car. Where rooms containing records are stored, they must be kept locked

3.5 Tracking and Tracing

- The movement of records is the point at which information is at the greatest risk of being lost or inappropriately accessed
- In this circumstance, staff may have a requirement to hold personal confidential information outside of NHS systems or premises. This should only be done if the service has been given Caldicott Guardian or delegated authority approval for this and there is no alternative way of working. This should be discussed with the responsible line manager.

- The Department of Health has mandated that there should be no transfers of unencrypted personal confidential data held in electronic format across the NHS. This is the default position to ensure that patient and staff personal data are protected. Any data stored on a PC or other removable device in a non-secure area or on a portable device such as a laptop or mobile phone must be encrypted to the recommended NHS standard
- Tracking and tracing procedures that are implemented must enable the movement and location of records to be controlled. This provides an auditable trail of record transactions.
- Tracking mechanisms to be used include:
 - The item reference number of identifiers
 - A description of the item e.g. title
 - The person, position or operational area/team who may have possession of the item
 - The date and time of movement that took place
 - Regular records audits must take place.

3.6 Retention/Disposal

- Records must be secure from unauthorised or inadvertent alteration or erasure. Access and disclosure must be properly controlled, and audit trails must track all use and changes. Records must be held in a robust format, which remains readable for as long as records are required.
- The ICB has adopted the retention/disposal procedure and the retention schedules detailed within the Records Management Code of Practice for Health and Social Care 2021; Appendix 3 of the Code contains the detailed retention schedules – both documents are available here: -

[Records Management Code of Practice - NHS Transformation Directorate \(nhsx.nhs.uk\)](https://nhs.uk/records-management-code-of-practice)

- Records selected for archival preservation that are no longer in use by the ICB are to be transferred as soon as possible to an archival institution or an agreed place of deposit
- Non-active records should be transferred no later than 30 years from creation of the record as required by the Public Records Act 1958
- A record of the destruction of records, showing their reference, description and date of destruction will be maintained and preserved so that the ICB can accurately identify which records have been destroyed and are no longer available
- Disposal schedules will constitute the basis of such a record

4 Equality and Diversity

- 4.1 The ICB aims to design and implement policy documents that meet the diverse needs of the services, population, and workforce, ensuring that none are placed at a disadvantage over others. It considers current UK legislative requirements, including the Equality Act 2010 and the Human Rights Act 1998, and promotes equal opportunities for all.
- 4.2 This document has been designed to ensure that no-one receives less favourable treatment due to their personal circumstances, i.e. the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity. Appropriate consideration has also been given to gender identity, socio-economic status, immigration status and the principles of the Human Rights Act.
- 4.3 In carrying out its functions, the ICB must have due regard to the Public Sector Equality Duty (PSED). This applies to all the activities for which the organisation is responsible, including policy development, review, and implementation.

5 Due Regard

- 5.1 This policy has been reviewed in relation to having due regard to the Public Sector Equality Duty (PSED) of the Equality Act 2010 to eliminate discrimination, harassment, victimisation; to advance equality of opportunity; and foster good relations.

6 Review and Monitoring

- 6.1 All managers are responsible for regular monitoring of the quality of records and documentation and managers must periodically undertake quality control checks to ensure that the standards as detailed in this policy are maintained.
- 6.2 This policy will be reviewed every three years unless new legislation, codes of practice or national standards are introduced.

7 References

- Data Protection Act 2018 and Freedom of Information Act available from [Legislation.gov.uk](https://legislation.gov.uk)
- Records Management Code of Practice for Health and Social Care available from <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016>

8 Extract from Records Management Code of Practice Retention Schedules (Health and Social Care 2021)

Broad descriptor	Record Type	Retention Start	Minimum Retention period	Action at end of retention period	Notes
Corporate Governance	Board Meetings	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Corporate Governance	Board Meetings (Closed Boards)	Creation	May retain for 20 years	Transfer to a Place of Deposit	Although they may contain confidential or sensitive material, they are still a public record and must be transferred at 20 years with any FOI exemptions noted or duty of confidence indicated.
Corporate Governance	Chief Executive records	Creation	May retain for 20 years	Transfer to a Place of Deposit	This may include emails and correspondence where they are not already included in the board papers and they are considered to be of archival interest.

Corporate Governance	Committees Listed in the Scheme of Delegation or that report into the Board and major projects	Creation	Before 20 years but as soon as practically possible	Transfer to a Place of Deposit	
Corporate Governance	Committees/ Groups / Sub-committees not listed in the scheme of delegation	Creation	6 Years	Review and if no longer needed destroy	Includes minor meetings/projects and departmental business meetings
Corporate Governance	Destruction Certificates or Electronic Metadata destruction stub or record of information held on destroyed	Destruction of record or information	20 Years	Consider Transfer to a Place of Deposit and if no longer needed to destroy	The Public Records Act 1958 limits the holding of records to 20 years unless there is an instrument issued by the Minister with responsibility for administering the Public Records Act 1958. If records are not excluded by such an instrument, they must either be transferred to a place of deposit as a public record or destroyed 20

	physical media				years after the record has been closed.
Corporate Governance	Incidents (serious)	Date of Incident	20 Years	Review and consider transfer to a Place of Deposit	
Corporate Governance	Incidents (not serious)	Date of Incident	10 Years	Review and if no longer needed destroy	
Corporate Governance	Non-Clinical Quality Assurance Records	End of year to which the assurance relates	12 years	Review and if no longer needed destroy	
Corporate Governance	Patient Advice and Liaison Service (PALS) records	Close of financial year	10 years	Review and if no longer needed destroy	

Corporate Governance	Policies, strategies, and operating procedures including business plans	Creation	Life of organisation plus 6 years	Review and consider transfer to a Place of Deposit	
Communications	Intranet site	Creation	6 years	Review and consider transfer to a Place of Deposit	
Communications	Patient information leaflets	End of use	6 years	Review and consider transfer to a Place of Deposit	
Communications	Press releases and important internal communications	Release Date	6 years	Review and consider transfer to a Place of Deposit	Press releases may form a significant part of the public record of an organisation which may need to be retained
Communications	Public consultations	End of consultation	5 years	Review and consider transfer to a Place of Deposit	

Communications	Website	Creation	6 years	Review and consider transfer to a Place of Deposit	
Staff Records & Occupational Health	Duty Roster	Close of financial year	6 years	Review and if no longer needed destroy	
Staff Records & Occupational Health	Exposure Monitoring information	Monitoring ceases	40 years/5 years from the date of the last entry made in it	Review and if no longer needed destroy	A) Where the record is representative of the personal exposures of identifiable employees, for at least 40 years or B) In any other case, for at least 5 years.
Staff Records & Occupational Health	Occupational Health Reports	Staff member leaves	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner	Review and if no longer needed destroy	
Staff Records & Occupational Health	Occupational Health Report of Staff member	Staff member leaves	Keep until 75th birthday	Review and if no longer needed destroy	

	under health surveillance				
Staff Records & Occupational Health	Occupational Health Report of Staff member under health surveillance where they have been subject to radiation doses	Staff member leaves	50 years from the date of the last entry or until 75th birthday, whichever is longer	Review and if no longer needed destroy	
Staff Records & Occupational Health	Staff Record	Staff member leaves	Keep until 75th birthday (see Notes)	Create Staff Record Summary then review or destroy the main file.	This includes (but is not limited to) evidence of right to work, security checks and recruitment documentation for the successful candidate including job adverts and application forms. May be destroyed 6 years after the staff member leaves or the 75 th birthday, whichever is sooner, if a summary has been made.

Staff Records & Occupational Health	Staff Record Summary	6 years after the staff member leaves	75th Birthday	Place of Deposit should be offered for continued retention or Destroy	Please see page 36 for an example of a Staff Record Summary used by an organisation.
Staff Records & Occupational Health	Timesheets (original record)	Creation	2 years	Review and if no longer needed destroy	
Staff Records & Occupational Health	Staff Training records	Creation	See Notes	Review and consider transfer to a Place of Deposit	Records of significant training must be kept until 75th birthday or 6 years after the staff member leaves. It can be difficult to categorise staff training records as significant as this can depend upon the staff member's role. The IGA recommends: 1 Clinical training records - to be retained until 75 th birthday or six years after the staff member leaves, whichever is the longer2 Statutory and mandatory training records - to be kept for ten years after training completed3Other training records - keep for six years after training completed.

Procurement	Contracts sealed or unsealed	End of contract	6 years	Review and if no longer needed destroy	
Procurement	Contracts - financial approval files	End of contract	15 years	Review and if no longer needed destroy	
Procurement	Contracts - financial approved suppliers' documentation	When supplier finishes work	11 years	Review and if no longer needed destroy	
Procurement	Tenders (successful)	End of contract	6 years	Review and if no longer needed destroy	
Procurement	Tenders (unsuccessful)	Award of tender	6 years	Review and if no longer needed destroy	
Estates	Building plans and records of major building work	Completion of work	Lifetime of the building or disposal of asset plus six years	Review and consider transfer to a Place of Deposit	Building plans and records of works are potentially of historical interest and where possible be kept and transferred to a place of deposit

Finance	Accounts	Close of financial year	3 years	Review and if no longer needed destroy	Includes all associated documentation and records for the purpose of audit as agreed by auditors
Finance	Benefactions	End of financial year	8 years	Review and consider transfer to Place of Deposit	These may already be in the financial accounts and may be captured in other records/reports or committee papers. Where benefactions endowment trust fund/legacies - permanent retention.
Finance	Debtor records cleared	Close of financial year	2 years	Review and if no longer needed destroy	
Finance	Debtor records not cleared	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Donations	Close of financial year	6 years	Review and if no longer needed destroy	
Finance	Expenses	Close of financial year	6 years	Review and if no longer needed destroy	

Finance	Final annual accounts report	Creation	Before 20 years	Transfer to place of deposit if not transferred with the board papers	Should be transferred to a place of deposit as soon as practically possible
Finance	Financial records of transactions	End of financial year	6 Years	Review and if no longer needed destroy	
Finance	Petty cash	End of financial year	2 Years	Review and if no longer needed destroy	
Finance	Private Finance initiative (PFI) files	End of PFI	Lifetime of PFI	Review and consider transfer to Place of Deposit	
Finance	Salaries paid to staff	Close of financial year	10 Years	Review and if no longer needed destroy	
Finance	Superannuation records	Close of financial year	10 Years	Review and if no longer needed destroy	

Legal, Complaints & information Rights	Complaints case file	Closure of incident (see Notes)	10 years	Review and if no longer needed destroy	http://www.nationalarchives.gov.uk/documents/information-management/sched_complaints.pdf The incident is not closed until all subsequent processes have ceased including litigation. The file must not be kept on the patient file. A separate file must always be maintained.
Legal, Complaints & information Rights	Fraud case files	Case closure	6 years	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Freedom of Information (FOI) requests and responses and any associated correspondence	Closure of FOI request	3 years	Review and if no longer needed destroy	Where redactions have been made it is important to keep a copy of the redacted disclosed documents or if not practical to keep a summary of the redactions.

Legal, Complaints & information Rights	FOI requests where there has been a subsequent appeal	Closure of appeal	6 years	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Industrial relations including tribunal case records	Close of financial year	10 Years	Review and consider transfer to a Place of Deposit	Some organisations may record these as part of the staff record but, in most cases, they will form a distinct separate record either held by the staff member/manager or by the payroll team for processing.
Legal, Complaints & information Rights	Litigation records	Closure of case	10 years	Review and consider transfer to a Place of Deposit	
Legal, Complaints & information Rights	Patents / trademarks / copyright / intellectual property-	End of lifetime of patent or termination of licence/action	Lifetime of patent or 6 years from end of licence /action	Review and consider transfer to Place of Deposit	
Legal, Complaints & information Rights	Software licences	End of lifetime of software	Lifetime of software	Review and if no longer needed destroy	

Legal, Complaints & information Rights	Subject Access Requests (SAR) and disclosure correspondence	Closure of SAR	3 Years	Review and if no longer needed destroy	
Legal, Complaints & information Rights	Subject access requests where there has been a subsequent appeal	Closure of appeal	6 Years	Review and if no longer needed destroy	