Bedfordshire, Luton and Milton Keynes Integrated Care Board

Records Management & Information Lifecycle Policy

Document Status:

This is a controlled document. Any printed or downloaded copies are not controlled. The version of this document published on the Bedfordshire, Luton & Milton Keynes Integrated Care Board website is the controlled copy
www.befordshirelutonandmiltonkeynes.icb.nhs.uk

Sustainable Development - Environmental

Do you really need to print this document?

Please consider the environment before you print this document and where possible copies should be printed double-sided. Please also consider setting the page range in the print properties, when relevant to do so, to avoid printing the document in its entirety.

Document Control	
Document Owner:	Senior Information Risk Owner
Document Author(s):	Information Governance Team
Directorate:	Medical Directorate
Approved By:	Operational Group
Date of Approval:	25-03-2024
Date of Next Review:	25-03-2026
Effective Date:	25-03-2024

Version Control			
Version	**Date**	**Reviewer(s)**	**Revision Description**
v1.0	01-07-2022	IG Team	Reviewed – Renamed Head of Information Governance to Head of Safe Practice. Slight text changes with records section to include messages.
V2.0	25-03-2024		

Implementation Plan

Development and Consultation:	The following individuals were consulted and involved in the development of this document: ▪ Information Governance Team ▪ Information Governance Group
Dissemination:	Staff can access this document via the website and will be notified of new / revised versions via the staff briefing. This document will be included in the organisation's Publication Scheme in compliance with the Freedom of Information Act 2000.
Training:	All new staff are required to attend a compulsory Induction Programme which incorporates Information Governance. In addition to this, all staff are required to annually complete and pass the NHS Digital's Data Security Awareness Level 1 module on the Electronic Staff Record (ESR) e-Learning portal. A Training Needs Analysis (TNA) has been developed for staff in key Information Governance roles, as required by the Data Security and Protection Toolkit.
Monitoring:	An assessment of compliance with assertions which make up the Data Security and Protection Toolkit, will be undertaken each year and audited by internal auditors. In addition the ICBs Information Governance Team will undertake additional monitoring of compliance with this policy as a response to identification of any gaps or as a result of risks identified by incidents, external reviews or other sources of information and advice.
Review:	The Document Owner will ensure this document is reviewed in accordance with the review date on page 2. This policy will be reviewed by its review date or sooner in response to any organisational, regulatory or legislative changes.
Equality, Diversity and Privacy:	Appendix 1 - Equality Impact Assessment Appendix 2 - Data Protection Impact Assessment
Associated Documents:	The following documents must be read in conjunction with this document: o Information Governance Policy, Framework & Strategy o Data Protection Policy o Information Sharing Policy o Subject Access & Access to Health Records Policy o Social Media Policy

	○ Integrated Risk Management Policy ○ Offsite Storage Procedures ○ Controlled Environment for Finance Procedures ○ Information & Cyber Security Incident Procedure ○ Working From Home Guidance ○ Staff IG Handbook
References:	The following articles were accessed and used to inform the development of this document. Records Management Code of Practice for Health & Social Care 2021 which has been produced and published by NHSX. https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

Table of Contents

1.0 Introduction 6
2.0 Scope 7
3.0 Definitions 7
4.0 Policy Statement 8
5.0 Roles and Responsibilities 9
6.0 Processes and Procedures 10
6.1 NHS Standards 10
6.2 Departmental Records Management Procedures 10
6.3 Filing Systems and Storage (Electronic and Paper Records) 11
6.4 Accessibility (Electronic and Paper Records) 11
6.5 Security & Access (Electronic and Paper Records) 12
6.6 Retention, Archive, Appraisal and Destruction (All record types) 12
6.7 Paper Archives and Offsite Storage 13
6.8 Emails 13
6.9 Incident Reporting 14
Appendix 1 - Equality Impact Assessment Initial Screening 15
Appendix 2 - Data Protection Impact Assessment Initial Screening 17

1.0 Introduction

1.1 NHS Bedfordshire, Luton and Milton Keynes Integrated Care Board (ICB) aims to ensure robust governance through its formal written procedural documents, such as this document, which communicate standard organisational ways of working. These documents help clarify operational requirements and consistency within day-to-day practice. They can improve the quality of work, increase the successful achievement of objectives and support patient safety, quality and experience. The ICB aims to ensure its procedural documents are user friendly, up-to-date and easily accessible.

1.2 The ICB must design and implement procedural documents that meet the diverse needs of our service and workforce, ensuring that none is placed at a disadvantage over others, in accordance with the Equality Act 2010. The Equality Impact Assessment initial screening, which was used to determine the potential impact this policy might have with respect to the individual protected characteristics is incorporated at Appendix 1.

1.3 A Data Protection Impact Assessment is a process which helps assess privacy risks to individuals in the collection, use and disclosure of personal information. The Data Protection Impact Assessment initial screening, which was used to determine the potential impact this policy might have with respect to an individual's privacy is incorporated at Appendix 2.

1.4 The ICB recognises the need to have robust records management procedures in place to ensure information is held securely, available at the point of need and managed in line with statutory obligations and NHS standards.

1.5 All NHS records are public records under the Public Records Act 1958. This provides statutory obligations upon the ICB to comply with the legal requirements in relation to the records it holds, including, UK General Data Protection Regulations (GDPR), Data Protection Act 2018, Access to Health Records Act 1990, The Freedom of Information Act 2000 and Environmental Information Regulations 2004

1.6 Records (information) held by the ICB are important assets as they are the memory of the organisation and must be efficiently managed and available to those with authorised access in order to:

- Support the ICB's administrative and managerial decision making.
- Meet legal requirements including requests from service users under access to records legislation.
- Assist in providing evidence for internal and external reviews and other audits.
- Support day-to-day business.
- Provide clinical and managerial effectiveness through multi-disciplinary working within the ICB and with partner agencies.

2.0 Scope

2.1 This policy applies to all ICB staff members, including Ordinary Members of the Board of the ICB, and Practice Representatives, involved in the ICB's policy-making processes, whether permanent, temporary or contracted-in under a contract for service (either as an individual or through a third-party supplier).

2.2 This policy MUST be applied to ALL records held by the ICB in any format (paper or electronic), including but not limited to:

- Administrative records e.g. estates, financial, contracts, complaints, policies, meeting papers, agendas
- Emails (depending on their content)
- All patient records
- Staff/employee records
- Computer databases
- Audio and video recordings
- Messages and documents shared via communication tools such as WhatsApp or MS teams
- Tapes, cassettes, floppy disks and CD ROMs

3.0 Definitions

3.1 This section provides staff members with an explanation of terms used within this policy.

3.2 **Appraisal** – The process of deciding what to do with records when their business use has ceased. There will be one of three outcomes from appraisal:

- Destroy / delete
- To keep for a longer period (possibly at the ICBs Offsite Storage facility)
- To transfer to a place of deposit appointed under the Public Records Act 1958.

3.3 **Archives** – Records that are appraised as having permanent value for evidence of on-going rights or obligation, for historical or statistical research or as part of the corporate memory of the organisation.

3.4 **Confidential information** – can be anything that relates to patients, staff or any other commercially sensitive information (such as contracts and tenders) held in any form (e.g., paper, electronic, audio or video) howsoever stored (such as patient records, paper diaries, computer or on mobile devices such as laptops, tablets, smartphones) or even passed by word of mouth. Corporate record – includes:

- Administrative records (including personnel, estates, financial and accounting, contract records, litigation and records associated with complaints handling)
- Registers and rotas
- Office/appointment diaries
- Photographs, slides, plans or other graphic work (not clinical in nature)

- Audio and video tapes
- Records in all electronic formats including emails

3.5 **Destruction** – The process of eliminating or deleting records beyond any possible reconstruction (BS ISO 15488-1:2001).

3.6 **Health record** – 'consists of information relating to the physical or mental health or condition of an individual and has been made by or on behalf of a health professional in connection with the care of that individual' (Data Protection Act 1998 s68(2).

3.7 A **Place of Deposit** is a record office which has been approved by the National Archives for the transfer of public records in accordance with the Public Records Act 1958. The National Archives is the UK Government's official archive. They work with Government and public sector bodies, helping them to manage and use information more effectively.

3.8 **Personal Data** is information which relates to a living individual who can be identified from those data and includes any expression of opinion about the individual. Typical examples could include:

- Person's name, address, full postcode, date of birth
- Email address and telephone numbers
- Pictures, photographs, videos, audio-tapes or other images of patients

3.9 **Public records** – Records of NHS organisations are public records in accordance with Schedule 1 of the Public Records Act 1958.

3.10 **Records** – 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business' (ISO 15489-1:2016).

3.11 **Records management** – field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records. Records management includes processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

4.0 Policy Statement

4.1 The ICB will conduct an annual assessment of its compliance against the assertions which make up the Data Security and Protection Toolkit and have the evidence provided for the assessment further assessed by its internal auditors.

4.2 The ICB will conduct periodic reviews to ensure the way it manages its records is in line with statutory obligations and NHS standards.

5.0 Roles and Responsibilities

5.1 The following have specific responsibilities in relation to this policy.

5.2 The ICB recognises it has responsibility for ensuring it meets its legal responsibilities and for the adoption of national guidance. There is therefore a clear chain of management accountability and responsibility for Records Management and Information Lifecycle.

5.3 **Senior Information Risk Owner (SIRO)** - The SIRO is concerned with identifying and managing the information risks to the organisation. This includes oversight of the organisation's Information Asset Registers with the support of the Head of Safe Practice and the ICBs designated Information Asset owners (IAOs) – see below.

5.4 **Caldicott Guardian (CG)** - The CG 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 information is shared in an appropriate and secure manner regardless of the format the information is in.

5.5 **Head of Safe Practice** - The Head of Safe Practice 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 which promote compliance with this policy.

5.6 **Information Asset Owner (IAO)** - An IAO 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 IG objective that all information assets of the organisation are recorded together with the business importance of those assets.

5.7 **Information Asset Administrator (IAA)** - An IAA provides support to their IAO to: ensure that policies and procedures are followed with requirements applied to their assets; recognise potential or actual security incidents in relation to the security of the asset and, ensure their information asset registers are maintained, accurate and up to date.

5.8 **Heads of Departments/Service** - The responsibility for departmental records management (including retention and disposal of records) is devolved to the Heads of Departments within the ICB. They have overall responsibility for the management of records generated by the activities of their department/service and for ensuring the records are managed as detailed in this policy.

5.8.1 It is important for all Heads of Departments/Services to work in collaboration with the relevant IAO and IAA for their department to ensure IARs are updated with changes to their information assets.

5.8.2 They are also responsible for ensuring that they and their staff are familiar with this policy and for ensuring that any breaches of the policy are reported, investigated, and acted upon.

5.9 **All Staff -** Under the Public Records Act 1958, all NHS employees are responsible for any records which they create or use in the course of their duties. Therefore, any records created by an employee of the NHS are public records and may be subject to both legal and professional obligations.

5.9.1 ICB staff must ensure that they keep appropriate records of their work and manage those records in keeping with this policy and their departments Records Management & Information Lifecycle Procedures.

5.9.2 ICB staff are also responsible for ensuring this policy is applied to their own personal drive on the ICBs Network. Particular attention should be given to the Accessibility and the Retention, Archive, Review and Destruction sections of this policy.

5.9.3 ICB staff must comply with the procedures detailed in this policy and supporting guidance to ensure that:

- Records are available when needed
- Records can be accessed
- Records can be interpreted
- Records can be trusted
- Records can be maintained through time
- Records are secure
- Records are retained and disposed of appropriately

6.0 Processes and Procedures

6.1 NHS Standards

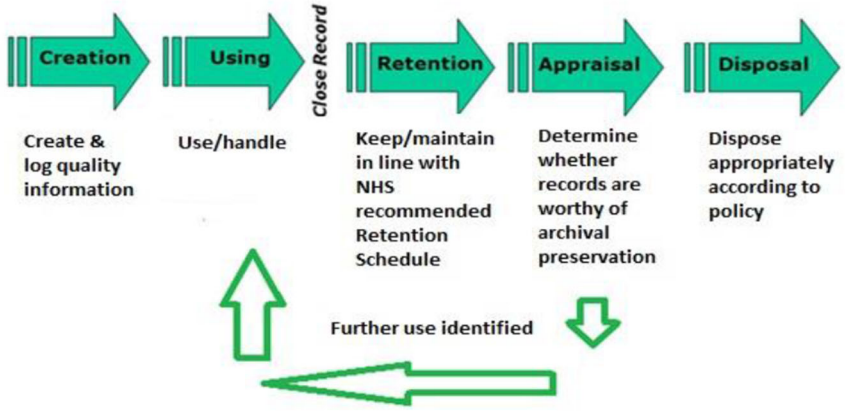
UK GDPR requires the ICB to ensure it stores, archives and destroys records, information and documents lawfully and appropriately. It does not define how this should be done. However, the Information Commissioners Office (ICO) expects all Health & Social Care organisations to comply with the Records Management Code of Practice for Health & Social Care 2021, which has been produced and published by NHS England (previously NHS X).

https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care

6.2 Departmental Records Management Procedures

Each department in the ICB is required to have defined Records Management Procedures in place. These should take into account the legislative and regulatory environment in which the department operates and the Information Lifecycle.

6.2.1 Information Lifecycle is a term that describes a controlled regime in which information is managed from the point it is created to the point it is either destroyed or permanently preserved as being of historical or research interest. This can be seen diagrammatically below:



6.3 Filing Systems and Storage (Electronic and Paper Records)

6.3.1 Paper filing systems should have simple, intuitive structures with each folder/file/record being given a unique identifier e.g., NHS Number (if for direct care) or staff number and where applicable dated by month or year.

6.3.2 Clearly defined structures for departmental shared folders on the ICBs Network are essential to enable staff to access files in a quick and effective manner. Defining an outline file structure with the involvement of the whole department/team will mean that staff will have a clearer understanding of where to store and retrieve documents from.

6.3.3 The saving of electronic records and storage of paper records should be performed in accordance with agreed departmental procedures.

6.3.4 Any location used to store paper records must comply with Health and Safety and fire regulations and be considered in accordance with any confidentiality and access issues e.g., an area/location with controlled and (where possible) auditable access.

6.4 Accessibility (Electronic and Paper Records)

6.4.1 The records and information held by the ICB are only useful if they can be accessed at the point at which they are required.

6.4.2 There should be fast and efficient access to records for authorised staff and access procedures should be effective in supporting request under the Freedom of Information Act 2000, the Environmental Information Regulations 2004 or an Access to Health Records or subject access request.

6.4.3 Records are not accessible when they are on a staff members own personal drive on the ICBs network. Any record or information that needs to be accessed by more than

one member of staff must be saved to the relevant departments share drive on the ICBs network.

6.4.4 Once a project or piece of work is completed, all associated documentation should be moved to the appropriate folder in the departments share drive on the ICBs Network. This will ensure all documentation is available when needed.

6.4.5 When considering sharing electronic and paper records, staff members should consider the requirements within the Information Sharing Policy before the sharing takes place.

6.5 Security & Access (Electronic and Paper Records)

6.5.1 All staff (as defined within the scope of this policy) have a duty for the maintenance and protection of records they use or create. Only authorised staff should have access to the ICB's records and the ICB's Head of Safe Practice should be contacted should access be required by any person outside of the organisation.

6.5.2 Records containing personal identifiable information (patient or staff records) must be treated as confidential with access given on a need-to-know basis only.

6.5.3 The movement and location of paper patient records should be controlled to ensure that its location is known at all times and can be retrieved as and when needed.

6.5.4 Records should only ever be taken off site (including home) with the approval of the line manager. Security of these records should be paramount, especially in the case of confidential records. Staff are responsible for the safe custody of records in their use both on and off ICB or client premises.

6.4.5 Confidential information should not be left unattended and visible to others. If the record is to be taken home, it must be stored securely and in the boot of the vehicle whilst in transit out of sight. DO NOT leave records in vehicles overnight.

6.6 Retention, Archive, Appraisal and Destruction (All record types)

6.6.1 Keeping unnecessary records uses up valuable space and can incur unnecessary costs. It can also cause problems when trying to retrieve important information e.g. to respond to a request under the Freedom of Information Act 2000, the Environmental Information Regulations 2004 or an Access to Health Records or Subject Access Request.

6.6.2 Some information/documents may have served their intended purpose but may need to be reviewed at a later date e.g. for an investigation or query, therefore it must be retained and archived securely until it reaches the relevant destruction period as detailed in the Retention Schedule (part of the Records Management Code of Practice

for Health & Social Care 2021 - Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk))

6.6.3 When a record is deemed to have no further value to the ICB, has reached its retention period and has no historical value or research interest which would require it to be sent to a 'Place of Deposit', it should be destroyed. However, it is important that staff follow their departmental procedures for destruction approval prior to deletion or destruction.

6.6.4 If records of historical value or research interest are identified (as defined in the Records Management Code of Practice for Health & Social Care 2021), the Head of Safe Practice MUST be informed immediately so assistance can be provided.

6.6.5 All paper information and records MUST be disposed of by placing them in the ICBs Shred Safe Bins.

6.6.6 Records that need to be preserved beyond their scheduled disposal date must be clearly marked on the relevant departments Information Asset Register by the IAO or IAA.

6.6.7 Emails and messages e.g. WhatsApp, MS teams, are subject to the same records management principles as the equivalent record in any other format.

6.7 Paper Archives and Offsite Storage

6.7.1 All departments are responsible for ensuring any paper documents they archive and store in ICB offices or send to the Offsite Storage facility are filed and catalogued correctly to enable them to retrieve items as and when required. Failure to do this may result in them not being able to retrieve what they need when they need it.

6.7.2 The ICBs has an Offsite Storage service provided by a third party. The ICBs IG Team has a process in place for the management of the service including retrieval of boxes and the sending of items for archive/safe storage.

6.7.3 An 'Archiving, Cataloguing and Offsite Storage Guidance for Staff' is available in the IG section on the Staff Intranet. In addition to the guidance, the IG Team will assist staff by providing advice and support when needed. This will help to ensure staff are confident with the task and to reduce the risk of information being misfiled and/or irretrievable.

6.8 Emails

6.8.1 All emails sent or received by anyone with a ICB email account are classed as ICB records. Once a project or piece of work is completed, all associated and relevant emails should be moved to the appropriate folder in the departments share drive on the ICBs Network. This will ensure all emails are available when needed.

The Email system should not be used for long term storage.

6.8.2 To manage email messages appropriately, staff need to identify email messages that are records of their business activities and decision making. It is important that email messages and their attachments which are considered as 'records' are moved from individual mailboxes and managed in the same way as other records.

6.9 Incident Reporting

6.9.1 If a record or information in any format is missing, lost or inappropriately disclosed it should be reported to the relevant line manager and the IG Team blmkicb.ig@nhs.net as soon as possible and an Incident Report form completed – available in the IG section on the Staff Intranet.

Appendix 1 - Equality Impact Assessment Initial Screening

Please answer the questions against each of the protected characteristic and inclusion health groups. If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken. It is against the law to discriminate against someone because of these protected characteristics. For support and advice on undertaking EQIAs please contact: agcsu.equalities@nhs.net

Name of Policy:	Records Management and Lifecycle Policy
Date of assessment:	16/03/2022
Screening undertaken by:	Head of Information Governance/DPO

Protected characteristic and inclusion health groups. Find out more about the Equality Act 2010, which provides the legal framework to tackle disadvantage and discrimination: https://www.equalityhumanrights.com/en/equality-act/protected-characteristics	Could the policy create a disadvantage for some groups in application or access? (Give brief summary)	If Yes - are there any mechanisms already in place to mitigate the potential adverse impacts identified? If not, please detail additional actions that could help. If this is not possible, please explain why
Age A person belonging to a particular age (for example 32 year olds) or range of ages (for example 18 to 30 year olds).	No	
Disability A person has a disability if she or he has a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day-to-day activities.	No	
Gender reassignment The process of transitioning from one gender to another.	No	
Marriage and civil partnership Marriage is a union between a man and a woman or between a same-sex couple. Same-sex couples can also have their relationships legally recognised as 'civil partnerships'.	No	
Pregnancy and maternity Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth and is linked to maternity leave in the employment context. In the non-	No	

work context, protection against maternity discrimination is for 26 weeks after giving birth, and this includes treating a woman unfavourably because she is breastfeeding.		
Race Refers to the protected characteristic of race. It refers to a group of people defined by their race, colour and nationality (including citizenship) ethnic or national origins.	No	
Religion or belief Religion refers to any religion, including a lack of religion. Belief refers to any religious or philosophical belief and includes a lack of belief. Generally, a belief should affect your life choices or the way you live for it to be included in the definition.	No	
Sex A man or a woman.	No	
Sexual orientation Whether a person's sexual attraction is towards their own sex, the opposite sex, to both sexes or none.	No	
Carers Individuals within the ICB which may have carer responsibilities.	No	
Please summarise the improvements which this policy offers compared to the previous version or position.		
Revised to include records management legislation 2021 https://www.gov.uk/government/publications/records-management-code-of-practice-for-health-and-social-care		
Has potential disadvantage for some groups been identified which require mitigation?		
No – (If there are significant impacts and issues identified a full Equality / Quality Impact Assessment (EQIA) must be undertaken.)		

Appendix 2 - Data Protection Impact Assessment Initial Screening

Data protection is the fair and proper use of information about people. Before completing this form, please refer to the Data Protection Impact Assessment (DPIA) Guidance in the Information Governance (IG) section on the staff Intranet or contact the Data Protection Officer for support via blmkicb.ig@nhs.net

A DPIA is a process to help you identify and minimise the data protection risks. You must do a DPIA for processing that is likely to result in a high risk to individuals. You can use our screening checklist below to help you decide when to do one. If you have answered 'Yes' to any of the 10 screening questions, you must then carry out a full DPIA using the Stage 2 form, which is also available on the Intranet in the IG section.

Name of Policy:	Records Management and Information Lifecycle Policy
Date of assessment:	16/03/2022
Screening undertaken by:	Head of Information Governance/DPO

Stage 1 – DPIA form **please answer 'Yes' or 'No'**

1.	**Will the policy result in the processing of personal identifiable information / data?** This includes information about living or deceased individuals, including their name, address postcode, email address, telephone number, payroll number etc.	Yes
2.	**Will the policy result in the processing of sensitive information / data?** This includes for living or deceased individuals, including their physical health, mental health, sexuality, sexual orientation, religious belief, National Insurance No., political interest etc.	Yes
3.	**Will the policy involve the sharing of identifiers which are unique to an individual or household?** e.g., Hospital Number, NHS Number, National Insurance Number, Payroll Number etc.	Yes
4.	**Will the policy result in the processing of pseudonymised information by organisations who have the key / ability to reidentify the information?** **Pseudonymised data -** where all identifiers have been removed and replaced with alternative identifiers that do not identify any individual. Re-identification can only be achieved with knowledge of the re-identification key. **Anonymised data -** data where all identifiers have been removed and data left does not identify any patients. Re-identification is remotely possible, but very unlikely.	Yes
5.	**Will the policy result in organisations or people having access to information they do not currently have access to?**	No
6.	**Will the policy result in an organisation using information it already holds or has access to, but for a different purpose?**	No
7.	**Does the policy result in the use of technology which might be perceived as being privacy intruding?** e.g., biometrics, facial recognition, CCTV, audio recording etc.	No
8.	**Will the policy result in decisions being made or action being taken against individuals in ways which could have a significant impact on them?** Including profiling and automated decision making. (This is automated processing of personal data to evaluate certain things about an individual i.e., diagnosis and then making a decision solely by automated means - without any human involvement)	No
9.	**Will the policy result in the collection of additional information about individuals in addition to what is already collected / held?**	No
10.	**Will the policy require individuals to be contacted in ways which they may not be aware of and may find intrusive?** e.g., personal email, text message etc.	No