Hertfordshire and West Essex Integrated Care System

NHS
Hertfordshire and West Essex
Integrated Care Board

Records Management & Information Lifecycle Management Policy (which includes Data Quality)

DOCUMENT CONTROL

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the website.

Do you really need to print this document?
Please consider the environment before you print this document and where 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 policy in its entirety.

Document Owner:	Michael Watson, Chief of Staff
Document Author(s):	Anna Cason, Corporate Governance Manager, IG.
Version:	2.0
Approved By:	Executive Team
Date of Approval:	23/10/2023
Date of Review:	24/10/2024
Link to Strategic Objective(s):	1. Increase healthy life expectancy and reduce inequality 2. Give every child the best start in life 3. Improve access to health and care service 4. Increase the number of citizens taking steps to improve their well-being 5. Achieve a balanced financial position annually

Change and Approval History:

Version	Revision Description	Reviewer / Approval Group	Date of Review / Approval
0.1	Draft – New HWEICB policy	Ruth Boughton, IG Manager	May/June 2022
1.0	**Final - Approved**	ICB Board	01/07/2022
1.1	Draft – Full review. Amendments to reflect staff changes and update to Records Management Code of Practice	Anna Cason, Corporate Governance Manager, IG	October 2023
2.0	**Final - Approved**	Executive Committee	23/10/2023

CONTENT

1.0 Introduction

This policy relates to Hertfordshire and West Essex Integrated Care Board (ICB). Records Management and Information Lifecycle relate to the policies, processes, practices, services and tools used by an organisation to manage its information through every phase of its existence, from creation to destruction. Records Management is the process by which the 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.

The Records Management: NHS Code of Practice has been published by the Information Governance Alliance on behalf of 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.

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.

ICB's records are our 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 ICB and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in uniform and equitable ways. They are a valuable resource because of the information they contain and support the delivery of high quality evidence based healthcare.

Information has most value when it is accurate, up to date and accessible when needed, good data quality is essential and the availability of complete, accurate, relevant, accessible and timely data is important in supporting patient care, clinical governance, management of contracts for healthcare planning and accountability.

The ICB has written this Policy and is committed to ongoing improvement of records management functions as they believe a number of organisational benefits will be gained from doing so, including:

- Better use of physical and server space;
- Better use of staff time;
- Improved control of valuable information resources;
- Compliance with legislation and standards;
- Data Quality;
- Reduced costs;
- Archiving and Disposal.

The ICB also believes that internal management processes will be improved by the greater availability of information that will accrue through the recognition of records management as a designated corporate function.

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

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

2.0 Purpose and Scope

The aim of this policy is to ensure that:

- **Records are available when needed** - from which the ICB 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 others.
- **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 disclosures 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 they 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.
- **Staff are trained** - so that all staff are made aware of their responsibilities for recordkeeping and management.

This policy relates to all records held in any format by H&WE ICB. These include:

- All administrative records (for example personnel, estates, financial / contracts and accounting and those associated with complaints);
- All patient health records (for Continuing health care team)
- 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, bullet points and e-mails;
- Audio, memory sticks and CD ROMs

This list is not exhaustive.

3.0 Definitions

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 ICB 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;

The term **Records Lifecycle** 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.

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

Information is a corporate asset. The ICB's records are important sources of administrative, evidential and historical information. They are vital to the ICB to support their 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 their history and procedures.

Data Quality is the ability to supply accurate, timely and complete data, which can be translated into information, whenever and wherever this is required. Data quality is vital to effective decision making at all levels of the organisation.

Data quality must be:

- Complete (in terms of having been captured in full)
- Accurate (the proximity of the figures to the exact or true values)
- Relevant (the degree to which the data meet current and any potential users' needs)
- Accessible (data must be retrievable in order to be used and in order to assess its quality)
- Timely (recorded and available as soon after the event as possible)
- Valid (within an agreed format which conforms to recognised standards – either national or local)
- Defined (understood by all staff who need to know and reflected in procedural documents)
- Appropriately sought (in terms of being collected or checked once during an episode)
- Appropriately recorded (in either paper or electronic format)

4.0 Roles and Responsibilities

4.1 The ICB recognises it has responsibility for ensuring it corporately meets its legal responsibilities and for the adoption of internal and external governance requirements The following definitions apply in the context of this policy:

Role	Responsibilities
Chief Executive	The Chief Executive has overall responsibility for ensuring appropriate mechanisms are in place to support service delivery and continuity.

	Records management is key to this as it will ensure appropriate, accurate information is available when required.
Executive Director	The ICB Executive Directors have local responsibility with the ICB. They are responsible for ensuring appropriate mechanisms are in place to support service delivery and continuity within their local area. Records management is key to this as it will ensure appropriate accurate information is available as required.
Caldicott Guardian	The Caldicott Guardian has particular responsibilities for protecting the confidentiality of patient's / service users information and enabling appropriate information sharing. This role is held by the Director of Nursing and Quality. Acting as the 'conscience' of the organisation, the Caldicott Guardian will actively support work to enable information sharing where it is appropriate to do so and for advising on options for lawful and ethical processing of information.
Senior Information Risk Owner (SIRO)	The role of ICB Senior Information Risk Owner (SIRO) is held by the Chief Finance Officer (CFO). The SIRO is responsible for leading on Information Risk and for overseeing the development of an Information Risk Policy (this forms part of the HWE Information Governance and Framework Policy). The SIRO is also responsible for ensuring the corporate risk management process includes all aspects of information risk and for guaranteeing the ICB Board is adequately briefed on information risk issues
Data Protection Officer (DPO)	To inform and advise staff about their obligations to comply with the UK General Data Protection Regulation (GDPR) and other data protection laws. To be the first point of contact for individuals whose data is processed (employees, patients etc.). The DPO for the ICB is the Head of IG and Risk.
Corporate Governance Manager, IG	The Corporate Governance Manager for IG is responsible for the overall development and maintenance of record management practices throughout the organisation; for drawing up guidance for good records management and data quality practice, promoting compliance with this policy in such a way to ensure the easy, appropriate and timely retrieval of information.
IG Forum	Is the group which will own and report any records management issues to Audit and Risk Committee which provides assurance to the Board.
Information Asset Owner (IAO)	Designated Information Asset Owners (IAOs) are senior members of staff at director / assistant director level or heads of department responsible for providing assurance to the SIRO that information risks within their respective areas of responsibility are identified and recorded and that controls are in place to mitigate those risks.
Information Asset Administrator (IAA)	Information Asset Owners can appoint an Information Asset Administrator (IAAs) to support in the management of records with their department / directorate. Information Asset Administrators are responsible for: • Ensuring that all staff within their directorate / department are fully aware of their responsibilities and legal obligations for records management in compliance with policy

	• Conducting regular audits of records management functions • Reporting policy breaches using the organisation incident reporting mechanism • Ensuring that effective and relevant file management systems are in place for information held within their directorate / department.
All Staff	Under the Public Records Act every member of staff is responsible for the records they create, receive and use in the course of their duties. Staff should ensure that they comply with this policy at all times and report any breaches through the appropriate incident reporting channels. Irrespective of its format, all staff must ensure that the following principles are applied to all records created: • A consistent definition should be adopted to the creation, use, storage, retrieval, archiving, and disposal of records. • All staff should ensure records are stored within a filing structure that reflects the ICB's business functions. Records must not be retained, disseminated or duplicated unnecessarily. • All staff should ensure that records are disposed of by the authorised member of staff and this must be done in accordance with the Records Management Retention and Disposal Schedules. • Staff should keep complete and accurate information of all records, activities and transactions and ensure records are captured and managed within the appropriate information and records management systems. • Staff should ensure e-mail is only used a source transmission and not for storage. • Staff MUST not store information in individual filing systems or on hard drive (that is ' my documents 'or 'desktop').

5.0 Records Management

5.1 Legal Professional Obligation

All NHS records are public under the Public Records Acts. The ICB will take actions as necessary to comply with the legal and professional obligations set out in the NHS Records Management Code of Practice and any new legislation affecting records management as it arises, in particular:

- The Public Records Act 1958.
- The Data Protection Act 2018.
- General Data Protection Regulation 2016
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice and
- The NHS Care Record Guarantee
- Please also refer to **section 11 Appendix**

5.2 Creation and Registration of Records

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

Creation and registration of records
Records are created to support the day-to-day running of the ICB's business. A record is created when it meets the legal requirement defined above (Section 3).

Records created by staff should be arranged in a recordkeeping system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of information.

Records are created to ensure that information is available within ICB:

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

5.3 Record registration and record keeping

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

5.4 Person identifiable and sensitive data (special category data)

Manual or electronic records or record systems (this includes files, indexes, databases, correspondence, lists etc. holding person identifiable information (names, addresses, data of birth, salary etc.) are specifically covered by the requirements of the General Data Protection Regulations (GDPR) and the Data Protection Act 2018. Release or sharing of such data is restricted and all reasonable precautions must be taken to safeguard this type of data.

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

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

Person identifiable data or sensitive data must not be stored on the local hard drive of a computer/laptop; it must be stored on the secure network drives.

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

5.5 Transportation of records

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

Manual records should be transported in an appropriate sealable container, envelopes, transit pouches or boxes. Records should never be left unattended. If being transported in a car they should be placed in the boot.

5.6 Electronic records

The ICB develops and refine procedures and protocols for the security, access, use (including sharing and transport) auditing, storage and archiving of electronic records incorporating NHS requirements and best practice.

Electronic records must not be stored on the hard disk drive of a PC. They should be saved to a dedicated place on the secure network drives, with suitable access controls. This will ensure routine security; disaster recovery and business continuity measures are in place to safeguard the records.

Highly confidential or sensitive records must have appropriate security, access and business continuity controls applied. Where the possibility exists that records could be used in a legal case, particular standards apply and the advice of the IG team must be sought and applied.

5.7 Policy on procedural documents

Certain documents such as policies and procedures undergo a consultation process with numerous drafts prior to approval. It is therefore necessary that reference is made to the document version and this is revised with each review using version controls for the management of multiple revisions to the same document to enable the author and other users to identify one version of a document from the other. These include:

- Keeping successive drafts of the document to provide adequate evidence of the process for example substantial changes during the development of policy.
- Inserting 'Draft' watermarks to indicate the status of the version.
- Following numbering system by using number with points to reflect minor and major version changes for example 0.1, 0.2 for minor changes.
- Changing the final version to v1.0 when the document has reached its 'Final' version and continue with 1.1, 1.2 for minor changes to the first version

The Governance Manager – Policies and Conflicts will be able to advise of the ICB's Policy Approval process and associated guidelines for formatting of policies and can be contacted via hweicbenh.policies@nhs.net

5.8 Referencing and naming conventions

A naming convention is essential for all corporate records. Records should be easily accessible and understandable to staff across the organisation. Corporate records need to follow an agreed naming convention using a systematic approach, for example it should be:

- easily understood by the staff that create and access records
- alphanumeric:
- Beginning with key letters or words identifying the directorate;
- Identifying the department, followed by the business activity;
- Identifying the document name

- Including the initials of the author/creator
- Including a version number
- Identifying the year of creation

5.9 Filing structure

A clear and logical filing structure that aids the retrieval of records must be used. The filing structure should reflect the way in which paper corporate records are filed to ensure consistency. However, if it is not possible, the names allocated to files and folders should allow ‘intuitive filing’. Filing of the primary corporate record to local drives & desktops on PCs and laptops is not permitted.

The agreed filing structure will also help with the management of the retention and disposal of records.

5.10 Shared drives

It is important to consider the content of a document when using this option. Where access to the document is to be limited, the creator of the document must ensure that the record is located in a restricted area on the shared drive. Similarly, where relevant and appropriate, items should be saved in locations accessible to those in the team that require access and in a logical place with a clear file name. Staff should ensure that any personal folders are not created on their department’s shared drive. Folders created on a shared drive should title the project / content subject name or intents.

Records should not be saved on local / personal drives or personal computers.

5.11 Mobile working and remote access to records

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

5.12 Retention periods for records

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

The ICB has adopted the retention periods set out in the Records Management Code of Practice 2021 (Updated 2023). Where further clarification is required, after thorough research and with approval of the IG team, different timescales may be incorporated.

Please see **Section 12 Appendix** for key asset retention periods (extracted from code of practice)

5.13 Destruction of records

Where a document / record has reached its retention date it should be considered for destruction. The process is as follows:

- Review by an appropriate clinician; head of service or a senior manager, to ensure that the records are not needed beyond their listed retention period. If records could be of particular public interest, they should also be considered for archival preservation with The National Archives. The reviewer should sign the ‘Destruction of Records’ sheet (Section 11 Appendix) to demonstrate they are happy with the records being destroyed.
- If documents are stored in an off-site archive, checking the index list of the documents should generally be sufficient (with input from appropriate staff

members where needed). If it is not clear what is in a document, this should be recalled from the archive so a more thorough check can take place.

- The 'Destruction of Records' sheet (Section 11 Appendix) should also be confirmed and signed off by the Caldicott (for patient records) or the SIRO (for corporate records) so destruction can be progressed.
- Secure destruction should be arranged.
- If the documents to be destroyed are with an off-site archive provider, they will usually have process in place to destroy boxes on our behalf. They will provide a certificate of destruction for those documents / boxes that have been destroyed.
- If the documents to be destroyed are on-site (either archived on site, recalled from off-site archive, or had been stored within ICB offices) destruction should be done separately to the usual confidential waste disposal, but can be done by the same company and at the same time. The disposal company will need to provide a certificate of destruction relating to just those documents that have been disposed of, i.e. separate to any certificate that comes with the usual confidential waste disposal.
- A log of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the Records Manager, so that the organisation is aware of those records that have been destroyed and are therefore no longer available.

If a record due for destruction is known to be the subject of a request for information, or potential legal action, destruction should be delayed until disclosure has taken place or, if the authority has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information Act have been exhausted or the legal process completed.

5.14 Archiving of manual records

Once a record has ceased to be accessed regularly, for example if the member of staff has left the organisation or the record refers to a historic business activity, it is necessary for the practical operation of the organisation that this then should be archived to an alternative storage location.

The ICB has adopted the retention periods detailed within the Records Management Code of Practice Section 5 Management of records when the minimum retention period is reached and appendix II Retention schedule details the minimum retention period for each type of record. Records, whatever the media, may be retained for longer than the minimum period, however this requires formal approval of the Information Governance Forum. They should not however be retained for more than 30 years. Where a period longer than 30 years is required (for example to be preserved for historical purposes), or for any pre-1948 records, the National Archives should be consulted.

It should be noted that records containing personal information are subject to the Data Protection Act 2018. Section 90 sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary).

If a particular record is not listed in the schedules the Information Governance Manager should be contacted for advice.

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

5.15 Data Quality

All staff must conform to legal and statutory requirements and recognised good practice, aim to be significantly above average on in-house data quality indicators, and will strive towards 100% accuracy across all information systems.

All data collection, manipulation and reporting processes by the ICB will be covered by clear procedures which are easily available to all relevant staff, and regularly reviewed and updated.

All staff should be aware of the importance of good data quality and their own contribution to achieving it and should receive appropriate training in relation to data quality aspects of their work.

Teams should have comprehensive procedures in place for identifying and correcting data errors, such that information is accurate and reliable at time of use.
It is imperative that regular validation processes are undertaken on data being recorded to assess completeness, accuracy, relevance, accessibility, and timeliness. Such processes may include checking for duplicate data, validating waiting lists, ensuring that national definitions and coding standards are adopted, pseudonymised data should be used for this purpose.
Validation should be accomplished using either of the following methods:

- Bulk reporting, which involves a large single process of data analysis to identify all areas where quality issues exist and correct them. Bulk Reporting can be used as an initial data quality tool as this will quickly highlight any areas of concern, however, further investigation will be required to identify more specific issues.

The use of data standards within systems can greatly improve data quality. These can be incorporated into systems either using electronic selection lists within computer systems or manually generated lists for services that do not yet have computer facilities. Either method requires the list to be generated from national or locally agreed definitions and must be controlled, maintained and updated in accordance with any variations that may occur. Any documentation that refers to the data standards must also be updated as needed and disseminated to all relevant parties.

5.16 Dealing with lost or misplaced records

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

- Inform your line manager as soon as you are aware of the loss.
- Contact the IG team via hweicbhv.dpo@nhs.net and complete an incident form as soon as you become aware of a loss or possible loss.

5.17 Confidential Waste/Shredder

The GDPR and The Data Protection Act 2018 states the correct procedures must be taken to protect personal data. All confidential material must be disposed of in a secure way either in a confidential waste bin or by use of a cross shredder. For disposal of electronic media the HBL ICT Services will arrange safe disposal.

5.18 Development Process

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

The audit will:

- Identify areas of operation covered by the ICB’s policies and identify which procedures should comply with the policy.
- Follow a mechanism for adapting the policy to cover missing areas if these are critical to the creation and use of records and use a subsidiary development plan if there are major changes to be made.

- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance and
- Highlight where non-conformance to the procedures is occurring and suggest a tightening of controls and adjustment to related procedures.

5.19 Scanning

For the purpose of business efficiency and adapting to paperless innovation, the ICB will consider the option of scanning paper records into electronic format; this will facilitate issues with storage space. Where this is proposed, the following factors will be taken into consideration:

- The costs of the initial and then any later media conversion to the required standard, bearing in mind the length of the retention period for which the records are required to be kept.
- The need to consult in advance with the local place of deposit or the National Archives with regard to records which may have archival value, as the value may include the format in which it was created; and
- The need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the ‘Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically.

Standards for a Scanned Image

Images must adhere to the following standards;

- Every image must be a true representation of the original document
- All text must be legible.
- The patient / staff member associated with the document must be clear on the scanned image.
- All images received from an external source must be date stamped when received, before scanning into electronic form. This must be clear on the scanned document.
- There must be an audit trail on the system of the date and time when the image was scanned into the system.
- There must be a completed audit trail of information detailing who scanned and saved the image into the system, inclusive of time and date.
- The image should be saved to a suitable agreed resolution to ensure quality.
- An audit trail must be kept detailing destruction of any documents. The best practice process would be to retain the original information with the scanned image.

Standards for an Adobe Image

Documents may be converted into an ‘Adobe’ image and saved like a scanned image. However, images must adhere to the following standards:

- Every image must be a true representation of the original document
- All text must be legible
- The patient / staff member associated with the document must be clear on the image
- There must be an audit trail on the system of the date and time when the image was saved into the system.
- There must be an audit trail of who saved the image into the system.
- The image should be checked before it is saved to ensure quality.

5.20 Tracking and Tracing

Tracking and tracing procedures implemented must enable the movement and location of records to be controlled. This will provide an auditable trail of record transactions. The process need not be a complicated one, for example, a tracking procedure could comprise of a book that staff members sign when a corporate record is physically removed from, or returned to, its usual place of storage (not when a record is simply removed from a filing cabinet by a member of staff from that department as part of their everyday duties).

Tracking mechanisms to be used should include:

- the item reference number or identifier.
- a description of the item (for example the file title)
- the person, position or operational area / team who may have possession of the item.
- the date and time of movement that took place.

5.21 Secure Transfer of Information & Protective Marking

It is important that when information needs to be shared, it is transferred and / or transported in a secure and efficient manner. There are many different methods of transferring information and it is vital that the most appropriate method is chosen, dependent on the type of information to be transferred.

For more information on methods of secure transfer, please see Information and Cyber Security Policy.

Government Security Classifications have been implemented to assist in deciding how to share and protect information. Please refer to section 22 of the Information and Cyber Security Policy.

5.22 The Intranet

The Intranet is a web-based communication tool. It has been set up in a centralised location to enable staff to easily locate any materials that they may need. This is to help them carry out their duties or to generally find out more information on a particular subject.

Examples of information which should be published on the Intranet are:

- Policies, Procedures and Strategies
- Forms
- Contact Lists
- Minutes of Meetings
- General Information
- Newsletters

Examples of information which ***should not*** be published on the Intranet are:

- Confidential Information
- Patient / Personal Information
- Commercially Sensitive Information
- Incomplete Information for example. draft documents

5.23 Public Facing Website

Information that is intended to be made publicly available should be published through the Freedom of Information (FOI) Publication scheme located on the Public Facing Website. Requests for new content to be added should be made via the IG Lead / FOI Co-ordinator.

Examples of information which should be routinely published on the public facing website are:

- The ICB Annual Report
- Press Releases
- Up to date contact Information for the ICB
- Information about services provided by the ICB
- A list of the main categories of Information that have been most frequently requested via the FOIA
- A list of data sets requested previously under the FOIA

Examples of information which ***should not*** be published on the public facing website are:

- Person Identifiable Information of any description
- Confidential Reports
- Commercially Sensitive Information
- Incomplete Information for example draft documents, any information not approved or finalised

6.0 Monitoring Compliance

The Policy will be monitored by the IG Forum and the Audit and Risk Committee. The IG Forum has a responsibility to provide assurances that this framework is adequate for providing clear guidance in the event of significant changes which may affect it. The designated IG Manager will ensure that adequate arrangements exist for:

- Reporting incidents, Caldicott issues
- Analysing and upward reporting of incidents and adverse events
- Reporting IG work programs and progress reports
- Reporting Data Security and Protection Toolkit (DSPT) assessments and improvement plans
- Communicating IG developments

It is the responsibility of all the ICB staff to ensure compliance with this policy and procedure. Data quality will be subject to internal control processes within the ICB, and subject to external scrutiny.
The ICB can also use complaints as a monitoring tool for data quality.

All staff need to protect patient confidentiality and they are reminded they may be subject to disciplinary action if they breach the UK GDPR/DPA 2018. The Information Commissioner's office has made it clear they will impose fines on organisations and individuals for serious breaches of the UK GDPR/Data Protection Act 2018.

7.0 Education and Training

All staff (permanent, temporary, contract or seconded) likely to be in post for 3 months or longer, are required to complete the online mandatory IG training module- Data Security Awareness Level 1, within the first month of employment (or within two weeks of joining if they work with person identifiable information).
The Data Security Awareness Level 1 e-learning module can be accessed either through ESR (https://my.esr.nhs.uk/) or e-learning for health (https://www.e-lfh.org.uk/)

Further training is required for staff who process personal information, and staff within specific roles

8.0 References

NHS Records Management Code of Practice
Records Management Code of Practice for Health and Social Care 2021
UK General Data Protections Regulations (GDPR)
Data Protection Act 2018
Freedom of Information Act 2000

9.0 Associated Documentation

Information Governance Framework and Policy
Access to information Policy
Information & Cyber Security Policy

Appendix 1

Legal Acts Pertaining to this Document

The Data Protection Act 2018: all staff must abide by the Data Protection Act 2018 which controls how personal information is used. It incorporates the UK General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED).

Personal information relating to staff, suppliers, etc. may only be accessed and used by staff on a need to know basis. Unauthorised disclosure of such "personal data" may result in disciplinary action and prosecution. Under the Act, Article 5 states personal data must be:

- Processed fairly, lawfully and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- Processed in a manner than ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Every individual, including staff are entitled to be informed of any personal data held on them by the organisation, to access that data and to have it corrected if it is inaccurate All enquiries relating to the Data Protection Act must be referred to the Data Protection Officer.

- **The Public Records Act 1956 and 1967 and Freedom of Information Act 2000:** These Acts regulate the storage and publication of records held by public bodies.
- **The Copyright, Designs and Patents Act 1988**: It is illegal to copy, without the appropriate consent, software except for backup purposes, and each machine must have a license for its software. The copyright owner has the right to bring civil proceedings and in certain circumstances criminal proceedings against those that infringe their rights.

Department of Health Guidance: Guidance and standards for the Protection and Use of Patient Information and Caldicott Guardian guidance can be found on the Department of Health website.

Destruction of Records

Appendix 2

Data Controller:

Team:

Description of records:

Reviewing clinician / Head of service / Senior manager name*

Reviewing the information:

*Enter **X** in the appropriate box below*

- I confirm that these documents / boxes have been reviewed and are no longer required □
- I confirm that these records have been reviewed and should be kept. □

The records should be reviewed again after a period of □ months / years

*Signature	Date

Confirmation of destruction by:

Caldicott Guardian □ **SIRO** □

Name:

By signing this you are confirming that you agree with the opinion above and that these records should:

Be kept and reviewed again after the period mentioned above □

Be offered to The National Archives for archival preservation □

Be securely destroyed □

SIRO/Caldicott Guardian Signature	Date

Appendix 3

Records Retention Schedule Extract

Care Records

Record type	Category	Retention period	Disposal action	Notes
Adult health records not covered by any other section in this schedule (includes medical illustration records such as x-rays and scans as well as video and other formats. Also includes care plans)	Care Record	8 years	Review and consider transfer to Place of Deposit	Records involving pioneering or innovative treatment may have archival value, and their long term preservation should be discussed with the local Place of Deposit or The National Archives.

Record type	Category	Retention period	Disposal action	Notes
Adult social care records (including care plans)	Care Record	8 years	Review and destroy if no longer required	

Record type	Category	Retention period	Disposal action	Notes
Children's records (including midwifery, health visiting and school nursing) : can include medical illustrations, as well as video and audio formats	Care Record	Up to 25th or 26th birthday	Review and destroy if no longer required	Retain until 25th birthday, or 26th if the patient was 17 when treatment ended.

Record type	Category	Retention period	Disposal action	Notes
Dental records: clinical care records	Care Record	11 years (note this changed from 15 years	Review, and destroy if no	Based on Limitations Act 1980. This applies to all dental care

		in May 2023 following legal advice)	longer required	settings and the BSA. This also includes FP17 or FP17O forms.

Record type	Category	Retention period	Disposal action	Notes
Dental records: finance related	Care Record	2 years	Review, and destroy if no longer required	These include PR forms. NHS BSA may retain financial records for a minimum 6 years.

Record type	Category	Retention period	Disposal action	Notes
Electronic Patient Record Systems (EPR)	Care Record	Refer to notes	Review and destroy if no longer required	Where the system has the capacity to destroy records in line with the retention schedule, and where a metadata stub can remain, demonstrating the destruction, then the Code should be followed in the same way for digital as well as paper records with a log kept of destruction. If the EPR does not have this capacity, then once records reach the end of their retention period, they should be made inaccessible to system users upon decommissioning. The system, along with the audit trails, should be retained for the retention period of the last entry related to the schedule.

Corporate Governance

Record type	Category	Retention period	Disposal action	Notes
Board meetings*	Corporate Governance		Review and transfer to	A local decision can be made on how long to retain the minutes of board meetings, and associated

		Up to 20 years	Place of Deposit	papers linked to the board meeting, but this must not exceed 20 years, and will be required to be transferred to the local Place of Deposit or The National Archives for National Bodies.

Record type	Category	Retention period	Disposal action	Notes
Board meetings: closed boards*	Corporate Governance	Up to 20 years	Review and transfer to Place of Deposit	Although these may still contain confidential or sensitive material, they are still a public record and must be transferred at 20 years, and any FOI exemptions noted, or indications that the duty of confidentiality applies.

Record type	Category	Retention period	Disposal action	Notes
Chief Executive records*	Corporate Governance	Up to 20 years	Review and transfer to Place of Deposit	This may include emails and correspondence where they are not already included in board papers.

Record type	Category	Retention period	Disposal action	Notes
Committees: major, listed in Scheme of delegation or report direct into the board, including major projects*	Corporate Governance	Up to 20 years	Review and transfer to Place of Deposit	

Record type	Category	Retention period	Disposal action	Notes
Committees: minor, not listed in scheme of delegation*	Corporate Governance	6 years	Review and consider transfer to Place of Deposit.	Includes minor meetings, projects, and departmental business meetings. These may have local historical value required transfer consideration.

Record type	Category	Retention period	Disposal action	Notes
Data Protection Impact Assessments (DPIAs)	Corporate Governance	6 years	Review and destroy if no longer required	Should be kept for the life of the activity to which it relates, plus six years after that activity ends. If the DPIA was one -off, then 6 years from completion.

Record type	Category	Retention period	Disposal action	Notes
Destruction certificates or record of information held on destroyed physical media	Corporate Governance	20 years	Review and dispose of if no longer required	Where a record is listed for potential transfer to Place of Deposit have been destroyed without adequate appraisal, consideration should be given to a selection of these as an indicator of what has not been preserved.

Record type	Category	Retention period	Disposal action	Notes
Electronic metadata destruction stubs	Corporate Governance			Refer to destruction certificates.

Record type	Category	Retention period	Disposal action	Notes
Incidents: serious	Corporate Governance	20 years	Review and consider transfer to Place of Deposit	Retention begins from the date of the Incident; not when the incident was reported.

Record type	Category	Retention period	Disposal action	Notes
Incidents: not serious	Corporate Governance	10 years	Review and destroy if no longer required	Retention begins from the date of the incident; not when the incident was reported.

Record type	Category	Retention period	Disposal action	Notes

Incidents: serious incidents requiring investigation	Corporate Governance	20 years	Review and consider transfer to Place of Deposit	These include independent investigations into incidents. These may have permanent retention value so consult with the local Place of Deposit. If they are not required, then destroy.

Record type	**Category**	**Retention period**	**Disposal action**	**Notes**
Non-clinical QA records	Corporate Governance	12 years	Review and destroy if no longer required	Retention begins from the end of the year to which the assurance relates.

Record type	**Category**	**Retention period**	**Disposal action**	**Notes**
Patient advice and liaison service (PALS) records	Corporate Governance	10 years	Review and destroy if no longer required	Retention begins from the close of the financial year to which the record relates.

Record type	**Category**	**Retention period**	**Disposal action**	**Notes**
Patient surveys: individual returns and analysis	Corporate Governance	1 year after return	Review and destroy if no longer required	May be required again if analysis is reviewed.

Record type	**Category**	**Retention period**	**Disposal action**	**Notes**
Patient surveys: final report	Corporate Governance	10 years	Review and consider transfer to Place of Deposit	Organisations may want to keep final reports for longer than the raw data and analysis, for trend analysis over time. This period can be extended, provided there is justification and organisational approval.

Record type	Category	Retention period	Disposal action	Notes
Policies, strategies and operating procedures, including business plans*	Corporate Governance	Life of organisation plus 6 years	Review and consider transfer to Place of Deposit	Retention begins from when the document is approved, until superseded. If the retention period reaches 20 years from the date of approval, then consider transfer to Place of Deposit.

Record type	Category	Retention period	Disposal action	Notes
Risk registers	Corporate Governance	6 years	Review and destroy if no longer required	Retention period in accordance with the Limitation Act and corporate awareness of risks.

Record type	Category	Retention period	Disposal action	Notes
Staff surveys: individual returns and analysis	Corporate Governance	1 year after return	Review and destroy if no longer required	Forms are anonymous so do not contain PID unless provided in free text boxes. May be required again if analysis is reviewed.

Record type	Category	Retention period	Disposal action	Notes
Staff surveys: final report	Corporate Governance	10 years	Review and consider transfer to Place of Deposit	Organisations may want to keep final reports for longer than the raw data and analysis, for trend analysis over time. This period can be extended, provided there is justification and organisational approval.

Communications

Record type	Category	Retention period	Disposal action	Notes
Intranet site*	Communications	6 years	Review and consider transfer to	

			Place of Deposit	

Record type	Category	Retention period	Disposal action	Notes
Patient information leaflets	Communications	6 years	Review and consider transfer to Place of Deposit	These do not need to be leaflets from every part of the organisation. A central copy can be kept for potential transfer.

Record type	Category	Retention period	Disposal action	Notes
Press releases and important internal communications	Communications	6 years	Review and consider transfer to Place of Deposit	Press releases may form part of a significant part of the public record of an organisation which may need to be retained.

Record type	Category	Retention period	Disposal action	Notes
Public consultations	Communications	5 years	Review and consider transfer to Place of Deposit	Whilst these have a shorter retention period, there may be wider public interest in the outcome of the consultation, particularly where this resulted in changes to the services provided, and so may have historical value.

Record type	Category	Retention period	Disposal action	Notes
Website*	Communications	6 years	Review and consider transfer to Place of Deposit	The Place of Deposit may be able to receive these by a regular crawl. Consult with the Place of Deposit on how to manage the process. Websites are complex objects, but crawls can be made more effective if certain steps are taken.

Staff Records & Occupational Health

Record type	Category	Retention period	Disposal action	Notes
Duty roster	Staff Records and Occupational Health	6 years	Review and if no longer needed destroy	Retention begins from the close of the financial year.

Record type	Category	Retention period	Disposal action	Notes
Exposure monitoring information	Staff Records and Occupational Health	40 years or 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.

Record type	Category	Retention period	Disposal action	Notes
Occupational health reports	Staff Records and Occupational Health	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner	Review and if no longer needed destroy	

Record type	Category	Retention period	Disposal action	Notes
Occupational health report of staff member under health surveillance	Staff Records and Occupational Health	Keep until 75th birthday	Review and if no longer needed destroy	

Record type	Category	Retention period	Disposal action	Notes
Occupational health report of staff member under health surveillance where they have been subject to radiation doses	Staff Records and Occupational Health	50 years from the date of the last entry or until 75th birthday, whichever is longer	Review and if no longer needed destroy	

Record type	Category	Retention period	Disposal action	Notes
Staff record	Staff Records and Occupational Health	Keep until 75th birthday (see notes)	Review, and consider transfer to Place of Deposit	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. Some Place of Deposits accession NHS staff records for social history purposes. Check with your local Place of Deposit about possible accession. If the Place of Deposit does not accession them, then the records can be securely destroyed once the retention period has been reached.

Record type	Category	Retention period	Disposal action	Notes
Staff record: summary	Staff Records and Occupational Health	75th Birthday	Review, and consider transfer to Place of Deposit	Please see the good practice box staff record summary used by an organisation. Some organisations create summaries after a period of time since the staff member left (usually 6 years). This practice is ok to continue if this is what currently occurs. The summary, however, needs to be kept until the staff member's 75th birthday, and then consider transferring to Place of Deposit. If the Place of Deposit does not require them, then they can be securely destroyed at this point.

Record type	Category	Retention period	Disposal action	Notes
Timesheets (original record)	Staff Records and Occupational Health	2 years	Review and if no longer needed destroy	Retention begins from creation.

Record type	Category	Retention period	Disposal action	Notes
Staff training records	Staff Records and Occupational Health	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 following is recommended: Clinical training records - to be retained until 75th birthday or six years after the staff member leaves, whichever is the longer. Statutory and mandatory training records - to be kept for ten years after training completed. Other training records - keep for six years after training completed.

Record type	Category	Retention period	Disposal action	Notes
Disciplinary records	Staff Records and Occupational Health	Retain for 6 years	Review and destroy if no longer required	Retention begins once the case is heard and any appeal process completed. The record may be retained for longer, but this will be a local decision based on the facts of the case. The more serious the case, the more likely it will attract a longer retention period. Likewise, a one-off incident may need to only be kept for the minimum time stated. This applies to all cases, regardless of format.

Legal, Complaints and Information Rights

Record type	Category	Retention period	Disposal action
Complaints: case files	Legal, Complaints and Information Rights	10 years	Review and destroy if no longer required

Record type	Category	Retention period	Disposal action
Fraud: case files	Legal, Complaints and Information Rights	6 years	Review and destroy if no longer required

Record type	Category	Retention period	Disposal action
Freedom of Information (FOI) requests, responses to the request and associated correspondence	Legal, Complaints and Information Rights	3 years	Review and destroy if no longer required

Record type	Category	Retention period	Disposal action
Freedom of Information (FOI) requests: where there has been an appeal	Legal, Complaints and Information Rights	6 years	Review and destroy if no longer required

Record type	Category	Retention period	Disposal action
Industrial relations: including tribunal case records	Legal, Complaints and Information Rights	10 years	Review and consider transfer to Place of Deposit

Record type	Category	Retention period	Disposal action
Litigation records	Legal, Complaints and Information Rights	10 years	Review and consider transfer to Place of Deposit

Record type	Category	Retention period	Disposal action
Software licences	Legal, Complaints and Information Rights	Lifetime of software	Review and destroy if no longer required

Record type	Category	Retention period	Disposal action
Subject Access Requests (SAR), response, and subsequent correspondence	Legal, Complaints and Information Rights	3 years	Review and destroy if no longer required

Record type	Category	Retention period	Disposal action
Subject Access Request (SAR): where there has been an appeal	Legal, Complaints and Information Rights	6 years	Review and destroy if no longer required

APPENDIX 4

Equality Impact Assessment and Health Inequality Impact Assessment

Equality Analysis

Title of policy, service, proposal etc being assessed:
Records Management and Information Lifecycle Policy

What are the intended outcomes of this work?

This policy is necessary for identifying the resources needed to ensure records of all types are properly controlled, of good quality, tracked, accessible and available for use and eventually archived or otherwise disposed of in line with the principles contained within legal requirements and guidelines. It also ensure that the document meets the correct data quality standards.

How will these outcomes be achieved?

The Records Management and Information Lifecycle Policy v2.0 will be published and distributed to all employees. This policy will guide ICB's records management activities. It will replace v1.0, adopted on 1 July 2022.

Who will be affected by this work?
There is no scope for differential impact based on a person's characteristics.

Evidence

Impact Assessment Not Required

This is an information governance policy which specifies roles, responsibilities and processes that ensure the ICB comply with legislation and guidance. There is no differential impact on people. It has no differential impact on those who have or share a protected characteristic.

Equality and Diversity Lead Sign off

Full impact assessment not required.

Paul Curry, Equality and Diversity Lead, 7 November 2023