NHS
Coventry and Warwickshire
Integrated Care Board

Records Management Policy

Page 1 of 19

Reference Number:	*This will be applied to all new ICB-wide PPSs by the Governance and Corporate Affairs Team and will be retained throughout its life span.*
Version:	Version 2
Name of responsible Committee and date approved or recommended to Governing Body:	Clinical Quality and Governance Committee
Date approved by Integrated Care Board (if applicable):	1 July 2022
Next Review Date:	March 2024
Expiry Date:	Sept 2024
Name of author and title:	Kelly Huckvale, Compliance Manager (Information Governance),AGEM CSU
Name of reviewer and title:	Kelly Huckvale, Compliance Manager (Information Governance),AGEM CSU
Department:	Governance (Information Governance)

VERSION HISTORY

Date	Version	Changes made to previous version	Consulting and Endorsing Stakeholders, Committees / Meetings / Forums etc.
April 2021	1	New Policy	
April 2022	2	Amended in line with NHS Records Management Code of Practice 2021	

1. Introduction

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

1.2 Records are a valuable resource because of the information they contain. NHS Coventry and Warwickshire Integrated Care Board (hereafter referred to as the "ICB") records are its corporate memory, providing evidence of activities, actions and decisions and represent 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 service users, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

1.3 Records have most value when they are accurate, up to date and accessible whenever and wherever there is a justified need. The ICB is therefore committed to ensuring efficient and effective management of all aspects of records, in any format or media type, from their creation all the way through their lifecycle to their eventual disposal.

1.4 Any NHS record created and used by an individual is a public record[1] and is subject to information requests at any time up to disposal, for example under the Freedom of Information Act 2000 or the Data Protection Act 2018. It is therefore imperative that records are closely monitored and managed throughout their lifecycle. All NHS organisations have a duty under the Public Records Act 1958 to ensure the safekeeping, availability and eventual disposal of all types of records.

1.5 The ICB is committed to compliance with current legal requirements and professional best practice. This document sets out the ICB policy for managing records. It is based upon the "NHS Records Management Code of Practice 2021" [2]which has been published by NHS Transformation Directorate and from guidance issued by the National Archives[3].

1.6 This policy is a key component of the ICB's overall Information Governance framework and should be considered alongside the other Information Governance policies, and other relevant ICB policies, as listed in Appendix 1.

2. Objectives

2.1 To set out a Policy from which staff will manage records and from which managers can develop departmental procedures to ensure that records are controlled effectively to meet their operational needs, whilst complying with legal obligations.

2.2 To encourage common standards of practice.

2.3 To ensure that the ICB meets legal obligations with regard to retention periods and the final disposition of records, i.e. destruction or permanent archival preservation.

2.4 To ensure that the ICB's storage systems maintain the confidentiality, security and integrity of all records.

---

1 Public Records Act 1958, section 3 (1)-(2)

2 Records Management Code of Practice 2021

3 The National Archives, www.nationalarchives.gov.uk

2.5 To ensure that the records management standards of the NHS Digital Data Security and Protection Toolkit (DSPT) are met to a sufficient standard.

3. Scope

3.1 This policy must be adhered to by permanent and temporary staff, secondees, contracted staff, students and voluntary workers and anyone else who works within or under contract to the ICB.

3.2 This policy applies to all records of the ICB held in any format (e.g. paper, electronic, audio visual). These include (but are not limited to) records relating to the administration of either ICB, personnel, finance, estates, complaints, legal, commissioning, continuing health care funding, individual funding, individual placements funding.

3.3 This policy applies to the handling of GP patient health records in transit or inactive records held in storage. However, the actual content of such records is outside the scope of this policy.

3.4 This policy must be adhered to through the full lifecycle of a record (see 4.3 for definition of lifecycle).

3.5 Health records of patients/service users used for the direct delivery of care are outside the scope of this policy.

4. Definitions

4.1 *For the purposes of this policy, the difference between a **'document'** and a **'record'** is –*

4.1.1 A **document** is any piece of written or recorded information in any form, produced or received by an organisation or person. It may contain, for example, details of a business decision and will therefore need to become part of a formal record, or a document may be of very short- term value and will not need to be retained.

4.1.2 A **record** is anything that contains information (in any media or format) created or received and which forms permanent evidence of a business activity and which needs to be retained as evidence of such activity. A document becomes a record when it has been finalised and becomes part of the ICB's corporate information. At this point, the record should not be amended without clearly indicating that changes have been made and creating an audit trail.

Local guidance should be created to advise staff within a work area of the type of content that should be retained as a record, in what format it should be retained, where it should be stored etc. pertaining to the business function of that work area.

4.2 Corporate records - records other than health records that are of, or relating to, the ICB's business activities covering all the functions processes, activities and transactions of the ICB[4].

Corporate records may be held in any format (e.g. paper or electronic) and include any records stored on the ICB's networks or ICB issued or approved equipment/devices.

Examples of corporate records include (but are not limited to) meeting papers, reports of any description, tender documents, evaluation reports, ledgers, contracts, agreements, healthcare funding, strategies, policies and other administrative documents.

Corporate records may include service user information. Corporate records may include clinical or healthcare information which is used to support the funding or provision of care but is not used directly for the primary care of the patient. (Records used directly for the primary care of the patient are classed as clinical records, and usually held by provider organisations).

4.2 **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 destruction or archival preservation.

4.3 **National Archives** – The National Archives is a centre of expertise in creating, managing and preserving official information and is the UK government's official archive. They give detailed guidance to government departments and the public sector, including the NHS, on information management and advise others about the care of historical archives.

4.4 **Appraisa**l – the process of evaluating which records should be kept, and for how long; to meet the needs of the ICB, the requirements of government accountability and the expectations of researchers and other users of records. This also includes consideration as to whether records have archival value.[5]

4.5 **Disposal** – the implementation of appraisal and review decisions. These will either be the secure destruction of records or the transfer of custody of records for archival preservation.[6]

5. Roles and Responsibilities

5.1 The **ICB's Governing Body** has a duty to ensure that all records are managed in accordance with legal obligations and professional best practice. The Governing Body will be kept informed of any risks or issues in relation to compliance with this policy via the Clinical Quality and Governance Committee.

5.2 The **Chief Executive** has ultimate responsibility for the confidentiality, integrity, availability and processing of all records across the ICB.

5.3 The **Director of Corporate Affairs** is the lead for records management and is responsible for:

5.3.1 identifying records lead(s) who will develop a records management system, which meets the business needs of the organisation and which is in keeping with the requirements of this policy.

5.3.2 identifying records lead(s) who have responsibility for maintaining a department register of all records, as described in Section 15.0 of this policy.

5.3.3 ensuring that all records within their departments are managed in accordance with this policy.

5.3.4 developing records management procedures which comply with this policy and which meet the operational needs of the directorate/department/work area.

5.3.5 developing local guidance to advise staff within a work area of the type of

content that should be retained, in what format it should be retained, where it should be stored, etc. pertaining to the business function of that work area.

5.3.6 developing local procedures and guidance to ensure the quality of information across all systems, whether manual or electronic; and covering all information, e.g. staff related, corporate information, third party contractor information, service user information.

5.4 **All staff** (as listed in paragraph 3.1) will:

5.4.1 be aware that under the Public Records Act, anyone listed in paragraph 3.1 is responsible for any record that they create or use in the course of their duties.

5.4.2 comply with the most up-to-date version of this policy.

5.4.3 ensure that where a breach of this policy has occurred, or a significant risk has been identified, it is reported to their Line Manager so that the Incident Management process is invoked in accordance with the Policy and Procedure for the Reporting and Management of Clinical and Non-Clinical Incidents.

5.4.4 be aware that any breach of this policy may result in disciplinary proceedings. Furthermore, any breach of legal obligations may result in legal proceedings against an individual and/or the ICB.

5.5 The **Information Governance Steering Group** will**:**

5.5.1 agree local retention and disposal schedules for any records which are not listed in the current version of the NHS Records Management Code of Practice 2021.

5.5.2 monitor compliance with this policy and inform the Governing Body of any risks or issues via the Clinical Quality and Governance Committee.

5.5.3 review information security reports, risk assessments and audits, which relate to records management.

5.5.4 review all related incidents raised through the ICB's Incident Reporting process.

5.6 The **Arden & GEM CSU Compliance Manager (Information Governance)**:

5.6.1 provides guidance on records management as required.

5.6.2 assists the ICB with maintaining a log of local retention and disposal schedules for any records which are not listed in the current version of the Department of Health and Social Care Disposal and Retention Schedule.

5.6.3 assists with the implementation of this policy and keeps the Information Governance Steering Group informed of any issues.

5.6.4 monitors all records management incidents.

6. Legal and Professional Obligations

6.1 All NHS records are public records under the Public Records Acts. The ICB is committed to ensuring compliance with the legal and professional obligations set out in the NHS Records Management Code of Practice 2021, in particular:

- The Public Records Act 1958

- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice
- Any new legislation affecting records management as it arises.

7. General Principles

All records will be managed throughout their lifecycle to ensure that:

7.1 **records are available when needed -** from which the ICB is able to form a reconstruction of activities or events that have taken place.

7.2 **records can be accessed -** a record and the information within it can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist.

7.3 **records can be interpreted -** the context of the record can be interpreted - who created or added to the record and when, during which business process, and how the record is related to other records**.**

7.4 **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.

7.5 **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.

7.6 **records are secure -** from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required.

7.7 **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.

7.8 **staff are trained** – so that all staff are made aware of their responsibilities for record-keeping and record management.

8. Records Quality

8.1 Records should be complete and accurate in order to allow staff to undertake appropriate actions in the context of their responsibilities, to facilitate an audit or examination of either ICB by anyone authorised to do so, and to protect the rights of the ICB, service users, staff and any other people affected by the ICB's actions.

8.2 Records should be updated in a timely manner.

8.3 Anyone creating or making entries in or adding documents to a record is responsible for their accuracy.

8.4 Records should keep clear, accurate and legible management records of relevant decisions and transactions in line with the law and departmental requirements.

8.5 There must be a system in place to ensure the original information can still be accessed when additions or alterations are made. Details of the system should be contained in local procedures and guidance (as per 8.6).

8.6 Local procedures and guidance must be available across all systems and departments to ensure that information is of the highest quality. These procedures will contain details of controls to ensure accuracy and outline the process for dealing with inaccurate and/or duplicate information or records.

9. Record Tracking, Storage and Maintenance

9.1 The movement and location of paper records should be recorded on the ICB's Information Asset Register to ensure that the whereabouts of a record is always known and that it can be easily retrieved at any time.

9.2 Storage accommodation for manual records should be clean and tidy, should prevent damage to the records and should provide a safe working environment for staff.

9.3 Digital/electronic records must be saved to a ICB networked drive, which will be backed-up by the IT provider.

9.4 Back-up and planned migration to new digital/electronic platforms should be designed and scheduled to ensure continuing access to readable information.

9.5 Records containing confidential or person identifiable information must be protected from unauthorised access, inadvertent alteration or erasure, at all times.

9.6 Equipment/facilities used to store records on all types of media should provide storage that is safe and secure from unauthorised access and which meets health and safety and fire regulations, but which also allows maximum accessibility to the records commensurate with frequency of use.

9.7 Identification and safeguarding of vital records should be included in disaster recovery and business continuity plans.

10. Transporting Confidential Records (including GP Patient Records in transit)

10.1 Confidential records must only be taken off-site when absolutely necessary. A log of what information is being moved and why, and when applicable, details of where and to whom it is being taken, by whom and how, should also be recorded.

10.2 Confidential records which need to be dispatched externally must be sent by secure post or approved Courier.

Where secure post is required, a tracked and trace service should be used, for example Royal Mail Special Delivery. Recorded Delivery does not meet Department of Health standards as the post is not tracked throughout the whole journey.

A plain, robust envelope or packet must be used and must not be overfilled.

Caution should be exercised if re-using envelopes or packets, to ensure that there is no ambiguity as to the recipient, sender or content.

See paragraph 11.8 for more information on secure courier services.

10.3 When sending documents internally, confidential records must be transported in a sealed container/envelope/transit bag and labelled NHS CONFIDENTIAL. The recipient's details in full must be clearly visible. A return address should be visible.

Caution should be exercised if re-using envelopes or packets, to ensure that there is no ambiguity as to the recipient, sender or content.

10.4 When hand carried by staff, confidential records must be contained in a robust folder, wallet, or envelope, to safeguard against such things being accidentally viewed by unauthorised persons, accidental dropping or dispersing of documents by a gust of

wind. Diligence is required to ensure that the information is not left behind unintentionally.

10.5 Confidential records must not be left unattended unless it is unavoidable. In the event that they must be left unattended, every precaution must be taken to keep them secure and inaccessible to unauthorised persons. For example, do not leave them visible in a car; lock them in the boot for the shortest possible time. They must never be left in a vehicle overnight.

10.6 If appropriate obtain a receipt upon delivery.

10.7 When appropriate, ensure that confidential records are returned back on site as soon as possible. Record that the information has been returned.

10.8 Courier services for confidential records must only be obtained from an organisation that has signed up to the national agreement for public sector bodies, or that has provided adequate security assurances set out in a written contract with the ICB.

An up to date list of courier companies which have signed up to the national agreement for public sector bodies can be viewed on the Crown Commercial services website (https://www.crowncommercial.gov.uk/agreements/category/document-management-logistics).

11. Electronic Records

11.1 **Filing Structures** – a clear and logical filing structure that aids retrieval of records should be used. Ideally the structure for electronic records should be similar to that of paper records. If it is not possible to do this, the names allocated to files and folders should allow intuitive filing.

11.2 **Filing of primary records** to local drives on PCs, laptops or other mobile device is not permitted. All primary files must be stored on a network drive.

11.3 **Naming conventions** – meaningful folders and file names should be used that best suits operational needs. Each record should:

11.3.1 have a unique name.

11.3.2 have a meaningful name which closely reflects the records contents.

11.3.3 locate the most specific information at the beginning of the name and the most general at the end.

11.3.4 give a similar structure and worded name to records which are linked (for example, an earlier and a later version).

Examples of good practice are available in The National Archives document "Managing Digital Records without an Electronic Record Management System".[7] This document will be available in the Information Governance folder on the intranet.

12.4 Version Control

A system must be developed for file names so that the current version and previous versions can be easily identified.

Examples of good practice are available in The National Archives document "Managing Digital Records without an Electronic Record Management System"[8]. See page 23 of the above-named document.

12.5 **Audit trail** – electronic records should have an integral audit trail recording as a minimum detail of all transactions, e.g. creation, additions, updates, amendments and deletions, which are date and time stamped and record the user ID. Where possible the audit trail

should retain details of records (or parts of) which are viewed.

12. Access Control Management

12.1 Access to confidential records must be controlled so that only those that have legitimate entitlement to access such records can do so. Suitable storage areas will be created so that records, whether physical or electronic, are only accessible and usable by those who are authorised to do so.

12.2 Access to records must be controlled through a variety of security measures, for example, authorised access to storage and filing areas, lockable storage areas, user verification password protection and access monitoring.

7 The National Archives (2010) Managing Digital Records Without an Electronic Record
8 The National Archives (2010) Managing Digital Records Without an Electronic Record Management System

13. Conversion of Paper Records to Electronic Records (Scanning)

13.1 For reasons of business efficiency or in order to address problems with storage space, departments may consider the option of scanning into electronic format records which exist in paper format.

Where this is proposed, the evidential value of the record must be protected in accordance with British Standard 10008, in particular with the checklist for "Legal Admissibility of Electronic Records".

13.2 In the event that scanned records do not meet the British Standard (10008) for "Legal Admissibility of Electronic Records", the original paper records must be retained in accordance with normal retention and disposal schedules, as outlined in section 15 of this policy.

The ICB has commissioned a scanning process for GP records which meets British Standard 10008, provided by Iron Mountain.

Where documents have been scanned and are no longer in active use, consideration should be given to storing the original documents in the ICB's offsite records storage and archiving system. See Sections 15 and 16 of this policy.

14. Classification of Records/Protective Marking

14.1 The ICB will protectively mark confidential or personal identifiable information with the words "**NHS CONFIDENTIAL"** (as described in Section 18 of the Information Security Policy). This protective marking should be extended to commissioning and corporate records, so that all confidential records can be easily and quickly identified thus enabling appropriate security to be applied to them.

14.2 The endorsement **NHS CONFIDENTIAL** should also be used to mark all confidential or sensitive corporate or commissioning information. That is, material the disclosure of which is likely to:

- adversely affect the reputation of the organisation or its officers or cause substantial distress to individuals;

- make it more difficult to maintain the operational effectiveness of the organisation;
- cause financial loss or loss of earning potential, or facilitate improper gain or disadvantage for individuals or organisations;
- prejudice the investigation, or facilitate the commission of crime or other illegal activity;
- breach proper undertakings to maintain the confidence of information provided by third parties or impede the effective development or operation of policies;
- breach statutory restrictions on disclosure of information;
- disadvantage the organisation in commercial or policy negotiations with others or undermine the proper management of the organisation and its operations.

14.3 Examples of other descriptors that may be used with **NHS CONFIDENTIAL** can be found in Appendix 3.

14.4 15.4 Records marked **NHS CONFIDENTIAL** should be held securely at all times. When not in use they should be stored in a locked cabinet or room, or equivalently within secured electronic systems to which only authorised persons have access. They should not be unattended at any time in any place where unauthorised persons might gain access to them.

During transportation they should be in sealed containers and not unattended at any stage.

15. Register of Records and Systems Reviews

15.1 Each Department will establish and maintain a register of the records they are keeping, recorded on the ICB's Information Asset Register. The register will include:

- the type of records currently held
- the format in which the records are held
- the record keeping systems currently in use
- the retention period in accordance with the retention schedules published within the NHS Records Management Code of Practice 2021

15.2 Each Department will review the register annually and assess how effective the record keeping system is and identify and implement any improvements which need to be made.

16. Records no longer required for current business

16.1 When paper (or other hard copy format) records are no longer required for current business, they should be appraised and labelled to indicate:

16.1.1 how long they should be retained for, in accordance with the retention schedules published in the NHS Records Management Code of Practice 2021.

The destruction due date will also be calculated - in accordance with this retention schedule.

16.1.2 whether the records should be destroyed when they reach their minimum retention period and destruction due date.

16.1.3 whether the records need to be retained for a longer period (see paragraph 18.5).

16.1.4 whether they are worthy of archival preservation.

16.2 When paper (or other hard copy format) records are no longer required for current business and they have been appraised in accordance with 17.1, but they have not reached the minimum retention period, they should be archived – either to an on-site storage area or to the ICB's offsite records storage facility.

16.3 The detailed procedure for archiving and recalling records to/from the offsite storage facility will be available in the Information Governance folder of the intranet

17. Retention and Disposal of Records

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

17.2 Before any records are disposed of they must go through an appraisal process as per 17.1 above.

17.3 All ICB records will be retained and disposed of in accordance with the retention schedule as laid out in the NHS Records Management Code of Practice 2021.

Please see Appendix 2, paragraph 26.2 for a hyperlink to the current version of document.

17.4 In the event that a record type is not listed in the Retention and Disposal Schedules, advice should be sought from the Arden & GEM CSU Compliance Manager (Information Governance). Attention should be paid to other retention periods for similar record types. Where necessary, consultation with the National Archives may be required.

The decision regarding retention and disposal of record types not listed in the Retention and Disposal Schedules will be made by the Information Governance Steering Group. A Retention and Disposal Schedule log of such local approvals will be maintained by the ICB and published in the Information Governance folder on the intranet.

17.5 In the event that records need to be kept for longer than the minimum retention period due to ongoing administrative need, this should be referred to the Arden & GEM CSU Compliance Manager (Information Governance) in the first instance and then to the Information Governance Steering Group. If it is approved that the records should be retained for a period longer than the minimum (provided that this does not total a period of 30 years or more from creation), an internal retention schedule will be developed accordingly. (Records may not be retained for more than 30 years without the approval of the National Archives.)

17.6 Records will be destroyed in accordance with the NHS Records Management Code of Practice 2021.

When records in storage are due for destruction, a destruction review report will be produced. Each department must verify that the records listed on this report are actually due for destruction. Records must not be destroyed without such verification.

17.7 A log of all record disposals should be retained within each department.

18. Requests for Access to Personal Information

18.1 Individuals have the right under the Data Protection Act 2018 (DPA 2018) to see, or request a copy of, information that the ICB holds about them. The ICB has a Subject Access Request Procedure which explains the process that data subjects should follow if they wish to obtain this information.

18.2 DPA 2018 only applies to living persons but there are also limited rights of access to personal data of deceased persons under the Access to Health Records Act 1990.

18.3 Requests might come from the Executor or Administrator of a deceased person's estate (the Personal Representative) or any person who might have a claim on the estate.

18.4 The Common Law Duty of Confidentiality extends beyond death and guidance should be sought from the Caldicott Guardian in relation to requests for access to a deceased person's records.

19. Training

19.1 All staff who create or use records should receive local induction training in the records management system being used in the work area.

19.2 Local induction will provide staff with an understanding of:

20.2.1 what should be included in records and how it should be recorded.

20.2.2 how to identify and correct errors.

20.2.3 how records will be used – so that will understand why timeliness, accuracy and completeness are so important).

19.4 If more specific records management training is required, this should be referred to the line manager of the employee.

20. Equality

20.1 The ICB recognises the diversity of the local community and those in their employ. Our aim is therefore to provide a safe environment free from discrimination and a place where all individuals are treated fairly, with dignity and appropriately to their need.

20.2 The ICB recognises that equality impacts on all aspects of their day-to-day operations and have an equality impact assessment tool (EIA) to assess and address any potential or actual adverse effects. This is in respect of local communities and staff we employ. All policies, procedures and functions have a comprehensive impact assessment to determine the level and extent of the potential or actual adverse effects and remedial solutions to them. See Appendix 5.

21. Freedom of Information Act 2000

Any information that belongs to the ICB may be subject to disclosure under the Freedom of Information Act 2000. This allows anyone, anywhere to ask for information held by the ICB to be disclosed (subject to limited exemptions). Further information is available in the Freedom of Information Policy.

22. Policy Review

This policy will be reviewed every three years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation or guidance.

23. Monitoring

The effectiveness of this policy will be monitored by analysis of incident reports and the annual department reviews as outlined in Section 14 of this policy. An audit will be undertaken on an annual basis which reflects the requirements of the NHSD Data Security and Protection Toolkit. Where appropriate, incident reports, departmental reviews and audit results will be reported to the Information Governance Steering Group and then to the Clinical Quality and Governance Committee.

Appendix 1 - Related ICB Policies

- Information Governance Policy
- The Data Protection and Confidentiality Policy
- Information Security Policy
- Information Governance Management Framework
- Subject Access Request Procedure

Most Relevant Legislation

- The Public Records Act 1958
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice
- Any new legislation affecting records management as it arises

Appendix 2 - Most Relevant Standards and Guidelines

- Records Management Code of Practice for Health and Social Care 2021

  https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/

- The National Archives (2010) Managing Digital Records Without an Electronic Record Management System

  http://www.nationalarchives.gov.uk/documents/information-management/managing-electronic-records-without-an-erms-publication-edition.pdf

- Department of Health (2007) Information Security Management: NHS Code of Practice. Gateway Ref: 7974, London: HMSO. Available from:

  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200506/Information_Security_Management_-_NHS_Code_of_Practice.pdf

- Department of Health (2003) Confidentiality: NHS Code of Practice. Gateway Ref: 1656, London: HMSO. Available from:

  https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

Appendix 3 - Classification of Information

Table 1 – Descriptors that may be used with "NHS CONFIDENTIAL"	
Category	**Definition**
Appointments	Concerning actual or potential appointments not yet announced.
Barred	Where • there is a statutory (Act of Parliament or European Law) prohibition on disclosure, or • disclosure would constitute a contempt of Court (information the subject of a court order).
Board	Documents for consideration by an organisation's Board of Directors, initially, in private. (Note: This category is not appropriate to a document that could be categorised in some other way.)
Commercial	Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs.
Contracts	Concerning tenders under consideration and the terms of tenders accepted.
For Publication	Where it is planned that the information in the completed document will be published at a future (even if not yet determined) date.
Management	Concerning policy and planning affecting the interests of groups of staff. (Note: Likely to be exempt only in respect of some health and safety issues.)
Patient Information	Concerning identifiable information about patients
Personal	Concerning matters personal to the sender and/or recipient.
Policy	Issues of approach or direction on which the organisation needs to take a decision (often information that will later be published).
Proceedings	The information is (or may become) the subject of, or concerned in a legal action or investigation.
Staff	Concerning identifiable information about staff

Extract from: **Guidance for the Classification Marking of NHS Information Digital Information Policy, Department of Health, January 2009.[6]**

Appendix 4 – References

1. Public Records Act 1958, section 3(1)-(2)
2. NHS Records Management Code of Practice 2021
3. The National Archives Website: http://www.nationalarchives.gov.uk/
4. The National Archives, Records Management Standard RMS 1.1
5. The National Archives (2010) Managing Digital Records Without an Electronic Record Management System

Appendix 5 – Equality Impact Assessment

Policy	Records Management Policy	**Person completing EIA**	Laura Whiteley, Corporate Governance Manager Victoria Watts, Governance Officer
Date of EIA	21/11/18	**Accountable ICB Lead**	Anita Wilson, Associate Director of Governance and Corporate Affairs

Aim of Work	To set out the ICB approach to the management of records and to provide a framework from which managers can develop departmental procedures to ensure that records are controlled effectively to meet their operational needs, whilst complying with legal obligations.
Who Affected	All creators and users of ICB records

Protected Group	Likely to be a differential impact?	Protected Group	Likely to be a differential impact?
Sex	No	**Age**	No
Race	No	**Gender Reassignment**	No
Disability	Yes	**Marriage and Civil Partnership**	No
Religion / belief	No	**Pregnancy and Maternity**	No
Sexual orientation	No		

Describe any potential or known adverse impacts or barriers for protected/vulnerable groups and what actions will be taken (if any) to mitigate. If there are no known adverse impacts, please explain.

To ensure that individuals with specific disabilities can access the policy and its content, the document will be made available in alternative formats if required.