Records Management Policy

Once printed off, this is an uncontrolled document. Please check the Intranet for the most up to date copy

Version	9
Issue	0
Approved by	Caldicott & Information Governance Committee
Date approved	January 2024
Author	Information Governance Manager
Lead Director	Chief Digital Information Officer acting as Senior Information Risk Owner
Name of Responsible individual/committee	Caldicott & Information Governance committee TPSG
Consultation	Caldicott & Information Governance committee
BHT Document Reference	BHT Pol 125
Department Document Reference	IG0079
Date Issued	February 2024
Review Date	February 2027
Target Audience	All Trust Staff
Location	CAKE Intranet Policies & Staff Guidelines and SOPs, Information Governance and Freedom of Information
Equality Impact Assessment	November 2023

DOCUMENT CONTROL

Approval and Authorisation

Completion of the following detail signifies the review and approval of this document, as minuted in the senior management group meeting shown.

Version	Authorising Group	Approver	Date
5.0	Trust Management Committee	Anne Chilcott	Nov 11
6.0	Executive Management Committee	Lorraine Pask	Jan 2016
6.1	Caldicott and Information Governance Committee	Lorraine Pask	June 2017
7.0	Executive Management Committee		July 2018
8.0	Executive Management Committee		June 2021
8.1	TPSG		Jan 2023

Version	Authorising Group	Approver	Date
9.0	TPSG	Lorraine Pask	Jan 2024

Change History

Version	Status	Reason for change	Author	Date
4.1	Draft	Formal Review – minor changes to references, minor wording changes and new sections 9- Records Management Guidance Documents and 11 – Monitoring of the Policy	Anne Chilcott	Sept 11
5.0	Approved	Caldicott & IG Committee Chaiman's action	Anne Chilcott	Oct 11
5.0	Ratified	Trust Management Committee	Anne Chilcott	Nov 11
5.1	Draft	Informal annual review – New sub section 5.1 Classification marking for NHS Information, added new sub section 4.3, 4.4	Anne Chilcott	Nov 12
5.2	Draft	Formal review - New sub section 7.3 – '20 year rule'	Lorraine Pask	May 2015
	Approved	Caldicott and IG Committee	Lorraine Pask	Sept 2015
6.0	Approved	Trust Policy and Strategy Group Executive Management Committee	Lorraine Pask	Dec 2015 Jan 2016
6.1	Draft	Section 2.1 updated to include BS10008 standard regarding scanning of health records	Lorraine Pask	May 2017
6.1	Approved	Noted at the Caldicott Committee	Lorraine Pask	June 2017
6.2	Draft	Formal review to incorporate requirements from GDPR Added new section 6.2 to 6.7 – responsibilities of individual creating a record	Lorraine Pask	Mar 2018
6.2	Approved	Caldicott and IG Committee		Mar 2018
6.2	Approved	TPSG		July 2018
7.1	Draft	Formal review – web links added under Document References. Reference to EU GDPR changed to UK GDPR following UK's exit from EU	Lorraine Pask	Apr 2021
7.1	Approved	Caldicott and IG Committee and via Chairman's action	Lorraine Pask	Apr 2021
7.1	Approved	TPSG	Lorraine Pask	May 2021
8.1		Added record retention schedule. No changes to the policy. Also change in Lead Director from Finance Director to Chief Digital Information Officer	Lorraine Pask	Nov 2022
		Caldicott and IG Committee	Lorraine Pask	Nov 2022
8.1	Approved	TPSG	Lorraine Pask	Jan 2023

Version	Status	Reason for change	Author	Date
9.0	Draft	Formal review – update of NHSE Records Management Code of Practice details. • Addition of reference to approval from the Secretary of State for Digital, Culture, Media and Sport. Page 18 • Change to retention period for dental records. Page 20 • Addition of summary page • Replacement of reference to IG0092 and IG0093 with IG0128 Record Keeping Guidance for Network Folders	Lorraine Pask	Jan 2024

Document References

Ref #	Document title		
1	Record Management Code of Practice 2021 NHSE Records Management CoP 2023 (buckshealthcare.nhs.uk)		Internet
2	Records Management Guidance		Intranet
3	Health Records Management Policy	MR002	Intranet
4	Records Management Strategy	IG0080	Intranet
5	UK General Data Protection Regulation Guide to the UK General Data Protection Regulation (UK GDPR) | ICO		Internet
6	Freedom of Information Policy	IG0097	Intranet
7	Data Protection Policy	IG0117	Intranet
8	Subject Access Request Policy	IG0104	Intranet
9	IT User Account and Email Usage Policy BHT Pol 055	BHT Pol 055	Intranet
10	Agile working Policy v2.0 BHT-Pol-268-Agile-Working-Policy-v2.0-rvw-08-2025.pdf (buckshealthcare.nhs.uk)	BHT Pol 268	Intranet
11	Record Keeping Guidance for Network Folders	IG0128	Intranet

Contents

List of Acronyms

Acronym	Meaning
FOIA	Freedom of Information Act 2000
DPA	Data Protection Act 2018
NHSE	National Health Service England
RPSI	Re-use of Public Sector Information Regulations 2015
UK GDPR	UK General Data Protection Regulation
POD	Place of deposit
IAO	Information asset owner
IAA	Information Asset Administrator
DSPT	Data Security & Protection Toolkit
IG	Information Governance
ICO	Information Commissioner's Office
NHS BSA	National Health Services Business Services Authority
EPR	Electronic Patient Record
DARS	Data Access Request Service
MHA	Mental Health Act (MHA) 1983 (and 2007 amendments).
GUM	Genito-Urinary Medicine (GUM)
DPIA	Data Protection Impact Assessments (DPIAs)
MHRA	Medicines and Healthcare products Regulatory Agency
ONS	Office for National Statistics
HRA	Health Research Authority
CCG	Clinical Commissioning Group

Summary

The Records Management Policy sets out the organisational records management requirements for the Trust and provides advice and guidance to all colleagues on the creation, management, storing and disposal of records.

Buckinghamshire Healthcare NHS Trust is committed to the efficient management of our records for the effective delivery of our services, to document our principal activities and to maintain and comply with regulatory and legislative requirements. The benefits of effective records management are:

- protecting our business-critical records and improving business resilience
- making sure our information can be found and retrieved quickly and efficiently
- complying with legal and regulatory requirements
- reducing risk for litigation, audit and government investigations
- minimising storage requirements and reducing costs

The principles outlined in this policy have been developed to provide a consistent approach to managing records throughout their lifecycle and regardless of their format.

1. Introduction

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

1.2 As a Public Authority subject to the Freedom of Information Act (FOIA) the Trust has a duty to follow the Code of Practice for Records Management published by the Lord Chancellor in accordance with section 46 of the FOIA. The code provides guidance to public authorities on keeping, managing and destroying records.

The Data Protection Act (DPA) sets in law how personal and sensitive information may be processed and largely influences the way we handle care records. Further guidance on the confidentiality aspects of record keeping is provided in the NHS Confidentiality Code of Practice and the Trust Data Protection Policy.

NHSE Records Management Code of Practice August 2023 provides records management guidance for NHS and Social Care organisations based on current legal requirements and professional best practice. The Trust is committed to following the guidance issued in the code of practice and the procedures outlined in this policy are largely based on the guidance included in this Code of Practice.

1.3 The Trust's records are its 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 Trust and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways. Any information, whatever its medium, is considered public sector information and subject to the Re-use of Public Sector Information Regulations 2015 (RPSI). RPSI does not apply to information that would be exempt from disclosure under information access legislation, i.e., the UK General Data Protection Regulation (UK GDPR), the Freedom of Information Act (FOIA)

1.4 Good records management is a mandatory corporate function, and the Trust is committed to its ongoing improvement. This policy has been adopted by the Trust Board and the organisational benefits from doing so include:

- better use of physical and server space.
- better use of staff time.
- improved control of valuable information resources.
- compliance with legislation and standards; and
- reduced costs.

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

1.6 This policy document should be read in conjunction with the Trust's Records Management Strategy which sets out how the policy requirements will be delivered.

2. Scope and Definitions

2.1 This policy relates to all clinical and non-clinical operational records held in any format by the Trust. These include:

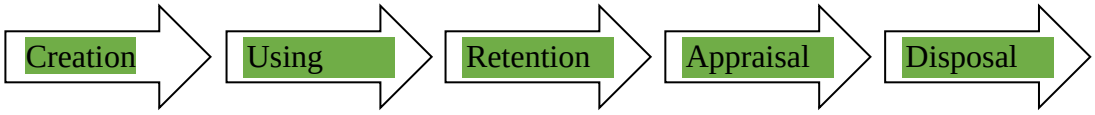
- all corporate/administrative records (e.g., personnel, estates, financial and accounting records, notes associated with complaints, client records, business accounting details and commercial correspondence through to supplier and partner emails)
- all patient health records (for all specialties and including private patients, including x-ray and imaging reports, emails, computerised records, microfiche, scanned records, text messages, registers, etc.)

This policy is mandatory and applies to all information in all formats. Staff must not alter, deface, block, erase, destroy or conceal records with the intention of preventing disclosure under a request relating to the Freedom of Information Act 2000 or the UK GDPR and Data Protection Act 2018.

2.2 ***Records Management*** is a discipline which utilises an administrative system to direct and control the creation, version control, access, 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 Trust and preserving an appropriate historical record. The key components of records management are:

- record creation: this must be achieved in a standard, consistent way of applying templates to common sets of records,
- record keeping;
- record maintenance (including tracking of record movements);
- access and disclosure;
- closure and transfer;
- retention
- appraisal;
- archiving; and
- disposal.

2.3 The term ***Records Life Cycle*** 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.



Stage 1: Creation
This part of the life cycle is when we put pen to paper, make an entry into a database or start a new electronic document. It is known as the first phase. It can be created by internal employees or received from an external source, and it is complete and accurate.

Stage 2: Using
This stage takes place after information is distributed. This is when records are used on a day-to-day basis to help generate organisational decisions, document further action or support other Trust operations. It is also considered the Active Phase

Stage 3: Retention
Retention is when records are not used on a day-to-day basis and are stored in the Records Management system. Even though they are not used on a day-to-day basis, they will be kept for legal or financial reasons until they have met their retention period. The retention phase includes filing, transfers and retrievals. The information may be retrieved during this period to be used as a resource for reference or to aid in a business decision. Records should not be removed from a records management system; the information should be copied and tracked to ensure no amendments were made.

Stage 4: Appraisal
The appraisal stage is when a record has reached the end of its assigned retention period. It is then reviewed and if appropriate destroyed under confidential destruction conditions. Not all records will be destroyed once the retention period has been met. Any records that have historical value should be considered for removal to the designated Place of Deposit (POD). For details of the agreed Place of Deposit, or further guidance if you are unsure whether your records have historical value can be sought from the Corporate Records Management Team.

Stage 5: Disposal
The disposal stage is when the appraisal phase has been completed and a documented agreement has been made that records can be confidentially destroyed. For medical records, this should be done in collaboration with the Head of Medical Records. For all records, the appraisal and destruction process should be recorded on a departmental records inventory and if applicable a destruction certificate produced to ensure there is a record of which documents have been sent for destruction.

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

2.5 ***Information*** is a corporate asset. The Trust's records are important sources of administrative, evidential, and historical information. They are vital to the Trust to support its current and future operations (including meeting the requirements of Freedom of Information legislation and Re-use of Public Sector Information Regulations 2015), for the purpose of accountability, and for an awareness and understanding of its history and procedures.

3. Aims of our Records Management System

3.1 The aims of our Records Management System are to ensure that:

- **records are available when needed** - from which the Trust 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 - history** - the history of the record can be understood: who created or added to the record and when, during which business process, and how the record is related to other records;

- **records tracking** – systems are to be put in place to enable tracking and location of records;

- **records can be trusted** – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated;

- **records can be maintained through time** – 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, access and disclosure are properly controlled, and audit trails will track all use and changes. Records are held in a robust format which remains readable for as long as records are required;

- **records are retained and disposed of appropriately** - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value; and

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

4. Roles and Responsibilities

Trust Board

The Trust Board is ultimately responsible for ensuring that the Trust corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements. Included within its responsibilities to maintain minimum standards of information governance is a responsibility for ensuring the quality of record keeping and record management in the Trust.

Chief Executive

4.1 The Chief Executive has overall responsibility for records management in the Trust. As accountable officer he/she is responsible for the management of the organisation and 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 as required.

4.2 The Trust has a responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance requirements.

4.3 **Director for Records Management**

The Senior Information Risk Owner is the Director for Records Management and has key individual empowerment to make operational decisions with clear responsibility for the management of all categories of records within the organisation, and corporate responsibility at a senior management level to the

Trust Board for records management. The day-to-day management of records is devolved to Information Asset Owners (IAO) and local records managers.

4.4 **Information Asset Owners (IAO)**

The IAO is a nominated senior member of staff who has the responsibility and accountability for records management within his/her operational area and will provide an essential supporting role to the Senior Information Risk Owner. The IAO will oversee the records management function and delegate responsibility to appropriate individuals, adopt policies and procedures to guide personnel and ensure auditability.

4.5 **Executive Management Committee**

The Executive Management Committee is responsible for ensuring that this policy is implemented, through the Records Management Strategy, and that the records management system and processes are developed, co-ordinated, audited and monitored. Coordination of this work is the responsibility of the Senior Information Risk Owner.

4.6 **Head of Medical Records**

The Head of Medical Records is responsible for the overall development and maintenance of health records management practices throughout the Trust, in particular for drawing up guidance for good records management practice and promoting compliance with this policy in such a way as to ensure the easy, appropriate, and timely retrieval of patient information.

4.7 **Local record managers**

The responsibility for local records management is devolved to the relevant directors, directorate managers and department managers. Heads of Departments, other units and business functions within the Trust have overall responsibility for the management of records generated by their activities, i.e., for ensuring that records controlled within their unit are managed in a way which meets the aims of the Trust's records management policies.

Senior Information Asset Owners are responsible for identifying local record managers within their areas of responsibility.

4.8 **All Staff**

All Trust staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular all staff must ensure that they keep appropriate records of their work in the Trust and manage those records in keeping with this policy and with any guidance subsequently produced.

5. Legal and Professional Obligations

All NHS records are Public Records under the Public Records Acts. The Trust will take actions as necessary to comply with the legal and professional obligations set out in the NHSE Records Management Code of Practice August 2023, in particular:

- The Public Records Act 1958
- The Data Protection Act 2018
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality; and
- The NHS Confidentiality Code of Practice

- Information Security Management NHS Code of Practice
- Copyright, Designs and Patent Act 1988
- Re-use of Public Sector Information Regulations 2015
- UK General Data Protection Regulation

And any new legislation affecting records management as it arises.

Failure to comply with the regulations could result in reputational damage to the Trust and carries substantial financial penalties imposed by the Information Commissioner. This policy applies to all employees and must be strictly observed.

6. Registration of Record Collections

6.1 Senior Information Asset Owners or their designated deputies are to establish and maintain mechanisms through which departments can identify the records they are maintaining. This should be achieved through registers and an inventory of record collections which will facilitate:

- the classification of records into series; and
- the recording of the responsibility of individuals creating records.

The register should be regularly reviewed.

6.2 Version Control

Document version control allows the management of multiple revisions to the same document and is important as it enables users to distinguish between different versions of a document and to identify if the document they are using is the latest version. When creating a document where more than one version does, or is likely to exist, a unique version number should be included in the document name and clearly displayed in the document. Consecutive whole numbers should be used to identify major revisions to documents. i.e., version 1, version 2 etc. The addition of the word Draft or Final at the end of the file name can be used to indicate the status of the document:

e.g. ……Record v1.0 Draft First draft version
……Record v1.1 Draft Second draft version
……Record v2.0 Final Third and final version

In key documents (policies, strategies etc) it is useful to display after the title page a version control table showing the development history of the document and the version changes that have been applied.

6.3 Record Confidentiality and Access

All NHS records are public records and thus are subject to a number of statutory provisions regarding confidentiality, access, and disclosure. Patients entrust the NHS or allow it to gather sensitive information relating to their health and other matters as part of their seeking treatment. They do so in confidence, and they have the legitimate expectation that staff will respect this trust. It is essential, if the legal requirements are to be met and the trust of patients is to be retained, that the NHS provides, and is seen to provide, confidential service.

Specific guidance on patient confidentiality issues is given in the Department of Health and Social Care publication Confidentiality: NHS Code of Practice.

The Trust's Health Records Management Policy is built on the guidance contained within this overarching Records Management policy. The policy defines a structure and clinical records management guidance to promote and maintain effectively a consistent and standardised practice throughout the Trust.

The Data Protection Act 2018 and UK GDPR also make provision in law for patients to obtain copies or otherwise gain access to their health records. The Trust Subject Access Request policy covers this aspect of records management and advice on the procedure can be obtained from the Trust Medical Records department.

In 2000 the government introduced the Freedom of information Act providing members of the public with the general right of access to recorded information held by a wide range of bodies across the public sector. The effect of this legislation is to make it possible for people to obtain copies of a wide range of Trust records that in the past would have remained confidential. Staff need to be aware that the records they keep may well be released to the public at a future date and the increased importance of adhering to the guidance provided in the Trust Freedom of Information Policy.

6.4 **Non-Paper Records**

Increasingly our records are being created and recorded electronically and held in a digital format. The principles of sound record management apply equally to electronic records as they do to traditional paper records. Electronic records should be organised into secure filing systems and maintained, reviewed, and archived or disposed of in line with the guidance in this document. When considering the use of alternative storage media, maintenance in the form of back up and planned migration to new platforms should be considered and discussed with the IT Department, and subsequently designed and scheduled to ensure continuing access to readable information.

In many cases copies of documents are distributed electronically and the original held in paper form. This often leads to duplicate records being unnecessarily retained, sometimes for periods beyond the recommended minimum retention period. This is particularly prevalent on file servers shared by several people/departments. Responsibility for the maintenance of such filing systems should be clearly defined and if appropriate restrictions placed on the ability to create new record folders.

E-mail has become a primary communication tool increasingly replacing letters and memoranda as a means of communicating and distributing information. The Trust has a separate policy on e-mail security and storage which users should be familiar with. IT User Account and Email Usage Policy BHT Pol 055

E-mail accounts should not be used to file records on a permanent basis but should be regarded as transient storage areas for working documents. Important e-mails or documents distributed by e-mail that need to be retained should be copied to the appropriate paper or electronic network file system and the e-mail copy destroyed as soon as practicable.

The increasing use of e-mail for personal communication can lead to business e-mails containing opinion and comment that may be inappropriate and would

not have been included in more formal documents. Users should be aware that, if relevant, copies of e-mails held in the Trust will be released to requesters under the provisions of the Freedom of Information Act.

6.5 **Record Maintenance, Access and Disclosure**

All staff should ensure that Trust records are managed and maintained responsibly and respectfully, kept up to date and stored safely. The movement and location of paper records should be controlled to ensure that a record can be easily retrieved at any time.

There are a range of statutory provisions that give individuals the right of access to information created or held by the trust such as Subject Access requests and Freedom of Information requests. In addition, under the new data protection legislation, individuals are given enhanced information rights e.g. the right to rectification, right to erasure, right to restrict processing, right to data portability, right to object, and rights in relation to automated decision making and profiling. Good record management will enable the Trust to process and respond to information requests in a timely manner.

There are a range of statutory provisions that limit, prohibit or set conditions in respect of the disclosure of records to third parties and similarly a range of provisions that require or permit disclosure.

.

6.6 **Storage of Records**

When not required for operational purposes, records should be kept in a secure storage area. Records in current use should ideally be stored close to the point of use while records no longer in current use can be transferred to secondary or archive storage more remote from the operational area.

Records should be stored in an appropriate environment to ensure they remain fit for purpose during their expected period of retention. When evaluating the suitability of a location for record storage the following points should be considered:

Environment. Is the location suitable for the type of material being stored? Is the area free from hazards that may cause the records to deteriorate or place at risk staff that may need to access the records? i.e., excessive dust, damp, restricted access.

Security. Is the level of security offered by the location acceptable for the type of record being stored?

Ease of Access. Can records be easily located and retrieved? Some restrictions on access may be acceptable for records that are not frequently recalled.

Layout. Consideration should be given to the design of the storage location to ensure the most cost-effective use is made of the space available.

A comprehensive record should be maintained of any records sent for commercial storage including a proposed date for review/destruction. A mechanism for reviewing these records for disposal should be developed and implemented to ensure records are not retained longer than necessary.

6.7 **Appraisal of Records**

The process of deciding what to do with records when their business use has ceased is called appraisal.

There will be one of three outcomes from appraisal:

- Destroy/delete
- To keep for a longer period
- To transfer to a place of deposit

Staff in the operational area that ordinarily uses the records will usually be able to decide whether to destroy or keep for a longer period. Operational managers are responsible for making sure that all records are periodically and routinely reviewed to determine what can be disposed of or destroyed in the light of local and national guidance.

7. Retention, Transfer and Disposal Schedules

7.1 It is a fundamental requirement that all the Trust'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 Trust's business functions.

7.2 The Trust has adopted the retention periods set out in the NHSE Records Management Code of Practice August 2023 which is available on the Internet (see Document Reference, Ref 1). It contains a comprehensive list of NHS clinical and corporate records and for each type of record sets out a recommended minimum period of retention along with advice on final disposal.

7.3 Place of Deposit - 20 year rule – As required by the Public Records Act 1958, and following implementation of the Constitutional Reform and Governance Act 2010, in particular Part 6: Public Records and Freedom of Information, central government departments and certain other public bodies including NHS, need to identify non-active records of historical value and transfer them for permanent preservation to National Archives or to another appointed Place of Deposit (PoD) by the time they are 20 years old. This rule applies to NHS also but is applicable only to 'corporate records' – records (other than health records) that are of or relate to an organisation's business activities covering all the functions, processes, activities, and transactions of the organisation and of its employees.

Records must be selected in accordance with the guidance contained within the NHSE Records Management Code of Practice August 2023and any supplementary guidance issued by the National Archives or local guidance from the relevant PoD. A documented list of any records being transferred to a PoD must be kept and a copy sent to the Information Governance department.

Once the appropriate minimum period has expired, the need to retain records further for local use should be reviewed periodically. Because of the sensitive and confidential nature of such records and the need to ensure that decisions on retention balance the interests of professional staff, including any research in which they are or may be engaged, and the resources available for storage, it is recommended that the views of the professional staff should be sought.

The overall responsibility for managing the process for the retention, disposal and destruction of patient health records lies with the Trust Clinical Records Manager. For further details please contact the Medical Records Department.

Records should not be kept longer than is necessary and should be disposed of at the right time. Unnecessary retention of records not only consumes time, space and equipment use but may also incur liabilities in respect of the Freedom of Information Act 2000 and the Data Protection Law, as we would be liable to disclose it upon request.

8. Records Management Systems Audit

8.1 The Trust will audit its records management practices for compliance with this framework.

8.2 The audit will:

- Identify areas of operational or information management /security risk
- Highlight where non-conformance to the procedures is occurring to enable tightening of controls and adjustment to related procedures.

8.3 The results of audits will be reported to the Caldicott & Information Governance and Committee.

9. Records Management Guidance Documents

The Trust has provided a number of guidance documents for staff in order to assist in day-to-day records management duties:

- Records Management Guidance ref [2]
- MR002 Health Records Management Policy ref [6]
- IG0080 Records Management Strategy ref [7]

10. Training

10.1 All Trust staff will be made aware of their responsibilities for record-keeping and record management through generic and specific statutory and mandatory training programmes and guidance. This policy is socialised to all colleagues via the Trust intranet and by way of regular reminders and reference on BHT Today bulletins and Information Governance newsletters.

11. Monitoring

Minimum requirement to be monitored	Process for monitoring e.g. audit	Responsible individual to undertake monitoring and production of a report	Frequency of monitoring/ auditing	Responsible individuals receiving the monitoring report and for development of action plan	Responsible committee for review of action plan	Responsible committee for monitoring of action and audit to ensure satisfactory conclusion

Ensuring that Trust records are managed, stored, archived and destroyed in line with the Records Management NHS Code of Practice	Data Security and Protection Toolkit (DSPT) expected standards Information Commissioner's Office guidance	Information Asset Owners (IAO) or Information Asset Administrators	Annually	Senior Information Risk Owner	Caldicott and IG Committee	Caldicott and IG Committee
A continual, systematic approach to responding to Subject Access, FOI requests and the Trust Publication Scheme in line with the DSP standards Process for managing records audits and the production of a Trust wide Information Asset Register and Publication Scheme	DSPT expected standards Report to Caldicott and IG Committee DSP Toolkit Compliance audit by IG Team	Information Asset Owners or Information Asset Administrators Senior Information Risk Owner and Information Asset Owners	Annually Quarterly Annually Quarterly	Divisional Head/IAO IAO	Caldicott and IG Committee Caldicott and IG Committee	EMC Caldicott and IG Committee EMC Caldicott and IG Committee

12. Review

12.1 This document should be subject to review when any of the following conditions are met:

a. The adoption of the Code of Conduct highlights errors and omissions in its content
b. Where other standards/guidance issued by the Trust or Government legislation conflict with the information contained
c. Where the knowledgebase regarding interpretation of the legislation evolves to the extent that revision would bring about improvement
d. Three years from the date of approval of the current version

Appendix 1

RECORD MANAGEMENT CODE OF PRACTICE
RETENTION AND DISPOSAL SCHEDULE

All health and care employees are responsible for managing records appropriately. Records must be managed in accordance with the law (see legal obligations).

This document is a guide for you to use in relation to the practice of managing records. It is relevant to organisations working within, or under contract to, the NHS in England. It provides a framework for consistent and effective records management based on established standards. It applies to all records regardless of the media they are held on.

LEGAL OBLIGATIONS

Public Records Act 1958
The Public Records Act 1958 is the principal legislation relating to public records. Records of NHS organisations are public records in accordance with Schedule 1 of the Act. This means that employees are responsible for any records that they create or use in the course of their duties. This includes records controlled by NHS organisations under contractual or other joint arrangements, or as inherited legacy records of defunct NHS organisations. The Act applies regardless of the format of the records. The Secretary of State for Health and Social Care and all NHS organisations have a duty under the Act to make arrangements for the safekeeping and eventual disposal of all types of records.

Freedom of Information Act 2000
The Freedom of Information Act (FOIA) governs access to and management of non-personal public records. The FOIA was designed to create transparency in government and allow any citizen to know about the provision of public services through the right to submit a request for information. This right is only as good as the ability of those organisations to supply information through good records management programmes. Records managers should adhere to the code of practice on record keeping issued by the Secretary of State for Culture, Media and Sport, under section 46 of the FOIA. The section 46 Code of Practice is used as a statutory statement of good practice by the regulator and the courts.

UK GDPR and Data Protection Act 2018
The UK GDPR is the principal legislation governing how records, information and personal data are managed. It sets in law how personal and special categories of information may be processed. The Data Protection Act 2018 principles are also relevant to the management of records. Under the UK GDPR, organisations may be required to undertake Data Protection Impact Assessments (DPIA) as set out in Section 3 of the Records Management Code. The UK GDPR also introduces a principle of accountability. The Information Commissioner's Office (ICO) Accountability Framework can support organisations with their obligations. Good records management will help organisations to demonstrate compliance with this principle.

Health and Social Care Act 2008
Regulation 17 under the Health and Social Care Act 2008 requires that health and care providers must securely maintain accurate, complete and detailed records for patients or service users, employment of staff and overall management. The CQC are responsible for regulating this and have issued guidance on regulation 17. The CQC may have regard to the Code when assessing providers' compliance with this regulation.

Other relevant legislation
Other legislation requires information to be held as proof of an activity against the eventuality of a claim. Examples of legislation include the Limitation Act 1980 or the Consumer Protection Act 1987. The Limitation Act sets out the length of time you can bring a legal case after an event and sets it at six years.

Caldicott principles
The Caldicott principles outline eight areas that all health and social care staff are expected to adhere to in addition to the UK GDPR.

MANAGEMENT OF RECORDS WHEN THE MINIMUM RETENTION PERIOD IS REACHED

The retention periods listed in this retention schedule must always be considered the minimum period.

Appraisal
Appraisal is the process of deciding what to do with records once their business need has ceased and the minimum retention period has been reached. This can also be known as the disposition of records. The National Archives has produced guidance on appraisal.
Selecting and transferring paper records - The National Archives

When appraising records that have come to the end of their minimum retention period, you should consider the following:
• **Ongoing use**: You might need to keep the record for longer than the minimum period for care, legal or audit reasons. In these cases, you can set an extension to the minimum period, provided it is justified and approved.
• **Classification of diseases (based on ICD10 code):** Some health conditions may lend themselves towards a longer, or extended, retention period.
• **Operational delivery**: The way a service was delivered may have been pioneering or innovative at the time, which may justify an extended retention period or long-term archival preservation.
• **The way care is delivered:** The records may be reflective of health or care policy at the time.
• **Series growth**: If the records are part of a series that will be added to (type of record rather than additional content into existing records), you need to consider space issues in your local records store or organisation archive. For example, continued expansion of a series that is hardly recalled would not justify an extension to the retention period.
• **Recall rates:** If a series of records is routinely accessed to retrieve records, then there may be justification for extending the retention period due to ongoing use. Whereas, for a series of records that has a very low recall rate, continued retention may be harder to justify.
• **Historical value**: If the record has potential historical or social value (for example, innovative new service or treatment or care delivery method), then consider retaining for longer. It would also be helpful to have early discussions with your local Place of Deposit (PoD) about potential accession, even if the record has ceased to be of operational value or use. PoDs will not normally accession records before 20 years retention has passed, unless there are exceptional circumstances for early transfer. The PoD must agree to the transfer PRIOR to it occurring. If early discussion with the PoD indicates the record (or series) will not be accessioned, and you have no ongoing operational use for the record or series, then you must securely destroy the record, and obtain evidence of destruction (for example, destruction certificate).

• **Previous deposits**: The records you hold may be a continuation of a series that has historically been accessioned by a local PoD. It is important to find out what has historically been accessioned from your organisation to the PoD, so that a series of records remains complete. It is likely that records that add to an already accessioned series will continue to be taken by the PoD.

(This list is not exhaustive, and organisations may have bespoke issues to consider as well).

Other types of records

For records that are not staff or patient records, for example, board minutes, a different arrangement is in place. Where an organisation needs to keep any other type of record beyond 20 years, then approval must be sought separately from the Secretary of State for Digital, Culture, Media and Sport. This is the case even where the recommended retention period is longer in the NHSE Records Management Code of Practice.

The only exceptions to this are records which mainly relate to information on (i) controlling asbestos including air monitoring records and (ii) ionising radiation including radioactive waste records. These types of records can be kept for the minimum retention period set out in the schedule below 1 without needing approval. Any required applications for approval should be made via the Executive Office or Information Governance Team, who will contact The National Archives in the first instance (asd@nationalarchives.gov.uk)).

DESTROYING AND DELETING RECORDS

If as a result of appraisal, a decision is made to destroy or delete a record, there must be evidence of the decision. It is good practice to get authorisation for destruction or deletion from an appointed committee or group with a designated function to appraise records, working to a policy or guidelines. Where the destruction or deletion process is new, or there is a change in the destruction process (such as a change of provider, or the method used), a Data Protection Impact Assessment (DPIA) must be completed and signed off by the organisation.

RECORDS FOR PERMANENT PRESERVATION

The Public Records Act 1958 requires organisations to select records for permanent preservation. Selection for transfer under this Act is separate to the operational review of records to support current service provision. It is designed to ensure the permanent preservation of a small core (typically 2-5%) of key records, which will:

• enable the public to understand the working of the organisation and its impact on the population it serves
• preserve information and evidence likely to have long-term research or archival value

Records for preservation must be selected in accordance with the guidance contained in this Code. Any supplementary guidance issued by The National Archives and local guidance from the relevant PoD should always be consulted in advance of any possible accession. This is to ensure it is appropriate to transfer the records selected. As a rule, national organisations, such as NHS England, will accession their records to The National Archives, and local NHS and social care organisations will accession their records to the local PoD (this could be the county record office, or a specialised facility run by local authorities for the county) as appointed by the Secretary of State for Culture, Media and Sport.

There will be a mandatory requirement to transfer some types of records whereas others will be subject to local agreement. The retention schedule included with this Code identifies records which should be transferred to the locally approved PoD when business use has ceased. There may also be records of local interest which need to be accessioned to the PoD (such as a continuation of a series already accessioned). Prior to any transfer being made, a discussion must be had with the local PoD to enable agreement on which records will be transferred and the process for doing so.

Transferred records should be in good condition and appropriately packed, listed and reviewed for any FOIA exemptions. Records selected for transfer to a PoD (after appraisal) may continue to be exempt from public access for a specified period after transfer in accordance with Section 66 of FOIA.

The selection and transfer must take place at or before records are 20 years old. (For more detail on the transfer process and sensitivity review refer to The National Archives guidance).

CONDUCTING A DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Under UK GDPR, organisations are required to conduct Data Protection Impact Assessments (DPIAs) where there is a new or change in use of personal data and a potentially high risk to privacy. Some uses require a mandatory DPIA (where processing is large scale or introduces new technologies). If you are looking to establish a new records management function, then it will be vitally important to complete a DPIA. This will highlight potential risks to privacy and data protection, allowing you to action, mitigate or eliminate that risk. This must be conducted prior to any processing being carried out. When you are looking to amend a record's function, you should check with the person responsible for records management first, for example, your record manager or your data protection officer. DPIA completion in this circumstance will depend on the amendments you are looking to make. For example, if you intend to add three racking shelves for paper HR files to the existing twenty shelves you would probably not complete a DPIA. If you were looking to send your records offsite for scanning or destruction you must complete a DPIA, as this is a new process, and the risk is greater.

A DPIA template can be found on the Trust's intranet - Data Protection Impact Assessment Template - Buckinghamshire Healthcare Intranet (buckshealthcare.nhs.uk)

Schedule 1
Clinical Records

Record Type	Retention Period	Notes	Disposal Action
Adult health records	8 years	Records involving pioneering or innovative treatment may have archival value and their long term should be discussed with the local PoD or the National Archive preservation	Review and consider transfer to PoD
Adult social care records (including care plans)	8 years	Review	Review and destroy if no longer required
Children's records (including midwifery, health visiting, school nursing and dental) – can include medical illustrations, video and audio formats	Up to 25th or 26th birthday	Retain until 25th birthday, or 26th if the patient was 17 when treatment ended	Review and destroy if no longer required
Clinical records that pre-dates the NHS (July 1948)		Contact your local PoD to arrange review and transfer. Records not selected by the PoD must be securely destroyed	Review and transfer to PoD as
Dental records - clinical care records	11 years	Based on Limitations Act 1980. This applies to all dental care settings and the BSA. This also includes FP17 or FP17O forms.	Review, and destroy if no longer required
Dental records - finance related	2 years	These include PR forms. NHS BSA may retain financial records for a minimum of 6 years.	Review, and destroy if no longer required
Electronic Patient Record Systems (EPR)		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.	Review and destroy if no longer required
Integrated records – all organisations contribute to the same single instance of the record	Retain for period of longest specialty	The retention time will vary depending upon which type of health and care settings have contributed to the record. Areas that use this model must have a way of identifying the longest retention period applicable to the record.	Review and consider transfer to PoD
Integrated records – all organisations contribute to the same record, but keep a level of separation (refer to notes)	Retain for relevant specialty period	This is where all organisations contribute into the same record system but have their own area to contribute to and the system still shows a contemporaneous view of the patient record.	Review and consider transfer to PoD
Integrated records – all organisations keep their own records, but enable them to be viewed by other organisations	Retain for relevant specialty period	This is the most likely model currently in use. Organisations keep their own records on their patients or service users but can grant 'view only' access to other organisations, to help them provide health and care to patients or service users.	Review and consider transfer to PoD
Mental health records including psychology records	20 years, or 10 years after death	Covers records made under the Mental Health Act (MHA) 1983 (and 2007 amendments). Records retained solely for any person who has been sectioned under MHA1983 must be considered for longer than 20 years where the case is ongoing, or the potential for recurrence is high (based on local clinical judgment). This applies to records of patients or service users, regardless of whether they have capacity or not.	Review and consider transfer to PoD
Obstetrics, maternity, antenatal and postnatal records	25 years	For record keeping purposes, these are considered to be as much the child's record as the parent, so the longer retention period should be considered.	Review and destroy if no longer required
Prison health records	10 years	A summary of their prison healthcare is sent to the person's new GP upon release and the record should be considered closed at the point of release. These records are unlikely to have long term archival value and should be retained by the organisations providing care in the prison, or successor organisations if the running of the service changes hands.	Review and destroy if no longer required
Cancer/oncology records –	30 years, or	Retention for these records begins at diagnosis rather than the end	Review and

Record Type	Retention Period	Notes	Disposal Action
any patient	8 years after death	of operational use. For clinical care reasons, these records must be retained longer in case of re-occurrence. Where the oncology record is part of the main records, then the entire record must be retained.	consider transfer to PoD
Contraception, sexual health, family planning, Genito-Urinary Medicine (GUM)	8 or 10 years	8 years for the basic retention requirement but this is increased to 10 in cases of implants or medical devices. If the record relates to a child, then retain in line with children's records. (Also refer to Appendix III: records dealt with under the NHS Trusts and Primary Care Trusts (Sexually transmitted disease) directions 2000).	Review and destroy if no longer required
Creutzfeldt-Jakob Disease – patient records	30 years or 10 years after death	Diagnosis records must be retained for clinical care purposes.	Review and consider transfer to PoD
Human Fertility and Embryology Authority (HFEA) records – treatment provided in licenced centres	3,10, 30 or 50 years	These retention periods are set out in HFEA guidance.	Review and destroy if no longer required
Long-term illness, or illness that may reoccur – patient records	20 years, or 10 years after death	Necessary for continuation of clinical care. The primary record of the illness and course of treatment must be kept where the illness may reoccur or it is a lifelong condition such as diabetes, arthritis or Chronic Obstructive Pulmonary Disease.	Review and destroy if no longer required
Sexual Assault Referral Centres (SARC)	30 years, or 10 years after death (if known)	These records need to be kept for medicolegal reasons because an individual may not be in a position to bring a case against the alleged perpetrator for a long time after the event. Once the retention period is reached, a decision needs to be made about continued retention. Records cannot be kept indefinitely just in case an individual might bring a case. Some individuals may never bring a case and indefinite retention may be seen as a breach of UK GDPR (keeping information longer than necessary). Consideration also needs to be given to the Police and Criminal Evidence Act 1984, Human Tissue Act 2004, and Criminal Procedure and Investigations Act 1996 legal requirements (other laws and regulations may also need to be taken into account).	Review and destroy if no longer required
Controlled drugs - registers	2 years	Misuse of Drugs Act 2001. NHS England has issued guidance in relation to controlled drugs.	Review and destroy If no longer required
Controlled drugs - order books, requisitions etc	2 years	Misuse of Drug Act 2001	Review and destroy If no longer required
Pharmacy prescription records	2 years	A record of the prescription will also be held by NHS BSA and there will be an entry on the patient record. Further advice and guidance on pharmacy records can be found on the Specialist Pharmacy Service website.	Review and destroy If no longer required
Pathology reports, Information about samples		This Code is concerned with the information about a specimen or sample. The length of time clinical material (for example, a specimen) is stored will drive how long the information relating to it is retained. Sample retention can be for as long as there is a clinical need to hold it. Reports should be stored on the patient file. It is common for pathologists to hold duplicate records. For clinical purposes, these should be retained for eight years after discharge or until a child's 25th birthday. If information is retained for 20 years, it must be appraised for historical value, and a decision made about its disposal.	Review and consider transfer to PoD
Blood bank register*	30 years minimum	Need to be disposed of if there is no on-going need to retain them (such as the currently ongoing Infected Blood Inquiry), subject to any transfer to the PoD.	Review and consider transfer to PoD
Clinical audit*	5 years	Five years from the year in which the audit was conducted. This includes the reports and data collection sheets/exercise. The data itself will usually be clinical so should be kept for the appropriate retention period, for example, data from adult health records would be kept for 8 years.	Review and destroy if no longer required
Chaplaincy records	2 years	Also refer to corporate governance records.	Review and consider transfer to PoD
Clinical diaries	2 years	Two years after the year to which they relate. Diaries of clinical activity and visits must be written up and transferred to the main patient record. If the information is not transferred from the diary (so	Review and destroy if no longer

Record Type	Retention Period	Notes	Disposal Action
		the only record of the event is in the diary), then this must be retained for eight years and reviewed. Some staff keep hardback diaries of their appointments or business meetings. If these contain no personal data, they can be disposed of after two years.	required
Clinical protocols	20 years	Clinical protocols may have preservational value. They may also be routinely captured in clinical governance meetings which may form part of the permanent record (refer to corporate governance records).	Review and consider transfer to PoD
Datasets released by NHS Digital and its predecessors	Delete with immediate effect	NHS Digital issue guidance through the Data Access Request Service (DARS) process on the retention and disposal of data released by them.	Delete in line with NHS Digital instructions
Destruction certificates, or electronic metadata destruction stub, or record of clinical information held on physical media	20 years	Destruction certificates created by public bodies are not covered by a retention instrument (if they do not relate to patient care and if a PoD or The National Archives do not accession them). They need to be destroyed after 20 years.	Review and consider transfer to PoD
Equipment maintenance log	11 years		Review and destroy if no longer required
General ophthalmic services – patient records related to NHS financial transactions	6 years		Review and destroy if no longer required
Inspection of equipment records	11 years		Review and destroy if no longer required
Notifiable diseases book	6 years		Review and destroy if no longer required
Operating theatre records	10 years	10 years from the end of the year to which they relate.	Review and consider transfer to PoD
Patient property books	2 years	Two years from the end of the year to which they relate.	Review and destroy if no longer required
Referrals – NOT ACCEPTED	2 years	Retention period begins from the DATE OF REJECTION. These are seen as an ephemeral record.	Review and destroy if no longer required
Requests for care funding – NOT ACCEPTED	2 years	Retention period begins from the DATE OF REJECTION. These are seen as an ephemeral record. NB: These may have potential PoD interest as what the NHS or social care can or cannot fund can sometimes be an issue of local or national significance and public debate.	Review and destroy if no longer required
Screening* – including cervical Screening – where no cancer or illness detected is returned	10 years	Where cancer is detected, refer to the cancer/oncology schedule.	Review and destroy if no longer required
Screening-children	10 years or 25th birthday	Treat as a child health record and retain for either 10 years or up to 25th birthday, whichever is the LONGER.	Review and destroy if no longer required
Smoking cessation	2 years	Retention begins at the end of the 12 week quit period.	Review and destroy if no longer required
Transplantation records	30 years	Refer to guidance issued by the Human Tissue Authority	Review and consider transfer to PoD
Ward handover sheets	2 years	This information relates to the ward. Any individual sheets held by staff may be destroyed confidentially at the end of the shift.	Review and destroy if no longer required
Recorded conversations – which may be needed later	6 years	Retention period runs from the date of the call and is intended to cover the Limitation Act 1980.	Review and destroy

Record Type	Retention Period	Notes	Disposal Action
for clinical negligence or other legal purposes*		Further guidance is issued by NHS Resolution.	if no longer required
Recorded conversations – which form part of the health record	Treat as a health record	It is advisable to transfer any relevant information into the main record, through transcription or summarisation. Call handlers may perform this task as part of the call. Where it is not possible to transfer clinical information from the recording to the record, the recording must be considered as part of the record and be retained accordingly.	Review and destroy if no longer required
Telephony systems record*	1 year	This is the minimum specified to meet NHS contractual requirements.	Review and destroy if no longer required
Birth notification to child health	25 years	Retention begins when the notification is received by the child health department. Treat as part of the child's health record if not already stored within the health record.	Review and destroy if no longer required
Birth registers	2 years	Where registers of all births that have taken place in a particular hospital or birth centre exist, these will have archival value and should be retained for 25 years and offered to the local PoD at the end of the retention period. Information is also held by the NHS Birth Notification Service electronic system, and by ONS. Other information about a birth must be recorded in the care record.	Review and consider transfer to PoD
Body release forms*	2 years		Review and destroy if no longer required
Death – cause of death Certificate counterfoil	2 years	These detail the name of the deceased and suspected cause of death (which initially may be different to the final cause of death as stated on the official death certificate). A death notification certificate is issued if a doctor is satisfied there is no suspicious or unexpected circumstances surrounding the death, and the counterfoil retained by the setting that issued the initial cause of death certificate (which is used to obtain the full death certificate from a registrar of births, death and marriages). Cases referred to the coroner would not be able to issue a certificate as the cause would be unknown. These are unlikely to have archival value	Review and destroy if no longer required
Death – register information sent to the General registry office on a monthly basis*	2 years	A full dataset is available from ONS.	Review and consider transfer to PoD
Local authority adoption record (usually held by the LA)*	100 years	The local authority Children's Social Care Team hold the primary record of the adoption process. Consider transferring to PoD only if there are known gaps in the primary local authority record, or the records predate 1976.	Review and consider transfer to PoD
Mortuary records of Deceased persons	10 years	Retention begins at the end of the year to which they relate.	Review and consider transfer to PoD
Mortuary register*	10 years		Review and consider transfer to PoD
NHS medicals for adoption records	8 years or 25th birthday	The health reports will feed into the primary record held by the local authority. This means that adoption records held in the NHS relate to reports that are already kept in another file, which is kept for 100 years by the relevant agency or local authority. Consider transferring to PoD only if there are known gaps in the primary local authority record or the records pre-date 1976.	Review and consider transfer to PoD
Post-mortem records*	10 years	The coroner will maintain and retain the primary post-mortem file including the report. Hospital post-mortem records will not need to be kept for the same extended time period as (subject to local policy) these reports may also be kept in the medical file.	Review and destroy if no longer required
Advanced medical therapy research - master file	20 years		Review and consider transfer to PoD
Clinical trials – applications for ethical approval	5 years	Master file of a trial authorised under the European portal, under Regulation 536/2014. For clinical trials records retention refer to the MHRA guidance. The sponsor of the study will be the primary holder of the study file and associated data. This is based on the Medicines for Human Use (Clinical Trials) Amendment Regulations 2006 (specifically Regulations 18 and	Review and consider transfer to PoD

Record Type	Retention Period	Notes	Disposal Action
		28).	
European Commission Authorisation (certificate or letter) to enable marketing and sale within EU member state's area	15 years		Review and consider transfer to PoD
Research - datasets	No longer than 20 years		Review and consider transfer to PoD
Research – ethics committee's and HRA approval documentation for research proposal and records to process patient information without consent	5 years	This applies to trials where opinions are given to proceed with the trial, or not to proceed. These may also have archival value.	Review and consider transfer to PoD
Research – ethics committee's minutes (including records to process patient information without consent)	20 years	Retention period begins from the year to which they relate and can be as long as 20 years. Committee minutes must be transferred to PoD.	Review and consider transfer to PoD
Board meetings	Up to 20 years	A local decision can be made on how long to retain the minutes of board meetings (and associated papers linked to the board meeting), but this must not exceed 20 years, and will be required to be transferred to the local PoD or The National Archives (for National Bodies).	Review and consider transfer to PoD
Board meeting (closed boards)	Up to 20 years	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.	Review and consider transfer to PoD
Chief executive records	Up to 20 years	This may include emails and correspondence where they are not already included in board papers.	Review and consider transfer to PoD
Committees (major) - listed in Scheme of delegation or report direct into the board (including major projects)	Up to 20 years		Review and consider transfer to PoD
Committees (minor) – not listed in scheme of delegation*	6 years	Includes minor meetings, projects, and departmental business meetings. These may have local historical value and require transfer consideration.	Review and consider transfer to PoD
Corporate records of health and care organisations and providers that predate the NHS (July 1948)		Contact your local PoD to arrange review and transfer. Records not selected by the PoD must be securely destroyed. An example might be the minutes of the hospital board from 1932, or midwifery diaries dated Dec 1922.	Review and consider transfer to PoD
Data Protection Impact Assessments (DPIAs)	6 Years	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.	Review and destroy if no longer required
Destruction certificates or record of information held on destroyed physical media	20 years	Where a record is listed for potential transfer to PoD have been destroyed without adequate appraisal, consideration should be given to a selection of these as an indicator of what has not been preserved	Review and destroy if no longer required
Electronic metadata destruction stubs		Refer to destruction certificates	
Incidents – serious	20 years	Retention begins from the date of the Incident – not when the incident was reported.	Review and consider transfer to PoD
Incidents- not serious	10 years	Retention begins from the date of the incident – not when the incident was reported.	Review and destroy if no longer required
Incidents – serious incidents requiring investigation	20 years	These include independent investigations into incidents. These may have permanent retention value so consult with the local PoD. If they are not required, then destroy	Review and consider transfer to PoD
Non-clinical QA records	12 years	Retention begins from the end of the year to which the assurance relates.	Review and destroy if no longer required
Patient advice and liaison service (PALS) records	10 years	Retention begins from the close of the financial year to which the record relates.	Review and destroy if no longer required

Record Type	Retention Period	Notes	Disposal Action
Patient surveys – individual returns and analysis	1 year after return	May be required again if analysis is reviewed.	Review and destroy if no longer required
Patient surveys – final report	10 years	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.	Review and consider transfer to PoD
Policies, strategies and operating procedures – including business plans*	Life of the organisations plus six years	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 PoD.	Review and consider transfer to PoD
Quarterly reviews from NHS trusts	6 years	Retention period in accordance with the Limitation Act 1980.	Review and destroy if no longer required
Risk register	6 years	Retention period in accordance with the Limitation Act and corporate awareness of risks.	Review and destroy if no longer required
Staff surveys – individual returns and analysis	1 year after return	Forms are anonymous so do not contain PID unless provided in free text boxes. May be required again if analysis is reviewed.	Review and destroy if no longer required
Staff survey – final report	10 years	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.	Review and consider transfer to PoD
Trust submission forms	6 years	Retention period in accordance with the Limitation Act 1980.	Review and destroy if no longer required
Intranet site*	6 years		Review and consider transfer to PoD
Patient Information leaflets	6 years	These do not need to be leaflets from every part of the organisation. A central copy can be kept for potential transfer.	Review and consider transfer to PoD
Press releases and important internal communications	6 years	Press releases may form part of a significant part of the public record of an organisation which may need to be retained.	Review and consider transfer to PoD
Public consultations	5 years	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.	Review and consider transfer to PoD
Website	6 years	The PoD may be able to receive these by a regular crawl. Consult with the PoD on how to manage the process. Websites are complex objects, but crawls can be made more effective if certain steps are taken. .	Review and consider transfer to PoD
Duty roster	6 years	Retention begins from the close of the financial year.	Review and if no longer needed destroy
Exposure monitoring information	40 years or 5 years from the date of the last entry made in it	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.	Review and if no longer needed destroy
Occupational health records	Keep until 75th birthday or 6 years after the staff member leaves whichever is sooner		Review and if no longer needed destroy
Occupational health report of staff member under health surveillance	Keep until 75th birthday		Review and if no longer needed destroy
Occupational health report of staff member under health surveillance where they have been subject to radiation doses	50 years from the date of the last entry or until 75th birthday, whichever is		Review and if no longer needed destroy

Record Type	Retention Period	Notes	Disposal Action
	longer		
Staff records	Until 75th birthday	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 PoDs accession NHS staff records for social history purposes. Check with your local PoD about possible accession. If the PoD does not accession them, then the records can be securely destroyed once the retention period has been reached	Review and consider transfer to PoD
Staff records-summary	75th birthday	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 PoD. If the PoD does not require them, then they can be securely destroyed at this point.	Review and consider transfer to PoD
Timesheets	2 years	Retention begins from creation.	Review and if no longer needed destroy
Staff training records	See notes	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	Review and consider transfer to PoD
Disciplinary records	6 years	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.	Review and if no longer needed destroy
Contracts sealed or unsealed	6 years after the end of the contract		Review and if no longer needed destroy
Contracts - financial approval files	15 years after the end of the contract		Review and if no longer needed destroy
Contracts - financial approved suppliers documentation	11 years after the end of the contract		Review and if no longer needed destroy
Tenders (successful)	6 years after the end of the contract		Review and if no longer needed destroy
Tenders (unsuccessful)	6 years after the end of the contract		Review and if no longer needed destroy
Building plans, including records of major building works	Lifetime (or disposal) of building plus 6 years	Building plans and records of works are potentially of historical interest and where possible, should be kept and transferred to the local PoD.	Review and consider transfer to PoD
Closed circuit television (CCTV)	Refer to ICO Code of Practice	The length of retention must be determined by the purpose for which the CCTV has been used. CCTV footage must remain viewable for the length of time it is retained, and where possible, systems should have redaction or censoring functionality to be able to blank out the faces of people who are captured by the CCTV, but not subject to the access request, for example, police reviewing CCTV as part of an investigation. guidance-on-video-surveillance-including-cctv-1-0.pdf (ico.org.uk)	Review and destroy if no longer required
Equipment monitoring, and testing and maintenance work where ASBESTOS is a factor	40 years	Retention begins from the completion of the monitoring or testing. This includes records of air monitoring and health records relating to asbestos exposure, as required by the Control of Asbestos Regulations 2012	Review and destroy if no longer required
Equipment monitoring – general testing and maintenance work	Lifetime of installation	Retention begins from the completion of the testing and maintenance	Review and destroy if no longer required

Record Type	Retention Period	Notes	Disposal Action
Inspection reports	Lifetime of installation	Retention begins at the END of the installation period. Building inspection records need to comply with the Construction (Design and Management) Regulations 2015.	Review and destroy if no longer required
Leases	12 years	Retention begins at point of lease termination.	Review and destroy if no longer required
Minor building works	6 years	Retention begins at the point of WORKS COMPLETION.	Review and destroy if no longer required
Photographic collections – service locations, events and activities	Up to 20 years	These provide a visual historical legacy of the running and operation of an organisation. They may also provide secondary uses, such as use in public inquiries.	Review and consider transfer to PoD
Radioactive records	30 years	Retention begins at the CREATION of the waste. If a person handling radioactive waste is exposed to radiation (accidental or otherwise), then the records relating to that person must be kept until they reach 75 years of age or would have attained that age. In any event, records must be kept for at least 30 years from the date of dosing or accident. This also includes patients or service users who require medical exposure to radiation, as required by the Ionising Radiation Regulations 2017.	Review and destroy if no longer required
Sterilix Endoscopic Disinfector Daily Water Cycle Test, Purge Test, Ninhyndrin Test	11 years	Retention begins from the DATE OF TEST.	Review and destroy if no longer required
Surveys – building or installation (not patient surveys)	Lifetime of Installation or building	Retention period begins at the END of INSTALLATION period. (See Inspection reports for legal basis for these records)	Review and consider transfer to PoD
Accounts	3 years	Retention begins at the CLOSE of the financial year to which they relate. Includes all associated documentation and records for the purpose of audit	Review and destroy if no longer required
Benefactors	8 years	These may already be in the financial accounts and may be captured in other reports, records or committee papers. Benefactions, endowments, trust fund or legacies should be offered to the local PoD.	Review and consider transfer to PoD
Debtors' records – CLEARED	2 years	Retention begins at the CLOSE of the financial year to which they relate.	Review and destroy if no longer required
Debtors' records – NOT CLEARED	6 years	Retention begins at the CLOSE of the financial year to which they relate	Review and destroy if no longer required
Donations	6 years	Retention begins at the CLOSE of the financial year to which they relate	Review and destroy if no longer required
Expenses	6 years	Retention begins at the CLOSE of the financial year to which they relate	Review and destroy if no longer required
Final annual accounts report*	Up to 20 years	These should be transferred when practically possible, after being retained locally for a minimum of 6 years. Ideally, these will be transferred with board papers for that year to keep a complete set of governance papers.	Review and consider transfer to PoD
Financial transaction records	6 years	Retention begins at the CLOSE of the financial year to which they relate	Review and destroy if no longer required
Invoices	6 years from end of the financial year they relate to		Review and destroy if no longer required
Petty cash	2 years	Retention begins at the CLOSE of the financial year to which they relate	Review and destroy if no longer required
Private Finance Initiatives	Lifetime of	Retention begins at the END of the PFI agreement. This applies to	Review and

Record Type	Retention Period	Notes	Disposal Action
(PFI) files	PFI	the key papers only in the PFI.	consider transfer to PoD
Staff salary information or files	10 years	Retention begins at the CLOSE of the financial year to which they relate	Review and destroy if no longer required
Superannuation records	10 years	Retention begins at the CLOSE of the financial year to which they relate	Review and destroy if no longer required
Complaints – case files	10 years	Retention begins at the closure of the complaint. The complaint is not closed until all processes (including potential and actual litigation) have ended. The detailed complaint file must be kept separately from the patient file (if the complaint is raised by a patient or in relation to). Complaint file must always be separate.	Review and destroy if no longer required
Fraud – case files	6 years	Retention begins at the closure of the case. This also includes cases that are both proven and unproven	Review and destroy if no longer required
Freedom of Information (FOI) requests, responses to the request and associated correspondence	3 years	Retention begins from the closure of the FOI request. Where redactions have been made, it is important to keep a copy of the response and send to the requestor in all cases, a log must be kept of requests and the response sent.	Review and destroy if no longer required
FOI requests – where there has been an appeal	6 years	Retention begins from the closure of the appeal process	Review and destroy if no longer required
Industrial relations – including tribunal case records	10 years	Retention begins at the CLOSE of the financial year to which it relates. Some organisations may record these as part of the staff record, but in most cases, they should form a distinctive separate record (like complaints files).	Review and consider transfer to PoD
Litigation records	10 years	Retention begins at the CLOSURE of the case. Litigation cases of significant or major issues (or with significant, major outcomes) should be considered for transfer. Minor cases should not be considered for transfer. If in doubt, consult with the PoD.	Review and consider transfer to PoD
Intel patents, trademarks, copyright, IP	Lifetime of patent, or 6 years from end of licence or action	Retention begins at the END of lifetime or patent, or TERMINATION of licence or action.	Review and consider transfer to PoD
Software licences	Lifetime of software	Retention begins at the end of lifetime of software	Review and destroy if no longer required
Subject Access Requests (SAR), response, and Subsequent correspondence	3 years	Retention begins at the CLOSURE of the SAR.	Review and destroy if no longer required
SAR – where there has been an appeal	6 years	Retention begins at closure of appeal	Review and destroy if no longer required

HOW TO DEAL WITH SPECIFIC TYPES OF RECORDS

Adopted persons health records

Notwithstanding any other centrally issued guidance by the Department of Health and Social Care or Department for Education, the records of adopted persons can only be placed under the new last name when an adoption order has been granted. Before an adoption order is granted, an alias may be used but more commonly the birth names are used. Depending on the circumstances of the adoption there may be a need to protect from disclosure any information about a third party. Additional checks before any disclosure of adoption documentation are recommended because of the heightened risk of accidental disclosure. It is important that any new records, if created, contain sufficient

information to allow for a continuity of care. At present the GP would initiate any change of NHS number or identity if it were considered appropriate to do so following the adoption.

Asylum seeker records
Records for asylum seekers must be treated in exactly the same way as other care records, allowing for clinical continuity and evidence of professional conduct. Organisations may decide to give asylum seekers patient or service user held records (section below) or hold them themselves. Patient or service user held records should be subject to a risk assessment because the record legally belongs to the organisation, and if required, they must be able to get it back. There is a risk that patient or service user held records could be tampered with or altered in an unauthorised way so careful consideration needs to be given to this decision.

Audio and visual records
Audio and visual records can take many forms such as using a dictaphone (digital or analogue) to record a session or conducting a health or care interaction using videoconferencing technologies. The following needs considering when patient or service user interactions are captured in this way:

• **Clinical appropriateness:** Organisations should decide when it is appropriate to use audio or visual methods for the provision of health or care. This should be documented in organisational policies and understood by the relevant health and care professionals.

• **Retention**: If the recording is going to be kept elsewhere (for example, as part of the health and care record) then there is no reason to keep the original recording provided the version in the main record is the same as the original or there is a summary into words which is accurate and adequate for its purpose. If the recording is the only version or instance of the interaction, then it must be kept for the relevant retention period outlined in this Code (for example, adult, child health or mental health retention periods). Some recordings may have archival value (although this is unlikely), and this should be considered on a case-by-case basis.

• **Digital continuity:** You must consider the medium on which the recording is made and ensure that it is available throughout its retention period (for example, if the system or file format is becoming obsolete, then you will need to migrate it to a newer platform or format to ensure availability). If it is a digital recording and you are looking to store it in the health and care record, ensure the transfer process captures the authenticity of the recording kept.

- **Storage:** Ensure your recordings are stored on systems you control or are provided to you under contract. If stored with the product provider, you must give them (as controller) clear instructions on the storage and retention of those images (for example, delete one month after the date of the recording because it has been summarised into the main health and care record or retain for 8 years from consultation with the patient or service user, then destroy). Providers acting under contract to a controller are obliged to carry out their written instruction.

• **Transparency:** You must be transparent with patients and service users regarding the use of audio and visual technology, and associated records, so that they have a reasonable understanding of how they will be used, why, and what will happen with the recording after the interaction. For example, it would be unfair to tell participants that the recordings are deleted if they are not.

Complaints records
Where a patient or service user complains about a service, it is necessary to keep a separate file relating to the complaint and subsequent investigation. Detailed complaint information should never be recorded in the health and care record. A complaint may be unfounded or involve third parties and the inclusion of that information in the health or care record will mean that the information will be preserved for the life of the record and could cause detrimental prejudice to the relationship between the patient or service user and the Health and Care Team. In some cases, it may be appropriate to share details of the complaint with the health and care professional involved in providing individual care in order to make improvements in care delivery. However, there may also be times where the complaint is about an individual but not care related and it might not be appropriate to share details of the complaint with that person in case further action is required. The Complaints Team should review each complaint on a case by-case basis.

Where multiple teams are involved in the complaint handling, all the associated records must be brought together to form a single record. This will prevent the situation where one part of the organisation does not know what the other has done. A complaint cannot be fully investigated if the investigation is based on incomplete information. It is common for the patient or service user to ask to see a copy of their complaint file and it will be easier to deal with if all the relevant material is in one file. Where complaints are referred to the Ombudsman Service, a single file will be easier to refer to.

Health and care organisations should have a local policy to follow with regards to complaints, covering how information will be used once any complaint is raised, and after the complaint has been investigated, regardless of outcome. The ICO has also issued guidance on complaints files and who can have access to them, which will drive what must be stored in them.

Contract change records
Once a contract ends, any service provider still has a liability for the work they have done and, as a general rule, at any change of contract the records must be retained until the time period for liability has expired.

In the standard NHS contract, there is an option to allow the commissioner to direct a transfer of care records to a new provider for continuity of service and this includes third parties and those working under any qualified provider contracts. This will usually be to ensure the continuity of service provision (for current cases) upon termination of the contract. It is also the case that after the contract period has ended, the previous provider will remain liable for their work. In this instance there may be a need to make the records available for continuity of care or for professional conduct cases.

When a service is taken over by a new provider, the records of the service (current and discharged cases) all transfer to the new provider (unless directed otherwise by the commissioner of the service). This is to ensure that the records for the service remain complete and enable patients or service users to obtain their record if they so request it. It also makes the records easier to locate if they are required for other purposes. This will also stop the fragmentation of the archive records for the service and make it much easier to retrieve records.

Where legislation creates or disbands public sector organisations, the legislation will normally specify which organisation holds liability for any action conducted by a former organisation. This may also include consideration of the identity of the legal entity, which must manage the records.

In some cases, records may end up orphaned. This may happen where the organisation that created them is being disbanded and there is no successor organisation to take over the service or provision. In these cases, orphaned records need to be retained by the highest level commissioner of that service or provision. For example, if a GP practice closes, patients will be offered the choice to register with another nearby practice. When they register with the new practice, the record will follow the patient to that new practice. However, if a practice closes, and the patient does not re-register elsewhere, the record will transfer to NHS England and Improvement, who commission primary care services in England for ongoing management.

Where the content of records is confidential, for example, health and care records, it will be necessary to inform the individuals concerned about the change. Where there is little impact upon those receiving care, it may be sufficient to use posters and leaflets to inform people about the change, but more significant changes will require individual communications. Although the conditions of UK GDPR may be satisfied, in many cases there is still a duty of confidentiality which may require a patient or service user (in some cases) to agree to the transfer, dependent upon the legal basis and the implications of their choice discussed with them. If the new provider has a statutory duty to provide the service, then consent does not need to be sought. If there is no statutory duty, then consent would need to be sought to satisfy the common law duty of confidentiality.

It is vital to highlight the importance of actively managing records, which are stored in offsite storage (refer to section three of the Code for further information on offsite storage including the importance of completing a DPIA). These principles and guidance can also apply to non-clinical situations as well, such as when CCGs merge or a trust takes over the running of another one.

For more information, please refer to
NHSE Records Management Code of Practice for Health & Social Care 2023 V5