University Hospitals Bristol and Weston NHS Foundation Trust

Records Management and Retention Policy

Document Data			
Document Type:	Policy		
Document Reference	19302		
Document Status:	Approved		
Document Owner:	Trust Secretary		
Executive Lead:	Director of Finance & Information (Senior Information Risk Owner)		
Approval Authority:	Executive Committee		
Review Cycle:	36		
Date Version Effective From:	23 November 2022	**Date Version Effective To:**	22 November2025

What is in this policy?
The contents of this policy set out the requirements for the creation, storage, retention and destruction of all documents held by University Hospitals Bristol and Weston NHS Foundation Trust (the Trust).

Document Change Control				
Date of Version	**Version Number**	**Lead for Revisions (Job title only)**	**Type of Revision**	**Description of Revision**
01/03/2014	2	Trust Secretary		
17/02/2016	3	Trust Secretary	Major	Re-write and update of policy.
30/04/2018	3.1	Trust Secretary	Minor	Inclusion of 5.8 (e), (f) and (g) in relation to agreed schedule of email deletion.
11/04/2018	4.1	Information Governance Officer	Major	First draft – Combination of Corporate Records Retention Policy and Health Records Retention Schedule
21/06/2018	4.2	Information Governance Officer	Minor	Addition of UHB decisions on Records Retention
16/08/2018	4.3	Deputy Trust Secretary	Minor	Clarifications and update of monitoring table
30/09/2022	5.0	Information Governance	Major	Update of NHS Records Management Code of Practice and inclusion of national inquiries and their effect on records retention at the Trust.

Table of Contents

Sign off Process and Dates	
Groups consulted	**Date agreed**
Information Risk Management Group	30/09/2022
Policy Assurance Group	15/11/2022
Executive Committee	23/11/2022

- **Stakeholder Group** can include any group that has been consulted over the content or requirement for this policy.
- **Steering Group** can include any meeting of professionals who has been involved in agreeing specific content relating to this policy.
- **Other Groups** include any meetings consulted over this policy.
- **Policy Assurance Group** must agree this document before it is sent to the **Approval Authority** for final sign off before upload to the DMS.

Do I need to read this Policy?

All Staff

Must be aware of their responsibilities in relation to data protection and information security.

Staff responsible for the maintenance, archiving and destruction of information.

Must read and be familiar with this full policy.

1. Introduction

This document sets out the Trust's Records Retention Policy, in compliance with the Records Management Code of Practice 2021 - NHS Transformation Directorate (nhsx.nhs.uk) produced by the Information Governance Alliance (or any succeeding document), to ensure that records are managed appropriately across the Trust.

Records Management is essential to making sure the Trust has high quality information available to support safe care and effective decision making and is in compliance with all relevant laws and regulations.

2. Purpose

This document aims to set out how records are created, stored, retained and destroyed with reference to the record's minimum retention period and the records ongoing value to the organisation or possible historical value, to ensure compliance with the Data Protection Act 2018 .

3. Scope

This policy applies to all Trust staff[1], and all records created across the Trust in all formats, including, but not limited to:

(a) Paper;

(b) Electronic;

(c) Email;

(d) Digital;

(e) Social Media;

(f) Audio/Video Recordings.

This policy will be applied as necessary to comply with the legal and professional obligations set out for records, in particular:

(g) Public Records Act 1958;

(h) Access to Health Records Act 1990;

(i) Freedom of Information Act 2000;

(j) Regulation of Investigatory Powers Act 2000;

(k) UK General Data Protection Regulation 2016;

[1] Including contractors and volunteers.

(l) Data Protection Act 2018.

4. Definitions

4.1 Corporate Records

All records held by the Trust that are not medical records, according to the definition below (**4.2**).

4.2 Medical Records

Any electronic or paper information that is recorded about a person for the purpose of managing their healthcare.

4.3 Minimum Retention Period

The minimum period of time that a record must be held for as defined in the Records Management Code of Practice 2021 - NHS Transformation Directorate (nhsx.nhs.uk)

4.4 Retention Period Start

The time or event that starts the minimum retention period as defined in the Records Management Code of Practice 2021 - NHS Transformation Directorate (nhsx.nhs.uk)

4.5 Records Lifecycle

The life of a record from its creation or receipt, through the period of active use, to a period of inactive retention and finally either confidential destruction or archival preservation.

4.6 Information Asset

Identifiable and definable system that stores information and has value to the Trust. These can be physical or electronic.

4.7 Place of Deposit

Local Records Archives appointed by The National Archives under the Public Records Act 1958.

5. Duties, Roles and Responsibilities

5.1 Trust Board of Directors

(a) Act on behalf of the Trust as a registered data controller.

(b) Be assured that the Trust complies with all prevailing legislation and regulation in relation to records management.

5.2 Senior Leadership Team

(a) Review and approve this policy.

(b) Ensure that the Trust complies with all prevailing legislation and regulation in relation to records management.

5.3 Divisional Management Boards

(a) Take responsibility for all records management practices and ensure compliance with this policy within their division.

5.4 Senior Information Risk Owner (SIRO)

(a) Take lead responsibility for all records management and for ensuring compliance with this policy across the Trust.

(b) Own and lead responsive action to any risks relating to records management or information assets.

(c) Be assured that the relevant assets and records are suitably managed and that risks are identified and mitigated accordingly.

(d) Take lead responsibility for Trust-wide compliance with this policy.

5.5 Caldicott Guardian

(a) Ensure that patient information that is used, stored and shared by the Trust complies with the Caldicott Principles.

5.6 Trust Secretary Director of Corporate Governance

(a) Take lead responsibility for the Trust's Records Retention Policy, to ensure good corporate records management practice across the Trust.

(b) Ensure information regarding the retention of records is disseminated to all staff.

5.7 Chief Information Officer (CIO)

(a) Ensure that Information Systems in use at the Trust comply with all requirements of systems that hold personal information, namely:

(i) Store information securely;
(ii) Control access to information based on operational need;
(iii) Are regularly backed-up;
(iv) Maintain the integrity of stored information;
(v) Remain accessible;
(vi) Can delete information on request;
(vii) Can retrieve useful, timely information in response to a Subject Access Request;
(viii) Can audit who has accessed or changed information.

(b) Ensure there are sufficient processes in place for the confidential disposal of old IT equipment and storage media.

5.8 Trust-wide Health Records and EDM Manager

(a) Produce and maintain Trust-wide health records policies and procedures.

(b) Take lead responsibility for all health records management and compliance with this policy.

5.9 Information Governance Team

(a) Provide guidance to ensure the policy remains up to date and compliant with relevant legislation and other regulations.

(b) Guide and advise all staff, especially information asset owners/administrators and departmental managers, on the contents of this policy.

(c) Maintain the Information Governance Risk Register including any risks relating to records management.

5.10 Information Asset Owners

(a) Ensure that the information assets under their responsibility comply with all requirements for information assets, namely:

(i) Store information securely;
(ii) Control access to information based on operational need;
(iii) Are regularly backed-up;
(iv) Maintain the integrity of stored information;
(v) Remain accessible;
(vi) Can delete information on request;
(vii) Can retrieve useful, timely information in response to a Subject Access Request;
(viii) Can audit who has accessed or changed information.

(b) Assure the SIRO that the assets they have responsibility for are suitably managed and to identify and mitigate risks accordingly.

(c) Assign an information asset administrator who is responsible for the day to day running of the information asset.

5.11 Information Asset Administrators

(a) Ensure that the information asset they are assigned the day to day responsibility for comply with all requirements for information assets, namely:

(i) Store information securely;
(ii) Control access to information based on operational need;

(iii) Is regularly backed-up;
(iv) Maintains the integrity of stored information;
(v) Remains accessible;
(vi) Can delete information on request;
(vii) Can retrieve useful, timely information in response to a Subject Access Request;
(viii) Can provide audit information on who has accessed or changed information.

(b) Report any problems or issues that arise from the day to day administration of the information asset to the information asset owner.

5.12 Departmental Managers

(a) Take responsibility for all records management practices and compliance with this policy within their department.

(b) Use the Departmental Record Security Checklist featured in Appendix D to assess information security in their own area at regular intervals

5.13 Risk Management Group

(a) Receive information and assurance from the Information Risk Management Group that it is fulfilling its duties in relation to the requirements of this policy.

5.14 Information Risk Management Group

(a) Provide oversight for all risks relating to records management.

(b) Regularly review the Information Governance Risk Register including any risks relating to records management.

5.15 Health Records Forum

(a) Coordinate and lead activity relating to issues of health records management.

(b) Advise the Trust's Information Risk Management Group on any issues relating to health records management.

5.16 All Staff

(a) Manage all records in keeping with this policy.

(b) Complete annual Information Governance training which includes a section on records management.

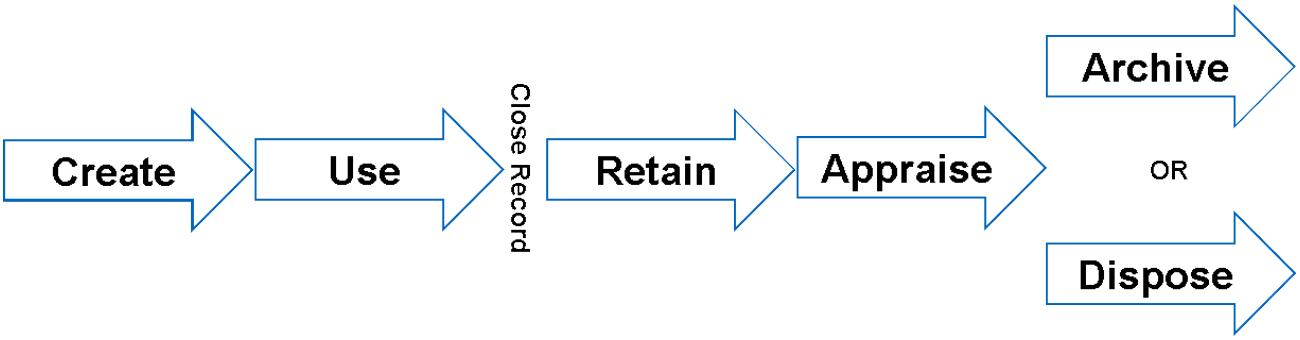
(c) Any procedural documents that are printed are uncontrolled copies. Document users are therefore responsible for ensuring printed copies are valid prior to use – i.e. that they are referring to the most up-to-date versions of all procedural documents (see **Section 6.8**).

6. Policy Statement and Provisions

6.1 Records Lifecycle

The Records Lifecycle is a term that is used to describe the life of a record from its creation or receipt, through the period of active use, to a period of inactive retention and finally either confidential destruction or archival preservation.

The lifecycle can be explained by the figure below and explained in more detail in sections 6.2 to 6.7.



6.2 Creation/Receipt of Records

When records are created or received they should be logically named with a clear title that describes what the record is.

If the record is a policy, form or procedural document then it must be version controlled to denote that all staff are working with the most up to date version of the record.

The information recorded must be useful, high quality information that is accurate, relevant and up to date.

6.3 Use of Records

Whilst in active use, the record should be stored and handled appropriately.

Paper records must be locked in drawers or cabinets when not in use and stored away from potential sources of damage, loss or theft at all times.

Electronic records must be appropriately protected, and all those stored on the Trust network are considered to have sufficient protection. Any portable IT equipment or removable media should be encrypted.

All proposed cloud storage must gain information governance approval through the Information Risk Governance Group before its use.

Primary electronic records should always be stored in appropriately secure shared folders, and never in personal folders. This allows other staff to access the record in the document owner's absence, and ensures appropriate security protections for stored documents.

Health records must be traced accurately at all times.

Staff members are encouraged to use electronic records wherever possible to assist the aim of a paper-free NHS. Paper records can be scanned and stored on shared folders.

Once the record is no longer in active use, it is regarded as closed, and it begins its retention period.

6.4 Retention of Records

All records across the Trust have a minimum retention period that starts at a predetermined moment. Records should continue to be stored securely throughout their retention period.

All information can be found in the Records Management Code of Practice 2021 - NHS Transformation Directorate (nhsx.nhs.uk)

6.5 Appraisal of Records

Once a record reaches the end of its retention period, it should be appraised as to whether the record holds further value to the Trust or has possible future historical value.

The disposal action in the record search details The of the Records Management Code of Practice for Health and Social Care 2021 give prompts whether a record may have historical value and should be offered to a Place of Deposit.

If the record is appraised as having further value to the Trust, this decision must be documented, a new review date established and then it must be further retained. The maximum length of time for retaining records is 30 years.

6.6 Archival of Records

Records that are appraised as having future historical value should be offered to a Place of Deposit for permanent preservation.

A Place of Deposit is a Local Records Archive run by The National Archives. The Bristol Archives are the Trust's Local Records Archive and can be contacted using the details on their website.

6.7 Disposal of Records

All records that hold no further value to Trust, nor have possible historic value should be disposed of in line with the Trust's Management of Waste Policy.

Records should only be destroyed in line with this policy. It is a criminal offence to destroy requested information in order to prevent a disclosure under either the Data Protection Act or the Freedom of Information Act. Unnecessary retention of records places the Trust at increased risk of not fully complying with requests for information under the Data Protection Act and Freedom of Information Act.

The disposal of records may be limited by external inquiries the Trust is subject to. Details of these

inquiries are listed in Appendix E. Once a "Stop Notice" has been issued, it is a criminal offence to destroy records in scope of a national inquiry.

6.8 Document Management Service

The Trust's Document Management Services (DMS) is a central repository for all Trust-wide policies and clinical guidelines and is managed by the Trust Secretariat.

6.9 Trust Decisions on Records Retention

The Trust manages its own email domain, @uhbw.nhs.uk, and therefore must outline the retention of staff emails by the Trust. Email is a communication tool and not an information repository. The Trust will retain copies of all emails sent and received by its staff for seven years as this corresponds with the civil statute of limitations.

Personal Electronic Folders are available for staff to store personal documentation they want to retain throughout their employment. The contents of a user's Personal Electronic Folder will be deleted seven years after they have left the Trust.

Cleaning Records should be kept for a minimum of 3 years. Any incidents resulting in personal injury involving the cleaning of wards and departments will be recorded on Datix which is subject to longer retention periods.

7. Standards and Key Performance Indicators

7.1 Applicable Standards

The applicable standards for this policy are the regulations and guidance listed in **Section 3**.

7.2 Measurement and Key Performance Indicators

Keeping an up to date, accurate Information Asset Register is a key requirement of the General Data Protection Regulation 2016 for the Trust, and is monitored by the Data Security and Protection Toolkit.

8. Associated Documentation

Records Management Code of Practice 2021 - NHS Transformation Directorate (nhsx.nhs.uk)

Information Governance Policy

Data Protection Policy

Procedural Document Management Policy

Management of Waste Policy

Health Records Policy

9. Appendix A – Monitoring Table for this Policy

The following table sets out the monitoring provisions associated with this Policy.

Objective	Evidence	Method	Frequency	Responsible	Committee
That digitally held information is only accessed by staff for appropriate professional purposes.	That audit evidence for digital systems shows that information is accessed appropriately by staff.	Reporting on appropriate usage of access to information on digital systems.	Quarterly	Information Management and Technology Department	Information Risk Management Group
To ensure Trust policies are compliance with overarching records management legislation.	That policies are accurate, up to date, and in use.	Audit evidence collation for the NHS Digital data protection toolkit.	Annually	Information Governance Team	Information Risk Management Group
To ensure Trust policies are maintained and updated in line with best practice, and the Trust's records retention requirements.	That Trust policies are version controlled and appropriately archived in line with the policy.	Internal audit	Three yearly	Trust Secretary	Risk Management Group
To ensure emails and personal folders are retained and deleted in compliance with this policy.	That relevant destruction schedules are maintained.	Reporting on destruction schedules.	Annually	Information Management and Technology Department	Information Risk Management Group

10. Appendix B – Dissemination, Implementation and Training Plan

The following table sets out the dissemination, implementation and training provisions associated with this Policy.

Plan Elements	Plan Details
The Dissemination Lead is:	Trust Secretary

Plan Elements	Plan Details
This document replaces existing documentation:	Yes
Existing documentation will be replace by:	Corporate Records Retention Policy Health Records Retention Schedule
This document is to be disseminated to:	All Staff
Method of dissemination:	Newsbeat
Training is required:	Yes
The Training Lead is:	Information Governance Officer

Additional Comments
[DITP - Additional Comments]

11. Appendix C – Equality Impact Assessment (EIA) Screening Tool

Query	Response
What is the main purpose of the document?	This document aims to set out how records are created, stored, retained and destroyed with reference to the records minimum retention period and the records ongoing value to the organisation or possible historical value.
Who is the target audience of the document (which staff groups)?	Add ☑ or ☒
Who is it likely to impact on? (Please tick all that apply.)	All staff

Could the document have a significant **negative** impact on equality in relation to each of these characteristics?	YES	NO	Please explain why, and what evidence supports this assessment.
Age (including younger and older people)		☑	
Disability (including physical and sensory impairments, learning disabilities, mental health)		☑	
Gender reassignment		☑	
Pregnancy and maternity		☑	
Race (includes ethnicity as well as gypsy travellers)		☑	
Religion and belief (includes non-belief)		☑	

Sex (male and female)		☑	
Sexual Orientation (lesbian, gay, bisexual, other)		☑	
Groups at risk of stigma or social exclusion (e.g. offenders, homeless people)		☑	
Human Rights (particularly rights to privacy, dignity, liberty and non-degrading treatment)		☑	

Will the document create any problems or barriers to any community or group? NO

Will any group be excluded because of this document? NO

Will the document result in discrimination against any group? NO

If the answer to any of these questions is YES, you must complete a full Equality Impact Assessment.

Could the document have a significant **positive** impact on inclusion by reducing inequalities?	YES	NO	If yes, please explain why, and what evidence supports this assessment.
Will it promote equal opportunities for people from all groups?		☑	
Will it help to get rid of discrimination?		☑	
Will it help to get rid of harassment?		☑	
Will it promote good relations between people from all groups?		☑	
Will it promote and protect human rights?		☑	

On the basis of the information / evidence so far, do you believe that the document will have a positive or negative impact on equality? (Please rate by circling the level of impact, below.)

Positive impact				Negative Impact		
Significant	Some	Very Little	NONE ☑	Very Little	Some	Significant

Is a full equality impact assessment required? NO

Date assessment completed: 16/08/2018

Person completing the assessment: Deputy Trust Secretary

12. Appendix D – Departmental Record Security Checklist

People	
Staff challenge visitors to the ward	
Staff ensure that nobody tailgates them through staff access doors	
Staff are wearing their Trust ID badges	
Paperwork	
Paperwork & medical records are stored in locked cabinets when not in use	
Hospital notes are traced accurately on Careflow	
Confidential waste is disposed of securely	
All paperwork is filed in the correct patient's record	
Visitors don't have direct sight of paperwork or medical records	
IT Equipment	
PCs aren't left unlocked or unattended	
Fax machines (if absolutely necessary) are stored out of sight of any visitors	
Printed documents aren't left in the printer tray	
Staff check PCs for any unauthorised USB devices	
Staff do not store confidential information on their own mobile devices	
PC screens in view of the public have privacy screens	
Security	
Offices are locked when not in use	
Store rooms are locked when not in use	
Treatment rooms are locked when not in use	
Buzzer systems are used where installed	

Completed by: .....

Date: .....

Signed: .....

13. Appendix E – Details of National Inquiries Impacting Trust Records Retention

Inquiry	Purpose	Terms of Reference
Independent Inquiry Child Sexual Abuse	To consider the extent to which State and non-State institutions have failed in their duty of care to protect children from sexual abuse and exploitation; to consider the extent to which those failings have since been addressed; to identify further action needed to address any failings identified; to consider the steps which it is necessary for State and non-State institutions to take in order to protect children from such abuse in future; and to publish a report with recommendations.	https://www.iicsa.org.uk/about-us/terms-reference
Infected Blood Inquiry	The Inquiry will examine why men, women and children in the UK were given infected blood and/or infected blood products; the impact on their families; how the authorities (including government) responded; the nature of any support provided following infection; questions of consent; and whether there was a cover-up.	https://www.infectedbloodinquiry.org.uk/terms-reference
UK Covid-19 Inquiry	The inquiry will examine, consider and report on preparations and the response to the pandemic in England, Wales, Scotland and Northern Ireland, up to and including the inquiry's formal setting-up date. In doing so, it will consider reserved and devolved matters across the United Kingdom, as necessary, but will seek to minimise duplication of investigation, evidence gathering and reporting with any other public inquiry established by the devolved administrations.	https://covid19.public-inquiry.uk/