Bridgewater Community Healthcare NHS Foundation Trust

Records Management, Archiving, Retention and Disposal Policy

Policy Number	**IG/Pol/012**
Target Audience	**All Bridgewater Staff within the Trust, including Agency, Locum, Bank Workers, and Learners in Practice**
Lead Executive Director	**Chief Nurse as Caldicott Guardian**
Recommending Committee/Group	**DIGIT**
Approving Committee(s)	**Corporate Clinical Policy Group**
Ratifying Committee	**Trust Board**
Date First Ratified	**August 2018**
Last Full Review Date	**November 2023**
Next Full Review Date	**November 2025**
Lead Author(s)	**Information Governance and Records Manager and Senior Information Governance Officer**
Version Number	**3.0**

Applicable Statutory, Legal or National Best Practice Requirements	Central Digital and Data Office (2017) Use cloud first guidance Data Protection Act 2018, c.12 Department for Digital, Culture, Media & Sport (2012) Instrument for the Retention of Public Records Department of Health and Social Care (2017) Data security and protection for health and care organisations Department of Health and Social Care (2016) Records management: code of practice for health and social care Department of Health Informatics Directorate (2011) Guidance: digital document scanning [Gender Recognition Act 2004 c.7 Information Governance Alliance (2016) Records management code of practice for health and social care 2016 National Data Guardian (2020) The Caldicott Principles NHS Digital (2022) NHSmail: Data Retention and Information Management Policy NHS England - Transformation Directorate - Records Management Code of Practice (2021, updated 2023)

	NHS England (2021) Records Management Code of Practice The National Archives Guidance (2015) Cloud Storage and Digital Preservation, UK GDPR Advisor (2021) UK General Data Protection Regulation (GDPR)

The Trust is committed to an environment that promotes equality, embraces diversity, and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the Trust's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Version Control Sheet

Version	Date	Reviewed By	Comment
1.0	15/2/18 9/8/18 August 2018 August 2018	Sharon Ramsdale Policy Approval Group S. Ramsdale S. Arkwright	Changed to policy, total rewrite. Previous document: Storage, Retrieval and Destruction of Health Records Standard Operating Procedure Approved subject to minor amendments and chair approval Amendments completed, references updated, submitted for chair approval Approved by chair action
2.0	Oct 2021 Nov 2021 Dec 2021 3rd February 2022	J. McKay Sharon Ramsdale Corporate Clinical Policy Group Trust Board (e-governance)	Full review, updates made Approved by DIGIT Approved, submitted for ratification by the Trust Board Ratified – Policy Officer notified 28/02/2022
2.1	October 2023	DIGIT	Full review, updates made – signed off
2.2	October 2023	M. Corkery	Reviewed, comments made
2.3	November 23	Corporate Clinical Policy Group	Approved subject to amendments and final chair approval
2.4	December 23	J. McKay	Amendments completed
3.0	December 23	J. Cheung	Approved by chair action

Equality impact assessment

Consider if this document impacts/potentially impacts:

- Staff
- Patients
- Family members
- Carers
- Communities

Yes [x] **complete box A**	**No** [ ] **complete box B**
Box A Contact the Trust's equality & inclusion manager at: **Email: ruth.besford@nhs.net** **Date contacted: 25.10.21**	**Box B** Complete details below: **Name:** **Email:** **Date:**

Education & Professional Development Question

To ensure that any training requirements are discussed, and resources planned and allocated to meet the needs of the service, you must consider whether this document has additional training requirements. Please answer the following question by entering a cross in the Yes or No box below:

	Yes	**No**
Does this document have any additional training requirements or implications?		X

If you have answered **YES** you must forward a copy of this document to Education & Professional Development **before** submitting to the Policy Officer.

Date submitted to Educations & Professional Development: ……

No further action is required if you have answered NO.

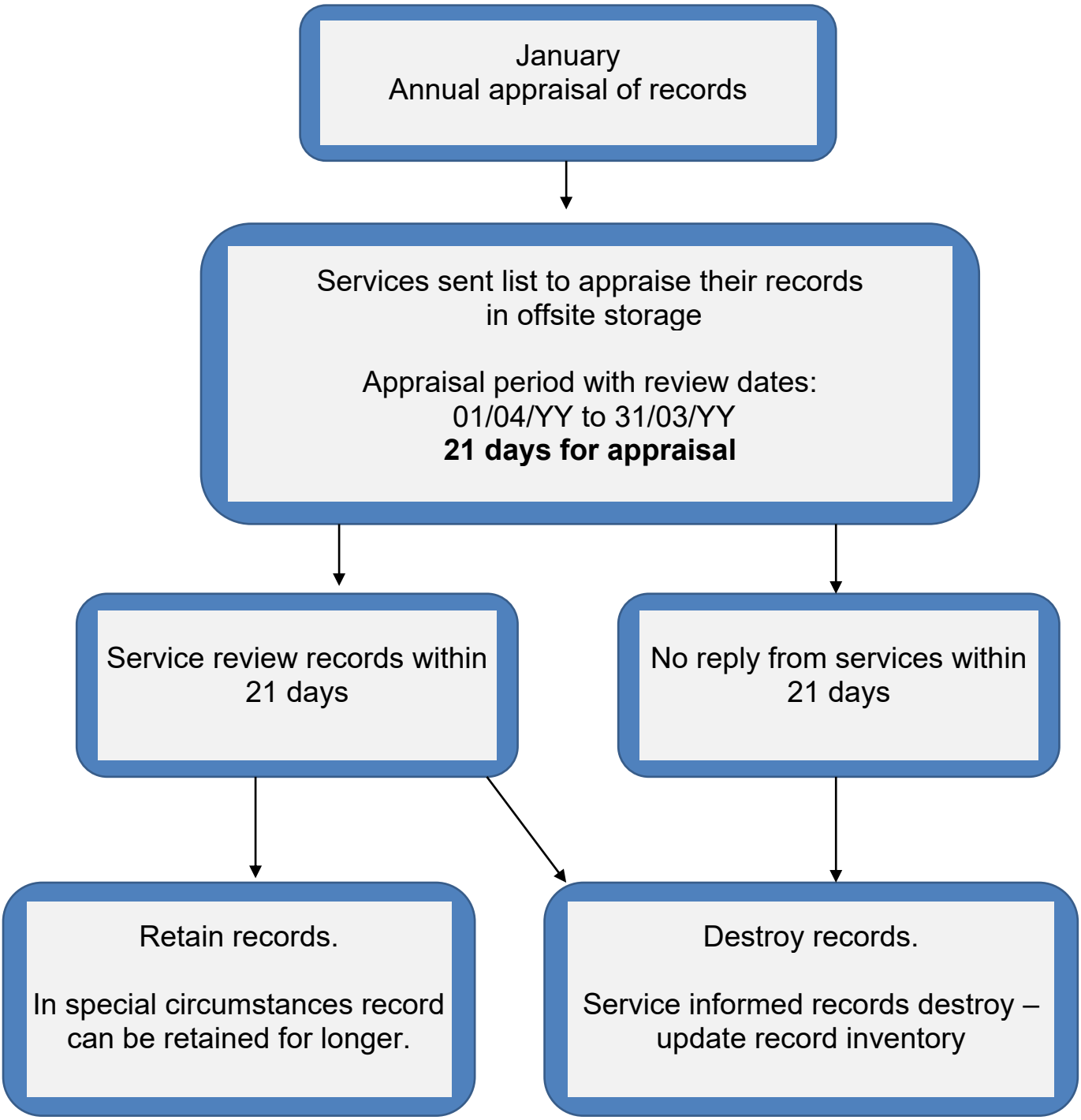
This table below must be completed in full for audit and governance purposes. Please note documents will be returned if section 1 in the table below is not completed fully. This will result in a delay in listing the document for approval.

Name of document	Records Management, Archiving, Retention and Disposal Policy
Document number	IG/Pol/012
Document author	Jackie McKay

Section 1 - actions required by author	**Authors response**
Date proposal form submitted to policy officer (new documents)	N/A
Date proposal form presented to CCPG (new documents)	N/A
Date proposal approved by CCPG (new documents)	N/A
Date literature search/reference review requested	N/A
Date EqIA considered	October 23
Date additional training requirements considered	N/A
Date fraud-proofed by the Anti-Fraud Specialist (AFS) if applicable	N/A
Date template accessed on the Hub Add 'OFFICIALSENSITIVE: COMMERCIAL' to front cover if the document can be shared on the internet Add 'OFFICIALSENSITIVE: PERSONAL' to appendices if they include or will include personally identifiable information (PID)	October 23
Date literature review completed (check references are formatted correctly, and hyperlinks working)	N/A
Date first draft submitted to policy officer for initial review	5th October 23
Date returned by policy officer following initial review	5th October 23
Date submitted to key individuals/groups/subject matter experts for comments (add names and designations of responders to consultation table)	October 23
For clinical documents, date document submitted to consultation group for sign-off i.e., IPC, Medicines Management (this applies if the document contains medication or medical gases - update version control sheet to confirm sign-off)	N/A
Name of Recommending Committee/group	DIGIT
Date sent to Recommending Committee/group for sign-off	October 23
Date signed-off by the Recommending Committee/group (update version control sheet once signed-off)	October 23
Date submitted to policy officer for listing at CCPG	7/11/23
Section 2 – for completion by the policy officer	
Date approved by CCPG	13th November 2023
The following policies require Board approval and must be submitted to Board following CCPG approval: • Risk Management Framework Policy • Health & Safety Policy • Policy and procedure for the production, approval and ratification of Trust-wide policies and procedures ("Policy for Policies") Date submitted for Board approval: Date approved by Board:	N/A

Contents

Appraisal process flowchart

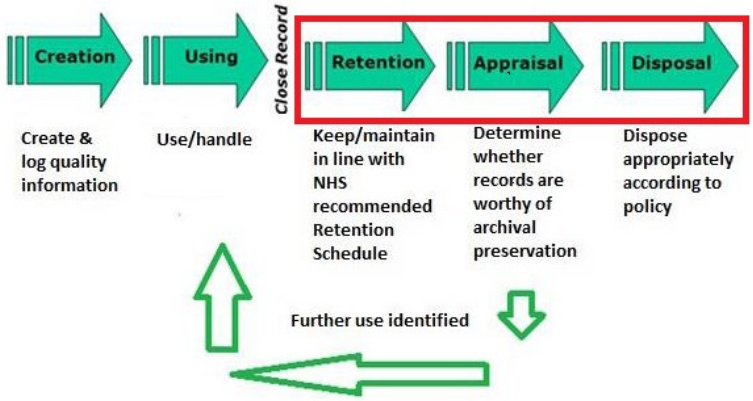


1 Introduction

This policy applies to all records (corporate and health records) paper or electronic, that are held by Bridgewater Community Health NHS Foundation Trust (hereafter the Trust). The aim of this policy is to ensure uniformity across the organisation, and to ensure that records management practice throughout the Trust complies with relevant legislation and national standards.

This policy sets out a framework for when a record is appraised and deemed "closed" or no longer "active" following its creation and use; this can be seen in the diagram below.

Records/Information Lifecycle – Figure 1"



The Trusts Health Records Policy and the Corporate Records (including Document Management) Policy has clear definitions on what constitutes a record, these policies also covers the creation and use of a record. The handling and movement of records can be found in the other record management policies listed below (see section 4).

This policy sets a standard framework for those who have been delegated responsibility for records management within the Trust. This policy is based on NHS England 'The Records Management Code of Practice' first published in August 2021 and updated August 2023

This policy applies to all records created, received, and maintained by all personnel working, commissioned or acting on behalf of the trust in the course of their work for and on behalf of the Trust and applies regardless of location of working environment, i.e., Trust premises, at home or elsewhere. The retention requirements listed within this policy apply to all records irrespective of media and format, or the system(s) in which the records are held.

1.1 Objective

To ensure staff responsible for implementing this policy, have a robust framework to enable them to develop local non-clinical standard operating procedures (LNCSOPs) within their service.

1.2 Scope

This policy applies to all Trust staff, including agency, locum, bank workers, and learners in practice.

2 Definitions

The definitions applicable to this document are as follows:

Appraisal	To review the record when it is deemed "closed" or no longer "active".
Archivers	The name given to nominated personnel within the Trust with the responsibility to deem when a record, can be placed in retention on the offsite storage facility.
Corporate records	Administration records relating to all functions of the Trust.
Deep store	A records management company holding historical records from Halton and St Helens. No new archiving.
Disposal / destruction	Permanent removal or destroying of the record. This has to meet NHS standards and applies to paper and electronic records. This is now undertaken by outside contractors and can only be done by nominated personnel within the Trust.
Data Protection Act (DPA) 2018	The DPA 2018 sets out the framework for data protection law in the UK.
Data Security and Protection Toolkit (DSPT)	An online self-assessment tool that allows organisations to measure their performance against the 10 data security standards.
Iron Mountain	A records management company holding historical records from Warrington. No new archiving.
Log	Detailed list of an application information, system performance, or user activities used within IT.
NHS England Records Management Code of Practice A guide to the management of health and care records	The Records management: code of practice for Health and Social Care (August 2021 updated August 2023) is a guide for staff to use in relation to the practice of managing records.
NHS England	NHS England supports local integrated care systems (ICS), made up of public services that provide health and care – NHS organisations, primary care professionals, local councils, social care providers and the community, voluntary and social enterprise sector.

NHS England - Transformation Directorate	Formerly NHSX responsible for driving the digital transformation of the NHS and social care.
Record	Any record held the NHS as a public body organisation, regardless of the media on which they are held. This includes health records, records of staff, complaints, corporate records, and any other records held in any format including both paper and digital records. The guidelines also apply to adult social care records where these are integrated with NHS patient records
Remote working	Remote work is the practice of employees doing their jobs from a location other than a central office operated by the employer. Such locations could include an employee's home
Retention / place of deposit	Records for (which) are held before destruction to support reasonably foreseeable litigation, public inquiries, an on-going Freedom of Information (FOI) request or similar exceptional statutory reasons, such as a public inquiry.
Retention schedule	The retention schedule (appendix 1) lists those records which should as a minimum be selected for transfer to a place of deposit.
Restore	A records management company currently contracted to manage the storage (place of deposit) and destruction of paper records as of 1st of April 2017.
Transgender	People have a gender identity or gender expression that differs from the sex that they were assigned at birth.
United Kingdom General Data Protection Regulation (GDPR)	UK GDPR formerly GDPR 2018 is a regulation by which the European Parliament, the Council of the European Union and the European Commission strengthened to unify data protection for all individuals within the European Union (EU). The 'UK GDPR' sits alongside an amended version of the DPA 2018.

3 Abbreviations

The abbreviations applicable to this document are as follows:

BSA	Business Services Authority
CEO	Chief Executive Officer
CCTV	Closed-Circuit Television
CJD	Creutzfeldt-Jakob Disease

CQC	Care Quality Commission
DN	District Nurse
DPA	Data Protection Act
DPO	Data Protection Officer
DSPT	Data Security and Protection Toolkit
EPR	Electronic Patient Record
EU	European Union
FOI	Freedom of Information
GP	General Practitioner
GUM	Genito-Urinary Medicine
HFEA	Human Fertilisation and Embryology Authority
HR	Human Resources
HSCIC	Health and Social Care Information Centre
ICO	Information Commissioner's Office
IG	Information Governance
IGA	Information Governance Alliance
IT	Information Technology
LNCSOP	Local-Non Clinical Standard Operating Procedure
MEP	Medicines, Ethics and Practice
MHRC	Medicines and Healthcare products Regulatory Agency
NHS	National Health Service
NHX	NHS Transformation Directorate
PHM	Population Health Management
PFI	Private Finance Initiative
SIRO	Senior Information Risk Owner
SAR	Subject Access Request
UKGDPR	United Kingdom General Data Protection Regulation
YY	Year

4 Other relevant procedural documents

This policy should be read in conjunction with the following documents:

Access to Records Policy

Complaints, Compliments, Comments & Concerns Handling of Policy

Equality Impact Assessment Policy

Corporate Records Management Policy

Data Protection and Confidentiality Policy

Disciplinary Policy and Procedure

Flexible Working Policy

Health Records Policy

Information Asset & System Audit Policy

Information Governance Framework Policy

Policy and Procedure for the Development and Review of Policy and Procedural Documents

5 Roles and responsibilities

5.1 Chief executive officer

The chief executive officer (accountable officer) has ultimate responsibility for the implementation of the provisions of this policy.

The Accountable Officer is responsible for the management of the organisation and for ensuring that appropriate mechanisms are in place to support service delivery and continuity.

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

5.2 Chief nurse and deputy CEO/Caldicott guardian

The chief nurse is the Trust Caldicott guardian and is responsible for the confidentiality of person identifiable information as designated in the Caldicott report and for the information governance agenda which incorporates data protection legislation, ensuring patient identifiable information is shared in an appropriate and secure manner according to the eight Caldicott principles (National Data Guardian, 2020).

5.3 Senior information risk owner

The senior information risk owner (SIRO) is currently the director of finance and is responsible for information risk throughout the organisation and has overall responsibility for implementing records management. The SIRO should have overall ownership of the organisation's information risks and risk management strategy and processes within the trust and advise the board on the effectiveness of information risk management across the Trust.

The SIRO will provide an essential role in ensuring that identified information security risks are followed up and incidents managed.

5.4 Data protection officer

The data protection officer (DPO) is currently the trust secretary.

The DPO has responsibility to ensure that the company or organisation is correctly protecting individuals' personal data according to current legislation.

The DPO must have expert knowledge of data protection law and practices and the ability to acquire detailed understanding of the organisation's business, the purposes for which it processes, or intends to process personal data.

5.5 Information governance and records manager

The information governance and records manager is responsible for ensuring that the Trust is working within all the legal frameworks in relation to handing information, specifically focusing on data protection.

The Information Governance and Records Manager is responsible for ensuring that this policy is implemented and that the records management system and robust data quality processes are developed, co-ordinated and monitored and will advise staff on records management issues.

5.6 Associate borough directors

Associate borough directors will be accountable for ensuring that all corporate policies, procedures and guidelines are fully implemented and approved within their directorate. This includes the responsibility for health records management outlined in the policy, making them the accountable record managers.

5.7 Heads of departments/operation managers/team leaders

Heads of departments/operation managers/Team Leaders are responsible for ensuring this policy is implemented across their area of their managerial responsibility and ensure that:

- Their staff are aware of and comply with this policy
- Ensure there is a service LNCSOP to support this policy
- Appoint a designated person for each location to ensure archiving is managed appropriately.

5.8 Information governance team

The Information Governance (IG) team are responsible for:

- Creating policies that govern the Trusts data management practices
- Ensure compliance with data privacy regulations

- Stay up to date with records management laws and policies
- Undertake risk assessments to ensure the Trust data security and protection risks are mitigated
- Submit and meet the standards of the data security and protection toolkit (DSPT) annually
- Advise the Trust and its staff on all data protection functions.

5.9 Staff

All staff has a duty to read and work within agreed policies, procedures and guidelines and to ensure that they keep themselves up to date with all procedural documentation.

Staff must ensure that they are aware of the location of procedural documents and how to access them on the Trust intranet site.

5.10 Digital information governance and information technology group

The Digital Information Governance and Information Technology Group (DIGIT) ensures the Trust operates within the Information Governance framework and monitors compliance with this policy regarding corporate records.

5.11 Patient services

The Patient Services department are responsible for managing, holding and retaining complaints records within the Trust as per this policy.

6 Equipment

Not applicable.

7 Complaints records

“Where a patient or client complains about a service, it is necessary to keep a separate file relating to the complaint and subsequent investigation. Complaint information should never be recorded in the clinical record. A complaint may be unfounded or involve third parties and the inclusion of that information in the clinical 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 and the health care team.” (NHS England – Transformation Directorate, 2021).

8 Retention

The retention schedule relates to each record type for both corporate and health records. All services need to adhere to the retention schedule.

The retention schedule can be accessed electronically by clicking on the following NHS England link:

https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice/#appendix-ii-retention-schedule

It is advised that the schedule is reviewed and a LNCSOP is developed to fit the retention schedule; this will be based on record type.

The following should be considered when developing a LNCSOP:

- Certain health records have non-standard retention periods and are based on diagnosis; these need to be considered as the changes could affect the retention time period

- Before closing a record where a service has hybrid records (electronic and paper) all paper documents produced since moving to an electronic patient record (EPR) should be scanned onto the electronic system. Once staff are assured of the the integrity of the scanned documents the paperwork can be destroyed as it is now a duplicate (NHS England: Records Management Code of Practice, 2021).

- Review what records must not be destroyed because of an ongoing public enquiry. The IG team can advise.

Note: In those services who have moved from paper to fully EPR, the EPR should state a paper record exists prior to this record, and that the paper record needs to be managed according to this policy.

It can be difficult to categorise staff training records to determine retention requirements but keeping all for the same length of time is also hard to justify.

8.1 Staff record

Upon termination of contract (for whatever reason), records must be held up to and beyond the statutory retirement age. Staff records may be retained beyond 20 years if they continue to be required for NHS or organisational business purposes, in accordance with Retention Instrument 122 (Department for Digital, Culture, Media & Sport, 2012). Where there is justification for long retention periods or protection is provided by the Code, this will not be in breach of GDPR Principle 5 (DPA, 2018).

Where an organisation decides to use a summary in a staff record, it must contain as a minimum:

- A summary of the employment history with dates
- Pension information including eligibility
- Any work-related injury
- Any exposure to asbestos, radiation and other chemicals which may cause illness in later life

- Professional training history and professional qualifications related to the delivery of care
- List of buildings where the member of staff worked, and the dates worked in each location.

NHS Trust staff record summary should also contain the following fields:

- Name
- Previous names
- Assignment number
- Pay bands
- Date of birth
- Addresses
- Positions held
- Start and end dates
- Reasons for leaving
- Building or sites worked at

Disciplinary case files should be held in a separate file so they can be expired at the appropriate time and do not clutter up the main file. That does not mean that there should be no record that the disciplinary process has been engaged in the main record, as it may be pertinent to have an indication to the disciplinary case, but the full details and file must be kept separately from the main file.

8.2 Staff training records

It is recommended (NHS England: Transformation Directorate, 2021) that:

- Clinical training records are retained until 75th birthday or six years after the staff member leaves, whichever is the longer
- Statutory and mandatory training records are kept for ten years after training is completed
- Other training records are kept for six years after the training is completed.

9 Records - additional considerations

The service should not hold or store duplicate records for one person. This will also affect those on paper health records where a patient has a long-term condition or a recurring illness the service may want to hold the record on site or have a process where the record can be retrieved from storage to avoid duplication of records.

- 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.

- Records need to be available for audit purposes for the short term for health records, an example would be clinical audit or an investigation. A process needs to be adopted that allows the record to be available, before moving to the offsite store, which has a cost implication.

- All records must be stored securely until minimum retention periods have expired.

- Storage space is limited and can pose a fire hazard in certain areas; this should influence the scheduling being archived. Storing closed records on site should always be subject to a risk assessment.

- Under no circumstance should a paper health record or corporate record be stored remotely, for example in a home office where staff may work. All paper records must be stored on Trust premises or the Trust archiving solution, Restore.

- Under no circumstance should an electronic health record or corporate record be stored electronically on a staff members personal device.

9.1 Offsite storage for paper records

It is vital to highlight the importance of actively managing records stored offsite. Services must ensure:

- There is a full inventory of what is held offsite
- Retention periods are applied to each record
- A disposal log is kept
- There is evidence of secure disposal of records and information.

All requests for records retrieval from offsite storage must be undertaken via the online tools. Access to the online web tools can be arranged by contacting the IG team using the email address below:

bchft.recordsmanager@nhs.net

9.2 File/box pre-preparation for paper records

Once a decision has been made to move the records to the offsite storage company Restore, the records should be checked to ensure they meet the following requirements:

- Ensure the record clearly displays date of closure (date of discharge from service) and the date of review (the date that the record is due to be appraised before being destroyed)

- No loose papers, the records contents are to be secure

- The records are to be in a durable material; this means no plastic wallets/folders. When plastic wallets are used the ink sticks to the wallet over a period of time

- No lever arch files, as this takes up to much room in the storage box.

Request the number of boxes and labels required. Ensure the correct label is used:

Once the staff member is ready to complete the process, they must create a list of the records that will need to be retained in the service. The list must include the following:

Minimum requirements for each record
Unique label number (the one placed on the box; you will get this once you are inputting onto the tool)
Box number
NHS number
Full name
Date of birth
Date / year of closure / discharge
Date / year of review
Record type

The information in the table below is an example of the how the label should describe what is in the box.

Minimum requirements	Example 1 - district nurse (DN)	Example 2 - dental
Service	DN	Dental
Base (of service)	Spencer	Pemberton-Central
Record type	Adult	Adult
Description	Surname A-D	Surname A-D
Date / year of closure / discharge	1/1/2017 – 1/3/2017	1/1/2017 – 1/3/2017
Date / year of review	31/3/2025	31/3/2027

Example 1 (based on the above):

Description: DN/Spencer. Adult. Surname A-D.
Discgarged:1/1/17-1/3/17
Review date: 31/3/2025

Example 2 (based on the above):

Description: Dental/Pemberton-Central. Adult. Surname A-D.
Discharged: 1/1/2017 – 1/3/2017
Review date: 31/3/2027

10 Emails

NHS mail, which is used by the Trust, has its own Data Retention and Information Management Policy. The document defines the data retention and information management approach for the NHS mail service and the minimum retention periods for which data will be kept. It also provides a description of the types of data and the account management lifecycle (NHSmail: Data Retention and Information Management Policy, 2022)

Email is a communication tool and is not for storing records. Information saved in emails will automatically be deleted after two years according to the NHS mail Policy. It is therefore important that anything that requires storing in NHS mail is saved in a folder on the appropriate drive.

Please be aware that email can form part of a subject access request. If an email is retained for longer than necessary, they are subject to disclosure in a subject access request.

11 Integrated health and care records

When patients are at their most vulnerable, providing health and care professionals with access to their records allows them to understand their needs and make the best decisions with them, and for them.

An integrated health and care records is when:

- All organisations contribute to a single record, creating the only record for that patient or service user. Consideration must be given to how this is managed in practice (for example, some records will be retained for 8 years and some for 20 years, but they will look the same at face value) (retain for the longest specialty period involved)

- All organisations pool their records into a single place but keep a level of separation between each type of record (retain for each specialty as applicable - because they are not merged)

- All organisations keep their own records, but allow others to view their records, but not amend or add to (retain for each specialty as applicable - because they are not merged).

If any of our services are looking to create integrated records, they must enter a joint controller arrangement, which detail the purpose and method of integrated records. It should also set out how disputes between controllers may be resolved. Information materials for patient or service users must also reflect how their records are used. The IG team can support this.

Increasingly, where organisations are using an integrated record, the information contained within has the potential to be used for purposes other than individual care, such as Population Health Management (PHM) and should be included in the Joint Controller Agreement (NHS England – Transformation Directorate, 2021).

12 Cloud based storage

Use of cloud-based solutions for health and care is increasingly being considered and used as an alternative to manage large networks and infrastructure. NHS and care services have been given approval to use cloud-based solution, provided they follow published guidance from NHS Digital and information from the Central Digital and Data Office (2017).

Before any cloud-based solution is implemented there are a number of records considerations (The National Archives Guidance, 2015) that must be addressed as set out by The National Archives. The ICO has issued guidance on cloud storage. Organisations must complete a DPIA when considering using cloud solutions.

Another important consideration is that at some point, the service provider or solution will change, and it will be necessary to migrate all of the records, including all the formats, onto another solution. Whilst this may be technically challenging, it must be done, and contract provisions should be in place to do this.

Records in cloud storage must be managed just as records must be in any other environment and the temptation to use ever-increasing storage instead of good records management will not meet the records management recommendations of this Code. For example, if digital health and care records are uploaded to cloud storage for the duration of their retention period, then they must contain enough metadata to be able to be retrieved and a retention date applied so it can be reviewed and actioned in good time.

Personal data that is stored in the cloud, and then left, risks breaching UK GDPR by being kept longer than necessary. This information would also be subject to subject access process, and if not found or left unfound, would be a breach of the patient or service user's rights.

13 Transgender records

Sometimes patients change their gender and part of this may include medical care. Records relating to these patients or service users are often seen as more sensitive than other types of medical records. While all health and care records are subject to confidentiality restrictions, there are specific controls for information relating to patients or service users with a Gender Recognition Certificate.

Transgender personal information can only be disclosed if explicit consent from the patient has been given unless there is a legitimate reason to do so under DPA 2018. Before disclosing any information, advice from the IG team should be sought:

Bchft.IG@nhs.net

The use and disclosure of the information contained in these records is subject to the Gender Recognition Act (GRA) 2004, which details specific restrictions and controls for these records.

14 Pandemic records

Health and care organisations will create records as part of a response to a global pandemic. Pandemic events are rare but will nevertheless create records that need to be managed.

Both patient and service user records will be created that detail the care given to people affected by the pandemic. Corporate records will also be created which record business decisions, policies and processes that were taken in response to a pandemic.

These records should be managed in accordance with the retention schedules set out in this Code. Organisations should be mindful that a public inquiry (or inquiries) is likely to take place after a pandemic so the pandemic related records could be used or requested as part of that Inquiry. The Government has already agreed to hold a public inquiry into the coronavirus pandemic that began in 2020.

If organisations have created records specifically in response to a pandemic, these should not be destroyed when they have reached their minimum retention period, unless the public inquiry has ended, or the Inquiry has provided guidance on what type of records it will be interested in.

For example, a policy on how to manage a new admission to a care home of an individual with a coronavirus diagnosis may be of interest to the Public Health England, whereas the care record might not have the same value and should be managed as a health and care record.

15 Public enquiries

Future public inquiries may lead to specific records management requirements, for example extending the retention period. Where that happens, services will be informed by the appropriately, and guidance issued.

16 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.

Records can possess different types or degrees of value and these values affect how records are managed and how long they need to be kept.

There will be one of three outcomes from appraisal:

- Destroy or delete
- Continued retention – this will require justification and documented reasons
- Permanent preservation.

The following factors should be considered when appraising patient records:

- The organisation has an unusually long or complete run of records of a given type
- The records relate to population or environmental factors peculiar to the locality
- The records are likely to support research into rare or long-term conditions
- The records relate to an event or issue of significant local or national importance (for example a public inquiry or a major incident)
- The records relate to the development of new or unusual treatments or approaches to care and/or the organisation is recognised as a national or international leader in the field of medicine concerned
- The records throw particular light on the functioning, or failure, of the organisation, or the NHS in general
- The records relate to a significant piece of published research.

Once records meet the review date (review before destruction) the service will be asked to appraise the records before they are destroyed. Appendix 1 shows the process and timescales.

Final authority to permanently destroy will be granted by the information governance and records manager, who will retain the certificates of destruction.

Note: the service needs to consider how they are going to destroy all information at this point relating to the record that they may hold on secondary systems, for example information regarding equipment allocated, emails and storage discs.

17 Consultation

Key individuals/groups involved in the development of the policy to ensure it is fit for purpose once approved:

Name	Designation
Ruth Besford	Equality and Inclusion Manager
Razia Nazir	Knowledge and Library Service Manager
Mary Corkery	Policy Officer
Digital, Information Governance and Information Technology Group (DIGIT)	
John Morris	Deputy Director of Finance
Tania Strong	Human Resources
Hitesh Chandarana	Head of Patient Experience
Val Harper	Complaints Manager
Corporate Clinical Policy Group	

18 Dissemination and Implementation

18.1 Dissemination

The IG team will disseminate this policy to associate borough directors for disseminating to staff via team meetings.

The policy will be made available on the Trust intranet and published in the team brief.

18.2 Implementation

Operational managers will ensure staff work to this policy.

All Trust staff will be made aware of their personal and organisational responsibilities regarding handling of NHS confidential records, through the Trust training program, and local induction and monitoring audits.

New employees will be made aware of this policy through the local Induction process.

19 Process for monitoring compliance and effectiveness

Process for reviewing compliance and effectiveness i.e., audit, review, survey, incident reporting	Responsible	Frequency of monitoring	Assurance Group
Audit	Information governance and records manager	Annually	DIGIT
DSPT	Information governance and records manager	Annually	DIGIT

The core aspects outlined within the policy are monitored through the Trusts corporate records audit.

Examples of the monitoring requirements are the annual DSPT submission, commissioning requested information both for performance and quality aspects and national and local clinical audits.

As requirements contained in this policy form one part of regulative requirements, for example Care Quality Commission (CQC) and professional bodies, failure to comply will be seen as an incident and upon investigation may lead to disciplinary and/or legal action in line with Human Resources (HR) policies and procedures by the Trust.

20 Standards/key performance indicators

Key Performance Indicator	Evidence required	Frequency	Committee/ person responsible
Annual audit report, that shows compliance to the core aspects within this policy	Report, submitted DIGIT	Annual	Information Governance and Records Manager
Incidents or issues relating to corporate records	Minutes from DIGIT	Quarterly	Information Governance and Records Manager
Destruction of records process	Audit trail and certificates	Annually	Information Governance and Records Manager

21 References

Central Digital and Data Office (2017) Use cloud first guidance [online]. Available at: https://www.gov.uk/guidance/use-cloud-first

Data Protection Act 2018, c.12 [online]. Available at: http://www.legislation.gov.uk/ukpga/2018/12/contents

Data Security and Protection Toolkit updated September 2023 (DSPT) [online]. Available at: https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides

Department for Digital, Culture, Media & Sport (2012) Instrument for the Retention of Public Records [online]. Available at: https://www.gov.uk/government/publications/signed-instrument-for-the-retention-of-public-records

Department of Health and Social Care (2017) Data security and protection for health and care organisations [online]. Available at: https://www.gov.uk/government/publications/data-security-and-protection-for-health-and-care-organisations

Department of Health Informatics Directorate (2011) Guidance: digital document scanning [online]. Available at: https://www.igt.hscic.gov.uk/WhatsNewDocuments/NHS%20IG%20guidance%20-%20Document%20Scanning%20V1%202011.pdf

European Commission (no date) Reform of EU data protection rules [online]. Available at: https://ec.europa.eu/info/law/law-topic/data-protection/reform_en.

Gender Recognition Act 2004 c.7 [online] Available at: https://www.legislation.gov.uk/ukpga/2004/7/contents

Information Commissioner's Office [webpage] Cloud computing [online]. Available at: https://ico.org.uk/for-the-public/online/cloud-computing/

Information Governance Alliance (2016) Records management code of practice for health and social care 2016 [online]. Available at: https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016

National Data Guardian (2020) The Caldicott Principles [online]. Available at: https://www.gov.uk/government/publications/the-caldicott-principles

NHS Digital [webpage] NHS and social care data: off-shoring and the use of public cloud services [online]. Available at: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/nhs-and-social-care-data-off-shoring-and-the-use-of-public-cloud-services

NHS Digital (November 2022) NHSmail: Data Retention and Information Management Policy version 10 [online]. Available at: https://comms-mat.s3.eu-west-1.amazonaws.com/Comms-Archive/NHS+Digital+Policy+Docs/NHSmail+Data+Retention+and+Information+Management+Policy.pdf

NHS England (no date) NHS standard contract [online]. Available at: https://www.england.nhs.uk/nhs-standard-contract/

NHS England Records Management Code of Practice A guide to the management of health and care records August 2021 updated august 2023 [online]. Available at: https://transform.england.nhs.uk/media/documents/NHSE_Records_Management_CoP_2023_V5.pdf

The National Archives Guidance (2015) Cloud Storage and Digital Preservation, Second edition [online]. Available at: https://cdn.nationalarchives.gov.uk/documents/CloudStorage-Guidance_March-2015.pdf

UK GDPR Advisor (2021) UK General Data Protection Regulation (GDPR) [online]. Available at: UK GDPR Updated for Brexit | UK GDPR (uk-gdpr.org)