Torbay and South Devon
NHS Foundation Trust

Health (and Adult Social Care) Records Management Policy

Document Information

This is a controlled document. It should not be altered in any way without the express permission of the author or their representative. On receipt of a new version, please destroy all previous versions.

Date of Issue:	April 2026	Next Review Date:	April 2027
Version:	1	Last Review Date:	April 2026
Author:	Information Governance Officer		
Director Responsible	Chief Nurse		
Approval Route			
Approved By:		**Date Approved:**	
Records Management Oversight Group		April 2026	
Links or overlaps with other policies:			
We are committed to preventing discrimination, valuing diversity and achieving equality of opportunity. No person (staff, patient or public) will receive less favourable treatment on the grounds of the nine protected characteristics (as governed by the Equality Act 2010): Sexual Orientation; Gender; Age; Gender Reassignment; Pregnancy and Maternity; Disability; Religion or Belief; Race; Marriage and Civil Partnership. In addition to these nine, the Trust will not discriminate on the grounds of domestic circumstances, social-economic status, political affiliation or trade union membership. We are committed to ensuring all services, policies, projects and strategies undergo equality analysis. For more information about equality analysis and Equality Impact Assessments please refer to the Equality and Diversity Policy.			

Amendment History

Issue	Status	Date	Reason for Change	Authorised
1	Final	April 2026		Information Governance Operational Group

Contents

1. Introduction ... 4
2 Purpose ... 4
3 Responsibilities ... 4
4 Definitions ... 6
5 Legal and Professional Obligations ... 7
6 Record Creation ... 8
7 Minimum Standards for Record Keeping ... 8
8 Record Retrieval and Storage ... 9
9 Record retention ... 11
10 Record appraisal ... 12
11 Record disposal ... 13
12 Destruction of records ... 13
13 Key Contacts ... 14
Appendices ... 15
Appendix 1: Rapid Equality Impact Assessment ... 15

1. Introduction

1.1 Health Records (including Adult Social Care) function as the Trust's clinical memory, providing evidence of actions and decisions and supporting consistency, continuity, efficiency and equity in the delivery of care to patients and service users. They also help in policy formation and in protecting the interests of the Trust as well as the rights of patients, staff and members of the public, including patients' right of access to data held about them.

1.2 The aim of this policy is to ensure the Trust creates, accesses, manages and disposes of health records in accordance with national standards, and professional accountability; and are compliant with legal, operational and information governance requirements.

1.3 The Trust must conform to several legislative requirements, regulations, and standards that outlines the management of records.

1.4 Health records are an integral part of the care provided which is generated on, or on behalf of, all employees involved in care. These records need to be accessed by the various employees involved in care delivery.

2 Purpose

2.1 The aim of this policy is to ensure that all health records generated by employees are contemporaneous, accurately reflect high standard care and support the delivery of evidence-based practice. This policy outlines the roles, responsibilities, and accountability of Trust employees in complying with guidance, legislation, and best practice for keeping records.

2.2 The health records policy governs all aspects of the information lifecycle including:

- record creation.
- record retrieval and location.
- record security and storage.
- record maintenance.
- tracking and transportation
- retention, disposal and destruction
- updating and redacting information in records

2.3 Where specialty areas develop additional local procedures then they must fully comply with the requirements of this policy and its supporting procedures.

3 Responsibilities

3.1 The Chief Executive Officer - The Chief Executive has overall accountability and responsibility for healthcare records within the trust. This function is delegated to the Data Protection Officer who is responsible for driving high quality standards of healthcare record keeping.

3.2 Senior Information Risk Officer (SIRO) – The SIRO is member of the Trust Board and is responsible for ensuring that organisational information risks are properly identified, managed, and that appropriate assurance mechanisms exist.

3.3 Data Protection Officer – The DPO reports direct to the Board on privacy issues and will provide reports where risks to the privacy of individuals have been highlighted. The DPO provides reports to the Information Governance Steering Group (IGSG) which is chaired by the Trust's Senior Information Risk Officer. The DPO also provides operational management of all health and social care records within the Trust.

3.4 Caldicott Guardian – All NHS organisations are required to appoint a Caldicott Guardian whose role is to govern the protection and use of patient-identifiable information. Upholding the Caldicott Principles, the Caldicott Guardian can provide assurances relating to the ethical use of patient information.

3.5 Senior Managers – Senior Managers hold responsibilities for managing records within or traced to their department, they oversee these records locally ensuring they are appropriately managed, maintained and accessed in accordance with Trust's policies.

3.6 Health Records Practice Manager – The Records Management Team oversee the availability, integrity and confidentiality of physical health records, and manage the Medical Records Library.

3.7 Health Records Governance Coordinator – The Governance Coordinator looks after the Trust's health records. They ensure that records are stored appropriately and retained for the duration of the information lifecycle. They also ensure that information is securely destroyed when it reaches the end of its retention period.

3.8 Information Governance – The IG Team look after all queries and concerns relating to information and data held by the Trust. This can include supporting any advice or enquiries; managing data related incidents or complaints; supporting with projects which collect, use or share data; reviewing contracts and helping complete the legal requirements relating to information management.

3.9 All employees – All employees of the trust are responsible for any records

which they create or use. This responsibility is established at, and defined by, the Public Records Act (1958). As an employee of the NHS any records created by an employee are public records. All employees must adhere to the relevant trust record keeping and records management policies. In addition, all employees have a professional responsibility and accountability to comply with record keeping standards and protocols specific to their professional codes of conduct or practice.

4 Definitions

4.1 Health Records – a collection of a patient's medical information, including their history, diagnoses, medications, and test results. This also includes social care records.

4.2 Section 205 of the Data Protection Act 2018 defines a health record as a record which:

- Consists of data concerning health
- Has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates.

4.3 Within the Trust, health records will include:

- Records of NHS patients receiving treatment by the Trust and records relating to private patients receiving treatment on Trust premises
- Registers - for example, birth, death, Accident and Emergency, theatre, minor operations
- X-ray and imaging reports, output and images

4.4 Examples of records formats that will be considered as part of the health record if relating to the above include:

- Digital records
- Paper records
- Photographs
- Microfiche and Microfilm
- Physical records (such as plaster, gypsum or alginate moulds)
- Audio and video recordings
- Emails, text messages and correspondence
- Digitised records (Scans or computerised)

4.5 ‘Core Systems’ - The Trust operates core health record systems. Outputs from the core systems form the primary patient record.

4.6 All systems for recording health information must be registered on the Trust’s Information Asset Register in order for the Trust to fulfil its legal and regulatory obligations.

4.7 Personal data is defined as data relating to an individual that enables any person to be identified either from that data alone or from that data in conjunction with other information in the data controller's possession. It therefore includes such items of information as an individual's name, address, age, race, religion, gender and physical, mental or sexual health.

4.8 Records Life Cycle describes the life of a record from its creation 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.

4.9 Transactional records are records that have only temporary value. They are produced in the completion of routine actions, in the preparation of other records that supersede them and / or for convenience of reference. They are NOT official copies of records which need to be retained as evidence of an activity, and they have no significant informational value after they have served their primary purpose.

5 Legal and Professional Obligations

5.1 All NHS records are Public Records under the Public Records Acts. The Senior Information Risk Owner will take actions as necessary to comply with the legal and professional obligations set out below:

- The Public Records Act 1958.
- Access to Health Records Act 1990
- The General Data Protection Regulation 2018
- Data Protection Act 2018
- Freedom of Information Act 2000
- Common Law Duty of Confidentiality; and The NHS Confidentiality Code of Practice.
- NHS Records Management code of practice
- International Standard ISO15489, Records Management
- Inquiries Act 2005
- NHS Act 2006

5.2 Many staff will also be obligated to follow standards set out by their regulatory bodies, including the General Medical Council, Nursing and Midwifery Council, General Pharmaceutical Council, and Health and Care Professionals Council.

5.3 All new starters to the Trust will undergo training, covering:

- Security
- Confidentiality
- Data protection
- Freedom of Information
- Information Governance

Annual refreshers of this training will be mandatory for all employees.

5.4 All employees will be aware of their responsibilities for record keeping and record management through training programmes, policy and guidance.

6 Record Creation

6.1 All areas should have processes for documenting its activities, taking into account the legislative and regulatory environment in which it operates. For example, theatres may require detailed documentation such as sign in / out sheets of a procedure to be created.

6.2 All records must be complete and accurate in order to:

- Allow staff to undertake appropriate actions in accordance with their responsibilities.
- Facilitate audits
- To protect the rights of the organisation, patients, staff and other persons

6.3 All records created should be catalogued including a reference identifier, title, protective maker.

6.4 All patient records must have a minimum of three patient identifiers, such as Name, Date of Birth and NHS / Hospital number.

6.5 Patients should only be registered with one NHS number. If patients are registered with multiple, please refer to the duplicate registration procedure.

6.5.1 If patients have multiple NHS numbers, please contact the Health Records Governance Coordinator.

7 Minimum Standards for Record Keeping

7.1 Failure to record information accurately in health records can have serious consequences for patients and their relatives. These failures may result in reduced quality of care and litigation. Poor record keeping is a factor in litigation cases brought against Trust and can hinder the defence of cases.

7.2 All patient contacts should be recorded legibly, accurately and contemporaneously. Each patient should be identified, and the notes should set out diagnosis, history, treatment, results and care plans in a format that promotes continuity of care.

7.3 Note Keeping audits should be carried out regularly to ensure areas for improvement are identified and standards are maintained. The Records Management Operational Group will advise where re-audits or additional

audits are required. These audits will be completed by Health Care Professionals.

7.4 Duplication of medical records should be avoided wherever possible, and one copy of clinical information retained.

8 Record Retrieval and Storage

8.1 Paper records storage and retrieval

8.1.1 All paper records must be stored in the Trust's Medical Records Library or approved archives unless required for legitimate purposes.

8.1.2 The movement and location of records must be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions.

8.1.3 Unavailability of paper records for clinic or inpatient attendance presents a clinical risk to the patient and therefore must be avoided wherever possible.

8.1.4 If tracering is unavailable the Health Records Department must be contacted, and Business Continuity Plans will be implemented in accordance with EPPR responses.

8.1.5 It is the responsibility of Managers to ensure their staff input the relevant paper records tracking information to maintain a comprehensive and up to date system. This includes keeping the details of current storage locations, including off-site storage.

8.1.6 Managers have full responsibility for ensuring that the list of storage locations associated with their area of work is reviewed and kept up to date.

8.2 Electronic records storage and retrieval

8.2.1 Where possible, electronic records management processes should be as environmentally friendly as possible to help contribute towards the NHS target to reduce its carbon footprint and environmental impact.

8.2.2 All electronic record systems which store health records must legal standards, including:

- BS 10008-2:2020 - Evidential weight and legal admissibility of electronically stored information (ESI)

8.2.3 All electronic records should be maintained and stored securely on approved systems within the Trust.

8.2.4 All electronic health record systems must be reviewed by Information Governance, Cyber Security and registered on the Trust's Information Asset Register, following SIRO approval. There must be a registered and appropriately trained Information Asset Owner.

8.2.5 Information Asset Owners should ensure they have a contingency or business continuity plan to provide protection for records which are vital to the continued functioning of the Trust's services.

8.2.6 Retrieval from electronic systems can take a variety of forms including download, print or extraction. The original data must be retained on the electronic system for the appropriate retention period and any copies maintained securely.

8.3 Sending paper records to other Trusts

8.3.1 Paper records must **not** be sent to any other organisation without prior approval from the Heath Records Department. In exceptional cases this is permitted but only if it is deemed to be a clinical risk to the patient, therefore, in all other circumstances please send photocopies / scans.

8.3.2 The following organisations have Trust approval to receive original paper records:

- Royal Devon University Healthcare NHS Foundation Trust (including North Devon District Hospital)
- University Plymouth Hospitals NHS Trust
- Nuffield Hospitals – Plymouth and Exeter
- Ramsey Healthcare – Mount Stuart Hospital
- HM Coroner's Offices – Torbay, Plymouth and Devon

8.3.3 Original paper records must be tracked to the receiving hospital and the tracking comments must include a contact number, name and location at the receiving hospital.

8.4 Missing / Mislaid paper records

8.4.1 A 'missing record' is defined as a record that cannot be located or is not available for patient consultation/inpatient stay or for other purposes, i.e. complaint/incident investigation.

8.4.2 All staff are responsible for the maintenance of comprehensive and orderly paper records whilst in their care. This means that all loose filing, nursing notes, discharge letters and reports must be filed inside the paper records folder, in the appropriate order at the point of care.

8.4.3 In the event of a missing paper records, the department/user where the

notes are currently tracked must make every effort to locate the record. When all efforts to locate the record have been exhausted, an incident form must be completed giving clear details of the actions undertaken.

8.5 Patient / Service user Held Records

8.5.1 Patient/service user held records have been introduced nationally to improve patient experience and outcomes with specific conditions

8.5.2 A patient/service user held records can range from a few documents and general information sheets to a folder, the records can be in paper or electronic format. The record is designed to be a supplement to the primary health record, managed by the Trust and Primary Care and to enable the patient to be informed and involved in their care, and to facilitate communication to different groups of people caring for the patient.

8.5.3 These types of records have proved to be valuable for certain groups of patients, namely:

- Those who visit the hospital frequently for a period e.g. Obstetric patient
- Those who are concerned with confidentiality and security e.g. HIV patients
- Those with long term or chronic conditions e.g. diabetes, sickle cell anaemia, MS, Cancer
- Patients/service users whose condition required care to be shared between the acute hospital and various primary/community care settings
- Community Nursing Complex Assessments
- Intermediate Care records
- Allied health professional records
- Multi-agency staff including those from the voluntary sector who contribute to patient/service user care

8.5.4 In all sections there should be space for date/time, name and signature of the person making the entry including their role or relationship to the patient/service user.

9 Record retention

9.1 All records should be retained for a minimum period as defined in the NHS Records Management Code of Practice, and TSDFT Retention and Destruction Schedule.

9.2 If the retention period detailed in the NHS Records Management Code of Practice and the TSDFT Retention and Destruction Schedule differ, the TSDFT Retention and Destruction Schedule should take precedence, and guidance should be sought from the Information Governance Team on tsdft.igteam@nhs.net

9.3 The recommended retention periods shown on NHS Records Management Code of Practice and TSDFT Retention and Disposal Schedule apply to the official or master copy of the Records. Any duplicates or local copies made for working purposes should be kept for as short a period as possible and securely destroyed.

10 Record appraisal

10.1 Before any health record is destroyed, it must be appraised for value.

10.2 A record appraisal will have one of three outcomes:

- Record held for ongoing use
  - Records may be held for continued use or within the Trust's archives.
  - Any records held in the Trust's archives must be appropriately inventoried. This will include:
    - details of the nature of the record
    - a unique box / reference number (barcoded boxes are available from the Medical Records Library)
    - any data subjects who the records pertain to
    - the original retention date
    - the appraisal date
    - the review date (for the records to be re-assessed)

- Records transferred for archiving
  - Records selected for archival preservation and no longer in regular use should be transferred to a 'Place of Deposit'. This must be approved by The National Archives and have adequate storage and public access facilities. For more information contact the Information Governance Team.
  - The Information Governance Team will liaise with The National Archives as appropriate to assist in the preparation and transfer of any records to the Place of Deposit.

- Record Destruction - Please refer to Section 12

10.3 From April 2026, all records held on Epic and the corresponding legacy systems are considered part of an integrated care record; and therefore, the retention of the latest specialty across all three Trust's will apply to the record.

10.4 An appraisal of health records must consider a number of questions. Please refer to the Health Records Appraisal Checklist found in the Health Records Procedures book.

10.5 All completed appraisals must be submitted to the Health Records Group for decision making and consideration for disposal.

11 Record disposal

11.1 Disposal is the implementation of appraisal and review decisions, and the term should not be confused with destruction. A review decision may result in the destruction of Records but may also result in the transfer of custody of Records, or movement of Records from one system to another. This could include from paper to microfilm/electronic system.

11.2 Records which have been appraised for disposal should be put to one side and clearly separated from records in active use; and retained for a minimum of 90 days.

12 Destruction of records

12.1 Destruction of paper records

12.1.1 If, because of appraisal, a decision is made to destroy or delete a record, there must be evidence of the decision, these are referred to as Certificates of Destruction.

12.1.2 If approval is given to destroy the records locally, a destruction certificate must be generated and submitted to the Health Records Team on the completion of the destruction.

12.1.3 Certificates of Destruction must contain the following information to provide clear evidence that specific records have been destroyed:

- Details of the nature of the record
- A unique box / reference number (barcoded boxes are available from the Medical Records Library)
- The original retention date
- The appraisal date
- The destruction date
- A signature of who approved the destruction
- A signature of who enacted the destruction

12.1.4 Destruction of any health records must be approved the Data Protection Officer or a delegated deputy.

12.1.5 If the Trust has contracted a third-party supplier to destroy the records, a destruction certificate will be provided to the Health Records Team on the completion of the destruction.

12.1.6 All contracted third-party destroyers of paper materials must be ISO15489-

1:2016 accredited.

12.2 Destruction of digital records

12.2.1 Destruction of digital records is the permanent action of removing information before the point of restoration.

12.2.2 Destruction of digital records is more challenging as deletion may not equate the permanent destruction of information. Therefore, the Trust must be assured that all ISO standards regarding IT systems are in place to enable appropriate destruction of digital information.

12.2.3 ISO 27001:2022 Annex A 7.14 states that two approaches can be taken to ensure secure and permanent erasure of information on equipment.

- Equipment that holds storage media devices that contain information should be physically destroyed.
- Annex A 7.10 and Annex A 8.10 concerning Storage Media and Information Deletion ensure all data stored on equipment is erased, overwritten or destroyed in a manner that precludes retrieval by malicious parties.

12.2.4 An electronic records system will retain a metadata stub which will show what has been destroyed. This will function as the certificate of destruction.

12.2.5 If a system doesn't allow permanent deletion, then all reasonable efforts must be made to remove the record from use. It should be marked in such a way that anyone accessing the record can recognise it as a dormant or archived record.

12.2.6 If deletion is not possible, the Information Governance Team should be alerted to the system and a risk reported.

13 Key Contacts

Department	Email	Telephone
Health Records	sdhis.recordsgovernance@nhs.net	01803 654343
Information Governance	tsdft.igteam@nhs.net	01803 654868
Data Access and Disclosure	dataprotection.tsdft@nhs.net	01803 654868
Cyber Security	sdhis.cybersecurity@nhs.net	0300 500 7000
Clinical Systems Administration Team	sdhis.dqia-requests@nhs.net	0300 500 7000

Appendices

Appendix 1: Rapid Equality Impact Assessment

Rapid Equality Impact Assessment *(for use when writing policies and procedures)*

<table>
<tr><td colspan="2">Policy Title (and number)</td><td>Health (and Adult Social Care) Records Policy</td><td colspan="2">Version and Date</td><td></td></tr>
<tr><td colspan="2">Policy Author</td><td colspan="4">Data Protection Officer</td></tr>
<tr><td colspan="6">An equality impact assessment (EIA) is a process designed to ensure that a policy, project or scheme does not discriminate or disadvantage people. EIAs also improve and promote equality. Consider the nature and extent of the impact, not the number of people affected.</td></tr>
<tr><td colspan="6">EQUALITY ANALYSIS: How well do people from protected groups fare in relation to the general population?
PLEASE NOTE: Any ‘Yes’ answers may trigger a full EIA and must be referred to the equality leads below</td></tr>
<tr><td colspan="6">Is it likely that the policy/procedure could treat people from protected groups less favorably than the general population? (see below)</td></tr>
<tr><td>Age</td><td>Yes ☐ No☒</td><td>Disability</td><td>Yes ☐ No☒</td><td>Sexual Orientation</td><td>Yes ☐ No☒</td></tr>
<tr><td>Race</td><td>Yes ☐ No☒</td><td>Gender</td><td>Yes ☐ No☒</td><td>Religion / Belief (non)</td><td>Yes ☐ No☒</td></tr>
<tr><td>Gender Reassignment</td><td>Yes ☐ No☒</td><td>Pregnancy / Maternity</td><td>Yes ☐ No☒</td><td>Marriage / Civil Partnership</td><td>Yes ☐ No☒</td></tr>
<tr><td colspan="5">Is it likely that the policy/procedure could affect particular ‘Inclusion Health’ groups less favourably than the general population? (substance misuse; teenage mums; carers[1]; travellers[2]; homeless[3]; convictions; social isolation[4]; refugees)</td><td>Yes ☐ No☒</td></tr>
<tr><td colspan="6">Please provide details for each protected group where you have indicated ‘Yes’.</td></tr>
<tr><td colspan="6">VISION AND VALUES: Policies must aim to remove unintentional barriers and promote inclusion</td></tr>
<tr><td colspan="5">Is inclusive language[5] used throughout?</td><td>Yes ☒ No☐</td></tr>
<tr><td colspan="5">Are the services outlined in the policy/procedure fully accessible[6]?</td><td>Yes ☒ No☐</td></tr>
<tr><td colspan="5">Does the policy/procedure encourage individualised and person-centred care?</td><td>Yes ☒ No☐</td></tr>
<tr><td colspan="5">Could there be an adverse impact on an individual’s independence or autonomy[7]?</td><td>Yes ☐ No☒</td></tr>
<tr><td colspan="6">If ‘Yes’, how will you mitigate this risk to ensure fair and equal access?</td></tr>
<tr><td colspan="6">EXTERNAL FACTORS</td></tr>
<tr><td colspan="5">Is the policy/procedure a result of national legislation which cannot be modified in any way?</td><td>Yes ☒ No☐</td></tr>
</table>

<table>
<tr><td colspan="4">What is the reason for writing this policy? (Is it a result in a change of legislation/ national research?)</td></tr>
<tr><td colspan="4">To facilitate a standardized approach to policy documents across the Trust</td></tr>
<tr><td colspan="4">Who was consulted when drafting this policy/procedure? What were the recommendations/suggestions?</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">ACTION PLAN: Please list all actions identified to address any impacts</td></tr>
<tr><td colspan="2">Action</td><td>Person responsible</td><td>Completion date</td></tr>
<tr><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="4">AUTHORISATION:
By signing below, I confirm that the named person responsible above is aware of the actions assigned to them</td></tr>
<tr><td>Name of person completing the form</td><td></td><td>Signature</td><td></td></tr>
<tr><td>Validated by (line manager)</td><td></td><td>Signature</td><td></td></tr>
</table>

Any issues Please contact Diversity & Inclusion Lead
For Torbay and South Devon NHS Trusts, please call 01803 656676 or email tsdft.diversityandinclusion@nhs.net

[1] Consider any additional needs of carers/ parents/ advocates etc, in addition to the service user.
[2] Travellers may not be registered with a GP - consider how they may access/ be aware of services available to them.
[3] Consider any provisions for those with no fixed abode, particularly relating to the impact on discharge.
[4] Consider how someone will be aware of (or access) a service if socially or geographically isolated.
[5] Language must be relevant and appropriate, for example referring to partners, not husbands or wives.
[6] Consider both physical access to services and how information/ communication is available in an accessible format.
[7] Example: a telephone-based service may discriminate against people who are d/Deaf. Whilst someone may be able to act on their behalf, this does not promote independence or autonomy.