


TRUST POLICY FOR RECORDS MANAGEMENT

Reference Number POL- RM/154/05	Version: 8	Status: FINAL	Author: Emily Griffiths Job Title: Head of Information Governance/DPO	
Version / Amendment History	Version	Date	Author	Reason
	1 – 6	August 2005 – April 2008	A Brown	Amendments to Policy
	7	Jan 2019	A Woodhouse	Merged UHDB Policy
	8	Oct 2022	E Griffiths	Scheduled review
Intended Recipients: All staff involved in the management and operational delivery of clinical and non-clinical records.				
Training and dissemination: Will be published on the Intranet (Neti) and Internet (Koha). Staff will also be made aware through IG communications and training.				
To be read in conjunction with: Information Governance Policy, Data Protection & dealing with Confidential Information Policy, Access to Personal Data (Subject Access) Policy, Standard Operating Procedures (SOPs) for Clinical Records, Postage and Mail Policy.				
In consultation with and Date: Information Governance Steering Group on 15/11/22 and Records Manager.				
EIRA stage One Completed Yes Stage Two Completed N/A				
Approving Body and Date Approved			Trust Delivery Group – 28 November 2022	
Date of Issue			December 2022	
Review Date and Frequency			November 2025	
Contact for Review			Head of Information Governance/DPO	
Executive Lead Signature			 Simon Crowther, Executive Director of Finance and Performance	

Contents

Section	Heading	Page number
1	Introduction	3
2	Purpose	3
3	Definitions used	4
4	Key Responsibilities/Duties	4-6
5	Records Management Principles	6-9
6	Monitoring Compliance and Effectiveness	9

1 Introduction

University Hospitals of Derby & Burton NHS Foundation Trust (the Trust) is dependent on its records to operate efficiently and account for its actions.

Records management is a corporate function and effective record keeping is an integral part of professional practice and is essential in providing good communications between professionals and to ensure services are delivered safely.

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

The Trust's records are its corporate memory, providing evidence of actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the Trust, and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

Trust records are important sources of administrative, evidential and historical information. They are vital to the Trust to support its current and future operations. Proper records management is a legal requirement under the Freedom of Information Act. Trust records need to be properly managed for the purposes of accountability, understanding of its history and procedures, and forming archives of research or public record.

2 Purpose

The purpose of this Policy is to define a structure to ensure adequate records are maintained and that they are managed and controlled effectively to comply with legal, operational and information needs and to reduce the risks associated with records management.

This Policy applies to all records in any format or medium: current, non-active, or archived; clinical or non-clinical; held by, or under the control of the Trust. There are examples in the definitions below, but this is not an exhaustive list.

3 Definitions Used

Records

Information created, received, and maintained by an organisation or person for legal obligations or the transaction of business.

Records include the health record which is information relating to the physical or mental health or condition of an individual that has been made by or on behalf of a health professional in connection with the care of that individual.

Examples of records include (but are not limited to):

- Administrative records (including personnel, estates, financial and accounting records, contract records, litigation and records associated with complaint- handling, minutes, and agendas)
- Clinical records - patient health records, both paper and electronic
- Theatre registers and all other registers that may be kept
- X-Ray reports
- Pathology reports and request forms
- Photographs, slides, and other images
- Scanned records
- Policies, procedures, guidelines, manuals
- Audio and video tapes, cassettes, CD-ROMs
- Records in all electronic formats, e.g. emails, databases, SMS, social media, website/intranet that provide key information to patients and staff

Record Management

The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, in a way that is legally and administratively sound, whilst serving the operational needs of the Trust.

Record Lifecycle

The record lifecycle is a term that describes a controlled regime in which a record is managed from the point that it is created to the point that it is either destroyed or permanently preserved as being of historical or research interest.

4 Key Responsibilities/Duties

4.1 Chief Executive

The Chief Executive has overall responsibility for records management in the Trust. As accounting officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key to this as it will ensure appropriate, accurate information is available as required.

4.2 Directors and Heads of Corporate and Clinical Departments

Directors and Senior Managers have responsibility for ensuring that:

- The Trust's records management policies and procedures have been implemented throughout their service.
- Formal responsibility for operational management of records activities within individual areas is assigned to personnel with appropriate skills.

4.3 Caldicott Guardian

The Trust's Caldicott Guardian has responsibility for reflecting patients' interests regarding the use of health records and for ensuring health records are used in an appropriate and secure manner.

4.4 Senior Information Risk Owner (SIRO)

The SIRO is responsible for ownership of information risk across the Trust. The SIRO acts as advocate for information risk on the board and provides written advice to the accounting officer on the content of their Statement of Internal Control regarding information risk.

4.5 Information Governance Steering Group (IGSG)

The IGSG is responsible for monitoring records management compliance within the Information Governance Framework and ensure that necessary policies are produced and implemented.

4.6 Information Asset Owners (IAOs) and Information Asset Administrators (IAAs)

The IAOs, with support from the IAAs, are responsible for control, risk assessment and management processes for the information asset they own. They are responsible for documenting the flows of information in and out of their asset, reviewing arrangements for assuring the quality and security of the data that is entered into their asset and recording any concerns they have in relation to the asset.

Each IAO should have in place a process for documenting activities in respect of records management which may include:

- Adopt and review tracking and registration systems for appropriate records
- Assist with Records Management audits as required
- Report Records Management risks and incidents following the Information Governance Breach Reporting Procedure
- Ensure there is an effective and efficient system for forwarding records as required
- Document records in long term storage so they can be appraised and destroyed as appropriate.
- Ensure that there is a mechanism for identifying records which must be archived
- Identify departmental staff requiring training

4.7 All Staff

It is the responsibility of all staff to ensure that they keep appropriate records of their work in the trust and manage those records in keeping with this policy and with any guidelines subsequently produced.

All staff handling manual health records must be made aware of the importance of tracking. Responsibility to locate health records rests with the manager of the area last known to handle the records.

4.7.1 Training for staff

All staff must be made aware of their record-keeping responsibilities through training programmes and guidance for them to understand their role.

Managers need to ensure staff are fully trained in record creation, use and maintenance of quality records. Training needs to cover:

- What is being recorded, how it should be recorded and why
- How to validate information with the patient or carers or against other records to ensure that staff are recording the correct data.
- How to identify and correct errors
- The use of information – staff must understand what the records are used for (and therefore why timeliness, accuracy and completeness of recording is so important); and
- How to update information and add in information from other sources.

5 Records Management Principles

5.1 Legal and Professional Obligations

All records created during Trust business are corporate records and Public Records. This includes email messages and other electronic records.

The Trust will take actions as necessary to comply with the legal and professional obligations of the:

- Common Law Duty of Confidentiality
- Public Records Act 1958
- Access to Health Records Act 1990
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Data Protection Act 2018
- UK General Data Protection Regulation
- NHS Records Management Code of Practice 2021
- Any subsequent statute or codes around records management.

Records should be:

- Factual, consistent, and accurate
- Created as soon as possible after an event has occurred, being mindful that they are disclosable
- Clear, legible, and protected from erasure

5.2 Purpose and Process for Creating Records

Records are generally created as part of the Trusts business process and serve various purposes:

- Allow employees and their successors to undertake appropriate actions in the context of their responsibilities
- Facilitate an audit or examination of the Trust by authorised individuals
- Protect the legal and other rights of the Trust, its patients, staff, and any other people affected by its actions
- Provide authentication of the records so that the evidence derived from them is shown to be credible and authoritative.

5.3 Process for Retrieval, Accessibility and Tracking

Those with a legitimate right of access can efficiently retrieve information, for as long as the records are held by the Trust.

To ensure that records can be identified and retrieved when needed file structures must be allocated to each set of records. The file title must be relevant to and easily understood by all users and should include version number.

Tracking of Health records – the responsibility for tracking health records rests with each individual as they access the record. For more information please refer to the SOP for casenote tracking.

The Gender Recognition Act 2004 gives transsexual people the legal right to live in their chosen gender. Under the Act, information relating to an application for a Gender Recognition Certificate is 'protected information' if it is acquired in a professional capacity. It is an offence to disclose protected information to any other person unless an exemption applies. For further advice and guidance please refer to the Health Records Manager.

5.4. Process for Disclosure

There are legal provisions that set limitations on the disclosure of records, just as there are also provisions that require or permit disclosure.

Two examples are given below:

- i) The Data Protection Act allows individuals to submit a Subject Access Request for information on or copies of records that the Trust holds about them. The Trust must ensure it is entirely open and subject to certain exemptions, provides patients with all the information the Trust holds for them. To meet this informational right, it is vital to ensure that all the information is traceable and kept within the patient record. Further details and application form can be found within the Access to Personal Data Policy.
- ii) The Freedom of Information Act puts a duty on public sector bodies to proactively publish information they hold and therefore to facilitate better understanding of how public duties are carried out. It also allows individuals to ask for information held by a public authority and the information must be disclosed unless a specific exemption applies. Members of the public are entitled to request official information on the Trust's services and how we operate.

The Caldicott Guardian and Information Governance team should be involved in any proposed disclosure or transfer of confidential patient information.

5.5 Process for Retaining and Disposing of Records

Most NHS records, even administrative ones, contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy records is fully effective and secure.

All records must be assessed at the appropriate time to determine whether or not they are worthy of archival preservation, if they need to be retained for a longer period or whether they should be destroyed. The [NHS Records](#)

[Management Code of Practice retention schedule](#) must be consulted to determine the most appropriate retention period for the information.

No health record should be destroyed without authorisation from the Health Records Manager and the appropriate procedure complied with to generate an audit trail and the required certificate of destruction.

If a record due for destruction is known to be the subject of a request for information, or potential legal action, destruction should be delayed until disclosure has taken place, or the case is closed.

5.6 Storage

Accommodation for the storage of current records should be clean and tidy, should prevent damage to the records and provide a safe working environment for staff.

All personal and sensitive information must be stored securely. Records must not be stored in an area that gives access to unauthorised individuals. Records should be clearly marked so that those accessing them are aware of their sensitivity.

All records should be closed, i.e. made inactive and transferred for storage once they have ceased to be in active use. All such files should be appropriately marked with date of closure and anticipated date of destruction.

Records which are stored in offsite storage need active management. This will ensure that the organisation maintains a full inventory of what is held offsite, retention periods are applied to each record, a disposal log is kept, and privacy impact assessments are conducted on the offsite storage providers

5.7 Transportation

The mechanisms for transferring records from one area to another, or one organisation to another, should be tailored to the sensitivity of the material contained within the records and the media on which they are held.

Labelling and packing: All records being delivered to another location should be enclosed in bags and sealed for transfer. For larger quantities, records should be boxed in suitable boxes, containers, or cages for their protection. Each box, bag or envelope should be addressed clearly and marked confidential with the sender's name and address on the reverse of the envelope.

Health records: Copies of patients' health records must be sent via a secure method of transport which tracks delivery of the package. This can be arranged via the Health Records Manager and any costs re charged to the relevant department.

Taking records off site: Records should only ever be taken off site with the approval of the Line Manager. In the case of health records, approval must be obtained from the Health Records Manager. Security of these records should be paramount, especially in the case of confidential records. The records must

be stored securely within the home. It is essential that any such records are tracked out of the department so that staff are aware of the location of the record.

Records should never be left unattended e.g. in the car or on the train.

It is recognised that on occasion staff may work beyond normal working hours and find themselves in the possession of records that they cannot return to their place of origin. In these circumstances the record should be held securely (i.e. under supervision and locked away) overnight.

Staff need to make provision for colleagues to access records in an emergency and maintain good practice by returning the records back to each base as soon as possible.

6 Monitoring Compliance and Effectiveness

Compliance with the Information Governance Framework will be monitored by the Information Governance Steering Group and by the annual Data Security & Protection Toolkit.

Monitoring compliance with clinical record keeping is covered in the various SOPs.