17. Records Management

Document Classification: Policy		**Document No:** 17
Issue No: 01		**Date Issued** 07.07.09
Policy Signed off by		**Christian Lyons**
Pages: 10	Author C. Lyons	**Next Review Date Due: 19/02/2027**
Revisions:		**ENSURE APPENDIX 82 - LIST OF POLICIES REVIEW DATE IS UP TO DATE AND UPLOADED ON TO THE**
Date:	Reviewed by:	

		WEBSITE.
		Reason for Changes:-
08.10.2014	MS	Reviewed
31/8/2016	RHK	Reviewed
30/8/2018	RHK	Reviewed
18/6/2019	RHK	Reviewed
27.10.2020	RHK	Reviewed
27/11/2021	NS	Reviewed
3.4.2023	RHK	Reviewed
04.04.2024	AF	Reviewed
04.07.2025	AF	Reviewed & Added Clinical Record Retention Schedule Timetable – as per DSPT
19/02/2026	RHK	Reviewed

Table of Contents

17.1 Records Management

17.1.1 Scope

This policy primarily addresses the management of Patient/Client Records in the Clinic.

The policy covers the following areas:

- Records System
- Privacy
- Informing new patients/clients
- Patient access to their personal records
- Alteration of patient records
- Confidentiality agreements
- Disclosure to third parties
- Requests for personal health information and medical records by other medical clinic or practices
- Security
- Staff training

While the policy focuses on the management of the patient's records, it also relates to other recorded information, for example, billing and accounting records, and letters to and from hospitals and other doctors.

17.1.2 Records System

Documents you make (including clinical records) to formally record your work must be clear, accurate and legible. You should make records at the same time as the events you are recording or as soon as possible afterwards. Staff must keep records that contain personal information about patients, colleagues or others securely, and in line with any data protection requirements.

Clinical records should include:

a. relevant clinical findings

b. the decisions made and actions agreed, and who is making the decisions and agreeing the actions

c. the information given to patients

d. any drugs prescribed or other investigation or treatment

e. who is making the record and when.

The Clinic uses EMIS/ Clinic Software which ensures:

- All entries in patients' health records by health care professionals are dated, timed and signed, with the signature accompanied by the name and designation of the signatory.

- All entries in patients' health records are legible.

- Any alterations or additions are dated, timed and signed, and made in such a way that the original entry can still be read.

- All health care professionals working on a patient's case record all treatment given and recommendations in the patient's health record.

17.1.3 Privacy

Personal health records information is defined as information concerning a patient's health, medical history, or past or present medical care; and which is in a form that enables or could enable the patient to be identified. It includes information about an individual's express wishes concerning current and future health services.

All doctors and clinic staff will ensure that patients can discuss issues relating to their health, treatments and that the clinicians can record relevant personal health information, in a setting that provides visual privacy and protects against any conversation being overheard by a third party.

Staff will not enter a consultation room during a consultation without knocking or otherwise communicating with the doctor or nurse.
Staff, registrars and students will not be present during the consultation without the prior permission of the patient.

17.1.4 Informing new patients/clients

Technician/Doctors will discuss the clinic's privacy policy with patients who are new to the clinic at their first visit or when it is clear that the patient is continuing with the clinic.
New patients will be given the clinic's leaflet about personal information, privacy and pricing, and will be offered access to the clinics information policy.

The clinic tries to make sure that the information on privacy available to patients is appropriate for the range of people who come here. Feedback about the information is welcome.

Clinic staff will ensure that current leaflets about the clinic's approach to personal privacy are available in waiting rooms, consulting rooms, and at clinic reception.

Information provided to patients, both by doctors, technicians and staff verbally, and in writing through the clinic leaflets will advise that, for the purpose of patient care and teaching, this clinic normally allows access to patient records by:

- other doctors in the clinic
- locums, and
- Other clinic staffs who need to view the records in their normal day to day duties.

17.1.5 Patient access to their personal health information:

All patients have the right to access their health information stored at the clinic.
The treating doctor or technician will provide an up to date and accurate summary of their health information on request or whenever appropriate.
If the doctor or technician is satisfied that the patient may safely obtain the record then he/she will either show the patient the record, or arrange for provision of a photocopy, and explain the contents to the patient.
Any information that is provided by others (such as information provided by a referring medical practitioner or another medical specialist) is part of the health record and can be accessed by the patient.
Appropriate administration costs may be charged to the patient.
This clinic will respond to a patient's request for access within 7 days of receiving the request, or within 20 days of the request, whichever is the later.

17.1.6 Alteration of patient records

The clinic will alter personal health information at the request of the patient when the request for alteration is straightforward (e.g. amending an address or telephone number).
With most requests to alter or correct information, the doctor or technician will annotate the patient's record to indicate the nature of the request and whether the clinic agrees with it. For legal reasons, the doctor or technician will not alter or erase the original entry. The Clinic software system, used by the clinic for recording patient information, will automatically record the time of the alteration and who did it.

17.1.7 Confidentiality agreements

In order to protect personal privacy, the clinic has staff, including temporary or casual staff; sub-contractors (e.g. software providers etc) and medical students sign a confidentiality agreement.

17.1.8 Disclosure to third parties

The clinic manager and staff will ensure that personal health information is disclosed to third parties only where consent of the patient has been obtained. Exceptions to this rule occur when the disclosure is necessary to manage a serious and imminent threat to the patient's health or welfare, or is required by law.
The doctor or technician will refer to relevant legislation before deciding whether the patient can make decisions about the use and disclosure of information independently (i.e. without the consent of a parent or guardian). For example, for the patient to consent to treatment, the clinic manager must be satisfied that the patient is aware and able to understand the nature, consequences and risks of the proposed treatment. This patient is then also able to make decisions on the use and disclosure of his or her health information.

The clinic manager will explain the nature of any information about the patient to be provided to other people, for example, in letters of referral to hospitals or specialists. The patient consents to the provision of this information by agreeing to take the letter to the hospital or specialist, or by agreeing for the clinic to send it. Doctors and staff will disclose to third parties only that information which is required to fulfil the needs of the patient. These principles apply to the personal information provided to a treating. The principles also apply where the information is transferred by other

means, for example, via an intranet. Information classified by a patient as restricted will not be disclosed to third parties without the explicit consent of the patient. Doctor or technicians' will make a contemporaneous note when such permission is given.

Should an outstanding debt be referred to a collection agency, the clinic will provide only the contact details of the debtor and the amount of the debt. No other personal information will be provided. Information supplied in response to a court order will be limited to the matter under consideration by the court.

17.1.9 Requests for personal health information and medical records by other Services

Access to accurate and up to date information about the patient by a new treating clinicians/doctors is integral to the clinic providing high quality health care.

17.1.10 Security

Doctors, clinicians, clinic staff and contractors will protect personal health information against unauthorised access, modification or disclosure and misuse and loss while it is being stored or actively used for continued management of the patient's health care.

Staff will ensure that patients, visitors to the clinic do not have unauthorised access to the medical record storage area or computers.
Staff will ensure that records, pathology test results, and any other papers or electronic devices containing personal health information are not left where they may be accessed by unauthorised persons.

Non clinical staff will limit their access to personal health information to the minimum necessary for the performance of their duties. E-mails and telephone messages will be treated with security equal to that applying to medical records. Computer screens will be positioned to prevent unauthorised viewing of personal health information. Through the use of, for example, password-protected screen-savers, staff will ensure that computers left unattended cannot be accessed by unauthorised persons.

Clinicians and staff will ensure that personal health information held in the clinic is secured against loss or alteration of data. This includes adherence to national encryption protocols. Patient records will not be removed from the clinic, except when required by clinical staff for patient care purposes.
Records will be kept securely while away from the clinic and the responsible clinician or nurse will ensure that records are returned to the clinic and left in an appropriate place.

Manual medical records and other papers containing personal health information will be filed promptly after each patient contact. Staff will ensure that manual and electronic records, computers, other electronic devices and filing areas are secured at the end of each day and that the building is locked when leaving. The data on the computer system will be backed up daily and a duplicate backup tape/cartridge given to the nominated staff member for storage in the clinic fire proof safe. Backups should be routinely tested to ensure daily duplication processes are valid and retrievable.

17.1.11 Staff training

The Clinics training and induction procedures for clinicians and staff should ensure that they demonstrate understanding of this policy.

17.2 Back Up Policy

- Clinic Software is responsible for backing up the clinic system.

17.3 Retention and Destruction of Records Policy

17.3.1 Introduction

Healthcare organisations are under a duty to keep all records (i.e. patient, staff and business records) for a minimum number of years.

The Department of Health publishes circulars which detail record retention requirements, of these the most relevant one for Acute Trusts is the HSC1999/053 "For the Record", see: http://www.dh.gov.uk/assetRoot/04/01/20/36/04012036.pdf

Other requirements can be found in the following documents:
For Ionising radiations HSG(95)3 Health Service Use of Ionising Radiations
For electronic patient records HSC1998/153 Using Electronic Patient Records in Hospital: Legal Requirements and Good Practice

For copies of these circulars go to:
http://www.dh.gov.uk/PublicationsAndStatistics/Publications/fs/en

The purpose of this document is to provide the minimum periods of retention of corporate records in a format that does not involve having to read lengthy circulars.

It lists how documents/files should be destroyed when no longer required and how and when to store if records need to be retained for a longer period of time than that specified within the relevant circular.

17.3.2 General guidance

A record is anything that contains information, in any media, which has been created or gathered as a result of any aspect of the work of the clinic's employees – including consultants, agency and/or casual staff[1].

All records should be managed in a way that allows the information contained within them to be available to the person who needs them, at the time and place they are needed.

[1] Definition taken from HSC1999/053 For the Record

17.3.3 Specific guidance

This policy is concerned with corporate records, i.e., those that concern the business of the organisation. It may however be incorporated into a wider records management policy covering all records within the organisation.

The records may be held electronically and/or manually and may contain information from any of the categories below:

- Administrative records including: personnel, estates, financial and accounting (e.g. budget information, annual report information)
- Information concerning complaint handling
- Manual (e.g. telephone messages, working papers)
- Printouts of audit trails from computer/automated systems
- Microfiche
- Audit tapes, cassettes
- Video tapes, CD-Rom
- Computer media e.g. CDs, floppy discs
- Computer output e.g. paper, printout from spooler

Regardless of type there is usually a requirement to keep a record for a minimum number of years. This period of time is calculated from the end of the calendar or accounting year following the last entry in the record (e.g. manual file, computer record)

17.3.4 Storage of records

Records should be stored in a secure location when not being used.

The accommodation should comply with health and safety requirements have proper environmental controls and adequate protection against fire, flood and theft.

17.3.5 Disposal of records

Disposal is wider than just destruction (see below), it can also refer to the transfer of records from one media to another e.g. paper records to CD Rom, or the transfer of records from one organisation to another e.g. authorised archive office.

When using another organisation to archive records it is essential an agreement/contract is in place detailing how the records will be archived and who will be allowed access to them.

When an archived record is accessed a note must be made of:

- The date access occurred,
- The details of the person gaining access, and
- The reason access was required.

When a record is removed from the archive a note must be made of:

- The taker of the record
- The taker's signature or a receipt from them
- The expected date of return
- The date the record is returned

Transportation of records removed from the archive must be in accordance with the organisation's current Transportation of Records Policy and with guidance issued by the Information Commissioner, DoH IPU. Additionally there should be compliance with Information Security requirements. All of this guidance requires that records are transported in a secure and confidential manner. Whoever transports them from one site to another should be contractually bound to comply with these requirements.

Any documents identified as requiring permanent preservation must be transferred to the appropriate repository e.g. the County Archive or Public Records Office

17.3.6 Destruction of records

The destruction of records is an irreversible act. Many records contain sensitive and/or confidential information and their destruction must be undertaken in secure locations and proof of secure destruction may be required. Destruction of all records, regardless of the media, should be conducted in a secure manner to ensure there are safeguards against accidental loss or disclosure.

The normal destruction methods used include:

- shredding,
- pulping
- incineration

The clinic's preferred method of destruction is shredding

For the secure destruction of computer media this is normally undertaken by IT experts and may involve taking a hammer to a computer hard disc, heating floppy discs or destroying e.g. with a screwdriver.

The destruction of records is normally undertaken on site or by an approved contractor. There should be a formal contract between the contractor/supplier and the clinic to detail the security and confidentiality requirements associated with transportation and destruction of confidential information. Proof of destruction should be provided in the form of a certificate. A register of destruction should be kept by the clinic as an audit trail.

17.3.7 Retention of Records

Retention periods are generally specific to the type of record. There are minimum lengths of time that each record should be kept.

17.3.8 Retention of Corporate Records

The most used records are described below – please see HSC1999/053 for further detail.

Record Type	Retention period (years)	Notes
FINANCIAL		
Accounts – Annual (Final – one set only)	Permanent	
Accounts - cost	3	
Accounts – working papers	3	
Accounts – minor records (cheques, petty cash, travel & subsistence accounts)	2	From completion of audit
Advance letters	6	
Approved suppliers list	11	Consumer Protection Act 1987
Audit Records – original records	2	From completion of the audit
Audit Reports (including management letters, final accounts)	2	After formal clearance by the Statutory Auditor
Bank Statements	2	From completion of the audits
Bills, receipts and cleared cheques	6	
Budgets	2	From completion of the audit
Buildings and engineering works, inclusive of major projects abandoned or deferred – key records	Permanent	
As above including town and country planning matters and all formal contract documents		For the life of the buildings and installations to which they refer
Buildings – papers relating to occupation (not H&S)	3	After occupation ceases (Construction Design Management Regulations 1994)
Capital Charges Data	2	From completion of the audit
Cash Books	6	The Limitation Act 1980
Cash Sheets	6	The Limitation Act 1980
Contracts – non sealed (property) on termination	6	The Limitation Act 1980
Contracts – non sealed (other) on termination	6	The Limitation Act 1980

Contracts - sealed	Minimum of 15 years	
Creditor payments	3	
Day files	.5 (6 months)	
Debtors records – cleared	2	From completion of the audit
Debtors records – un-cleared	6	
Deeds of title	Permanent	
Expense claims	2	From completion of audit
Forms – Superannuation SD55(ADP) and SD55J (copies)	10	Original are sent to Pensions Agency
Income and expenditure journal	6	
Invoices	6	The Limitation Act 1980
Ledgers	6	The Limitation Act 1980
Mortgage documents	Permanent	
Nominal role	6 (max)	Normally only current and the immediately preceding roll to be kept
Pay Roll – full-time medical staff	6	
Pay Roll – other staff	6	
Receipts	6	The Limitation Act 1980
Superannuation Accounts	10	
Superannuation Registers	10	
Tax forms	6	
VAT records	6	Unless shorted period agreed with Customs & Excise
Wages/Salary records	10	

Record Type	Retention period (years)	Notes
EMPLOYEE		
CVs for non-executive directors (successful)	5	Following term of office
CVs for non-executive directors (unsuccessful applicants)	2	Following term of office
Day files	.5 (6 months)	
Diaries – office – on completion	1	
Establishment records	6	After subject leaves

(personal files, contracts references & related correspondence)		service or until his/her 70th birthday – whichever is later Only a summary needs to be kept to age 70
Establishment records (attendance, annual leave, timesheets etc.)	2	
Job Advertisements	1	
Job Applications (following termination of employment)	3	
Job descriptions (following termination of employment)	3	
Leavers dossiers (provided summary retained)	6	
Nurses training records	30	
Study leave applications	1.5	
Record Type	Retention period (years)	Notes
SUPPLIES		
Contracts – non sealed (property) on termination	6	The Limitation Act 1980
Contracts – non sealed (other) on termination	6	The Limitation Act 1980
Contracts - sealed	Minimum of 15 years	
Day files	0.5 (6 months)	
Deeds of title	Permanent	
Delivery notes	1.5	
Products - liability	11	Consumer Protection Act 1987
Requisitions	1.5	
Stock control reports	1.5	
Stores records – major (stores ledgers etc.)	6	

Stores records – minor (requisitions, issue notes, good received books etc.)	1.5	
Supplies records – minor (ITTs, routine papers etc.)	1.5	
Tenders (unsuccessful)	6	The Limitation Act 1980
Record Type	Retention period (years)	Notes
ADMINISTRATION		
Litigation Dossiers (complaints including accident reports)	10	Where legal action has been commenced, keep as advised by legal representatives
Meeting papers – committees, sub-committees (master copies)	Permanent	
Minutes of the NHS Trust or Health Authority major committees and sub-committees - signed	Permanent	
Minutes – reference copies	1	
Press cuttings	1	
Receipt for registered and recorded delivery mail		
Record of custody and transfer of keys	1.5	
Software licenses	Lifetime	
Trust Administered by HAs – Terms of	Permanent	
Trust documents without	6	

permanent relevance		

Clinical and Patient Records

Record Type	**Retention Time**	**Notes**
Adult GP Records	10 years after date of last entry	Or 10 years after death if patient dies
Child GP Records	Until 25th birthday (or 26th if under 18)	Or 10 years after death (whichever is longer)
Maternity Records	25 years after birth of the child	Includes antenatal and postnatal records
Mental Health Records	20 years after last contact or 10 years after death	Whichever is longer
Safeguarding Records (Child & Adult)	Until 25th birthday or 10 years after death	Or longer if advised by safeguarding authority
Records of Deceased Patients	10 years from date of death	Covers all patient types
Vaccination and Immunisation Records	10 years from date of administration	Clinical record part of core GP record
Significant Events (clinical) Complaints	10 years from event closure 10 years after closure	Retain for legal or risk management purposes Ensure redacted appropriately if shared externally