Record Management Policy

Nominated Individual	Richard Drakeford
Registered Manager	Robin Page
Date Policy Completed	March 2025
Version no.	1.0
Previous Review Dates	3/25
Review Date	March 2027 (or when updates are required)
Applicable to	All staff and contractors
Policy Signed By	RICHARD DRAKEFORD

Contents

1.0 Introduction

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 to their eventual disposal.

Re-Pat Ltd's records provide evidence of actions and decisions and represent a vital asset to support daily functions and operations. Records support policy formation and managerial decision making, protect the interests of Re-Pat Ltd and the rights of patients, staff and members of the public. They support consistency, continuity and efficiency and help to deliver services in a robust way.

Records are required for a number of reasons and are essential to the organisation. Some examples are detailed below:

- To support patient care
- Support the day-to-day running of the service
- To support evidence based practice
- To support administrative and managerial decision making
- To meet legal requirements, including requests under subject access provisions of the General Data Protection Regulations, Data Protection Act and/or the Freedom of Information Act
- To assist with the auditing process
- To support improvements in clinical effectiveness
- To support patient choice and decision making
- To support regulatory activities and processes e.g. investigations, incidents and compliance activities.

2.0 Scope

All staff working at Re-Pat Ltd are responsible for making themselves aware of and complying with this policy.

3.0 Purpose

The Data Protection Act 1998 summarises a health record as 'one which relates to the physical or mental health of an individual, made by or on behalf of a health professional in connection with the case of that individual. Thus, with the exception of the anonymised information most if not all information concerning patients whether held electronically or on paper will fall within the scope of the Act'.

The term 'records' refers to all records which contain personal or sensitive information. This can cover both patients, relatives, employees and visitors of Re-Pat Ltd.

This policy sets out the standards and processes required for maintaining high quality record keeping standards for all patients.

Re-Pat utilises electronic recording processes and aims to reduce the amount of paper records over time.

4.0 Roles and Responsibilities

All staff must ensure confidentiality, integrity and accuracy of records. Staff are personally responsible for the records they create and will not be allowed access to company files or any other electronic system until they have completed information governance and confidentiality training.

Any person accessing the health information of patients has a common-law duty of confidentiality to the patient.

- Information recorded in a patient's record is legally binding. The record should be factual and contain only relevant information which is non-judgemental
- Any notes about a patient form part of the record and should be uploaded to their digital record
- The digital system ensures that all staff are aware of documentation and correspondence relating to a patient
- All staff should be familiar with the digital system and have an individual log-in which is password protected.
- Access to a patient's records without a legitimate reason may result in disciplinary action and/or dismissal and/or legal proceedings.

Data Controller
The Registered Manager is Re-Pat Ltd's Data Controller and has an overarching duty to make arrangements for the safety and integrity of the organisation's health records.

Data Protection Officer
The Company Director is Re-Pat Ltd's registered Data Protection Officer and has responsibility for ensuring health records meet statutory requirements.

Caldicott Guardian
The Company Director is the designated Caldicott Guardian and has responsibility for matters relating to patient confidentiality.

5.0 General principles

Health records must be accurate and recorded in a timely manner. They can be used to evidence the following:

- Care delivery and support
- Multi-disciplinary working
- Evidence-based clinical practice
- Managerial decision-making
- Legal requirements, including requests for access to records
- Clinical audit and effectiveness
- Statutory and contractual reporting requirements
- Regulatory compliance and monitoring.

Health records standards
Health records must:

- Be factual, consistent and be written according to organisational policy and accepted professional standards
- Contain as a minimum the patient's name, date of birth and NHS number (if they have one). Where the NHS number is not known it should be verified via SCR /PDS. To ensure continuing accuracy of records the patient's full name, address and key contact details (including NHS GP) should be verified at each contact and differing records synchronised
- Completed as soon as possible after the event.

5.1 Confidentiality

Any patient records must be held in complete confidence and only viewed by those directly involved in the provision of the person's care or otherwise authorised to do so.

Unauthorised disclosure and misuse of information constitutes a breach of confidentiality. Information contained in a patient's record should only be accessed on a 'need to know' basis. Individuals are specifically not permitted to access the records of people they know via a work, social or family connection or in response to media interest.

Re-Pat Ltd will undertake regular audits to ensure confidentiality has been maintained and will take appropriate action against any individual found to have inappropriately accessed a record.

5.2 Records Retention

Records must be retained according to Re-Pat Ltd's record retention and disposal processes, as shown in the table below.

TYPE OF RECORD HELD	MINIMUM RETENTION PERIOD
Ambulance Records	10 Years
Children and Young People	Until patients 25th Birthday or 26th if patient was 17yrs at treatment, or 8years after death.
Clinical Audit Records	5 Years
Clinical Protocol	10 years
Controlled Drug Documentation	10 years
Electrocardiagram (ECG) Records	7 years (each chart to be labelled with patient details)
Serious Untoward Incident	10 Years
Staff Records	3 Years
Workplace Accidents	10 years
Complaints	5 years after completion

Inactive records which have reached the minimum retention period should be reviewed annually to identify the need for extended retention or destruction. After reviewing, the list should be updated to show those identified for destruction and those identified for extended retention.

5.3 Confidential Waste

All confidential waste must be securely destroyed. Waste material should be sent to the designated confidential destruction site or shredded. All wastepaper baskets must be properly labelled to read 'No Confidential Waste'. In the absence of a shredder, confidential waste must be kept in a 'Confidential Bag' which should kept in secure location and send to the confidential destruction site.

5.4 Information Sharing

Generally, the following principles apply:

- Patient information may not be passed on to others without the patient's consent, except as permitted under schedule 2 and 3 of the Data Protection Act 1998
- Explicit consent is required if identifiable patient information is used in any publication
- Where identifiable information is disclosed, a record of the disclosure and the reasons for doing so should be recorded in the notes
- In circumstances where information is shared without the consent of the patient, the DPO or Caldicott Guardian should be consulted to advise
- When a child or vulnerable adult is believed to be at risk, relevant information should be shared without delay. This requirement will always override all other confidentiality considerations. If it is believed the disclosure may compromise an individual's safety, or that it is not in the public interest to disclose, then the information should not be shared. Reasons must always be documented in the person's record.

5.5 Mental Health Act Documentation

There are specific requirements regarding the receipt and scrutiny of documents under the Mental Health Act 1983:

- Receipt of section papers - only Mental Health Law staff and senior staff are able to receive section papers
- The patient's legal status in respect of their detention, leave and consent to treatment should be immediately apparent from the medical notes

5.6 Incident Reporting

- Where an incident relates to a patient, the incident form must be added to the record or as a minimum the incident form reference logged
- Any Duty of Candour correspondence should routinely be uploaded to the internal system and acted on accordingly. This may include following Duty of Candour processes and notifying CQC. Please refer to Re-Pat Ltd's Duty of Candour Policy.

5.7 Complaints Records

Complaints records must be filed separately from the patient's main record unless there is a need to record the complaint (for example, where it is directly relevant to the patient's health).

5.8 Electronic Records

Re-Pat Ltd's primary record keeping systems are electronic. Duplicate paper recording processes should **not** therefore be used.

5.9 Principles

The following principles apply:

- Only company approved scanners will be used for scanning documents
- All information about a patient received electronically will be uploaded to the system
- All information about a patient received in paper format will be scanned and subsequently uploaded to the system
- All services will set up team based shared folders on the company's digital system. Folders, files and documents will be specific to individuals
- When the system is unavailable, paper records should be scanned and temporarily held in the team folder on the company's digital system. Electronic records should similarly be temporarily held on the company's digital system rather than individual mailboxes or H drives. When the company's digital system becomes available, priority should be given to uploading documents back onto the system
- The electronic record is the **primary record**. No other records will be kept other than a small temporary folder outlined below. All original paper and electronic information will therefore be deleted once the scanned copy on the electronic company's digital system has been verified as attaining the same standard as the originating copy. This is to prevent duplication of systems and information and the potential for information to be missed, incorrectly added to or otherwise inappropriately processed
- Teams will set up a systematic process for alerting all members of the team to newly received and uploaded information, including incoming electronic and paper documents
- Electronic records are subject to the same retention and deletion periods as paper records (i.e. the retention period does not alter simply because the format is electronic rather than paper)
- Electronic records are subject to regular auditing, including record keeping standards and legitimate relationship access to records.
- Requests for access to records will be centrally managed by Access to Records leads. Where solicitors require access to the patient's electronic record this should be printed out and filtered for third party information. This should comply with the 40-day timescales referred to within the Data Protection Act 1998

5.10 Paper Records

The following principles apply:

- Paper records must be stored in an area where patients, members of the public and unauthorised staff are unable to gain access to them.
- Where records are stored in areas that do not have a 24/7 staff presence then they must be secured in an area that is securely locked when the premises are unstaffed

- Missing or part-missing health records must be reported via the organisations incident reporting process and will be investigated accordingly.

5.11 Paper records in transit

If paper records need to be transported from one care setting to another, it is the personal responsibility of the staff member transporting the records to ensure their safety and security whilst in transit. They must ensure that the records cannot be accessed by an unauthorised individual at any time during transit.

The following standards apply:

- Records should be handled carefully and never transported with materials that could cause risk to the records (e.g. chemicals, exposure to weather, excessive light or put at risk of theft)
- An approved courier must be used when transferring health records externally using 'track and trace' including the provision of a signature as proof of delivery
- All packages should be marked 'Private and Confidential. To be opened by the addressee only'
- Records should not be looked at in a public place, including public transport.

6.0 Training

Staff will be required to complete information governance and confidentiality training on induction and updated in-line with the staff training matrix.

7.0 Monitoring

Audits and risk reviews will be carried out regularly to monitor compliance with this policy.

8.0 Relevant Policies and Procedures

Confidentiality Policy
Information Governance Policy
Quality, Governance and Risk Policy
Consent Policy

9.0 Legislation and Guidance

NHS England (2023) Records Management Code of Practice
CQC (2024) Digital record systems: achieving good outcomes for people using adult social care services
Information Commissioners office Records management and security

Company Registered in England
13918654