Records Management Policy

1. Introduction

Records of any type are an information asset because of their contents. Such information is only useful if it is correctly recorded, regularly updated and easily accessible when needed. Information is essential for the delivery of high-quality evidence based health care, delivery of service and the organisation.

Records management is the process by which the organisation manages all aspects of information whether internally or externally generated and in any format or media type, from creation through to eventual disposal.

Serenta Homecare must comply with Information Governance Standards derived from legal and statutory obligations, to create and maintain accurate records of all its activities.

We must comply with the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR), Freedom of Information Act (2000), Public Health Records Acts (1958 and 1967) and standards set by the Department of Health. This guidance includes Caldicott Guidelines relating to the use of patient information and NHS codes of practice in relation to records management, confidentiality, information sharing and Information Security.

Records are an organisation's 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 organisation and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency, and productivity and help us to deliver services in consistent and equitable ways.

Under the UK GDPR, there is increased emphasis on the records management aspects of accountability. We are reviewing current and future systems arrangements to ensure that we are compliant with the additional requirements of GDPR in terms of record processing and working to the principles of Privacy by Design and Privacy by Default.

2. Purpose

Records are subject to standards imposed by legislation, best practice guidance, professional codes of conduct or government regulation. This policy is designed to ensure we meet our legal obligations in relation to Records Management and to work within the wider framework of Information Governance (IG) and the UK GDPR.

Every member of staff has an obligation to comply with legal and statutory requirements regarding the collection, storage, retention, use and disclosure of information that records are comprised from.

This policy will set out expected standards, and reference appropriate guidance, where applicable, for staff to follow in relation to the management of all records, clinical and corporate. Where appropriate, staff will then develop service/system/departmental procedures and guidance to ensure that records are:

- managed and controlled effectively and offer best value

- able to meet legal, operational and information needs
- readily accessible and available for use when needed to give a better use of staff time
- eventually archived or disposed of

The aims of the records management policy are to ensure that records are:

- available when needed so that events or activities can be followed through and reconstructed as necessary
- accessible, located and displayed in a way consistent with their initial use, with the original/current version being identified where multiple versions exist
- able to be interpreted and set in context: who created or added to the record and when, during which business process, and how the record is related to other records
- trustworthy and hold integrity, reliably recording the information that was used in, or created by, the business process
- maintained over time, irrespective of any changes of format so that they are available, accessible, able to be interpreted and trustworthy
- secure from unauthorised or inadvertent alteration or erasure, with access and disclosure being properly controlled and audit trails tracking use and changes
- held in a robust format which remains readable for as long as records are required
- retained and disposed of appropriately using documented retention and disposal procedures, which include provision for reviewing and permanently preserving records with archival value.

3. Definitions

The key definitions applicable to this policy are as follows:

Health Record

The Data Protection Act 2018 defines a health record 'as a record consisting of information relating to the physical or mental health or condition of an identified individual made by or on behalf of a health professional in connection with the care of that individual'. A Health Record may be recorded in computerised or manual form or in a combination of both. It may include handwritten clinical notes, letters, laboratory reports, radiography and other images i.e., X-rays, photographs, videos and tape recordings.

Corporate Record

Corporate Records are defined as 'recorded information, in any form, created or received and maintained by the Company in the transaction of its business or conduct of affairs and kept as evidence of such activity'

Information Life Cycle

Describes the life of a record from its initial creation/receipt 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 to confidential disposal or archival preservation (for records of historical importance);

4. Duties

Managing Director

The Managing Director has overall responsibility for records management within the Company. As the 'Accountable Officer' he is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Corporate records management is the key to this process as it will ensure appropriate, accurate information is available as and when required;

The company 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.

Information Governance Steering Group

The Information Governance Steering Group will ensure that each area of the business implements this policy through the Information Governance Policy and that records management systems and processes are developed, co-ordinated and monitored.

The Records Manager

The Records Manager is responsible for the overall development and maintenance of records management practice throughout the Company, in particular for drawing up guidance for good records management practice and promoting compliance with the records management policy in such a way as to ensure the easy, appropriate and timely retrieval of patient information.

Local accountable record managers

Managers, in all areas of the company have overall responsibility for the management of records generated by their activities, i.e. for ensuring that records created, used, maintained and controlled within their unit are managed in a way which meets the aims of the Company's records management policy and procedures.

Company personnel

Company staff who create, receive, or have access to health or corporate records have records management responsibilities. All staff must ensure that they keep appropriate records of their work in the Company and manage those records in accordance with this policy and with any guidance subsequently produced.

5. Aims

The aims of the Company Records Management System are to ensure that records:

- are available when needed - allowing the Company to form a reconstruction of activities or events that have taken place in the past
- can be accessed and the information within them can be located and displayed in a way consistent with their initial use, and the current version can be identified where multiple versions exist
- can be interpreted - i.e. who created or added to the record and when, and during which business process, and how the record is related to other records in the organisation
- can be trusted – the record reliably represents the information that was used in, or created by, the business process, and its integrity and authenticity can be demonstrated
- can be used and maintained through time – the qualities of availability, accessibility, interpretation, and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format
- are secure - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled, and audit trails track all use of and changes to records; The Company will ensure that corporate records are held in a robust format/medium, which remains readable for as long as the records are required
- are retained and disposed of appropriately - using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value
- staff are trained - so that all staff employed by or on contract to the Company are made aware of their personal and organisational responsibilities for record-keeping and records management; where individuals are employed by a third party the principles and requirements of this policy will be set out and agreed within the service contract.

6. Legal Obligations

All NHS records are Public Records under the Public Records Acts. The Company will take actions as necessary to comply with the legal and professional obligations set out in the Records Management: NHS Code of Practice, and in particular:

- The Public Records Act 1958

- The Data Protection Act 2018
- The UK Data Protection Regulation (UK GDPR)
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality
- The NHS Confidentiality Code of Practice

The Company will make provision for any new legislation affecting records management as it arises

7. Registration of Record Collections

The Company Corporate Records Manager will establish and maintain mechanisms through which departments can register the records they are maintaining by undertaking a Company-wide audit of personal and corporate records. An inventory of all records held by the Company, which identifies the managers responsible for each collection of records, will be created. The inventory of record collections will facilitate the:

- classification of records into series
- generation of a disposal schedule for records which have exceeded their retention period
- recording of the responsibility of individuals creating and managing records
- the inventory will be reviewed annually.

8. Retention and Disposal of Records

The Company recognises that both health and corporate records must be retained for a minimum period of time for legal, operational, research and safety reasons.

The Company will comply with the Data Protection Act 2018 principle that personal data should not be kept for longer than is necessary.

The Company will establish record retention periods in accordance with the type of record and its importance to the Company's business function by adopting the retention periods set out in the Records Management: NHS Code of Practice

The Company recognises that the destruction of records is an irreversible act and that the cost of preserving records worthy of permanent preservation is high. Guidance on the appropriate length of time that records should be kept for business purposes and on the identification of records worthy of permanent preservation will be provided to staff.

Local records managers in the Company will ensure that records that are no longer required for business purposes are reviewed as soon as practicable to avoid inappropriate destruction.

Whenever the retention schedule is used, the guidelines in the NHS Records Management Code of Practice will be utilised

9. Secure Storage

The Company will pay due regard to the principles of the Data Protection Act 2018 and will provide secure storage for all records whilst active.

Manual records that are no longer current but are inside of the record retention periods will be removed to a secure storage facility.

Electronic record keeping systems will be protected by appropriate technology in accordance with the Information Security Policy.

10. Records Management Systems of Audit

The Company will conduct annual audits of its internal records management practices for compliance with the framework set out in this document.

The audit will:

- Identify areas of operation that are covered by the Company's policies and identify which procedures and/or guidance should comply with the policy
- Follow a mechanism for adapting the policy to cover deficient areas if these are critical to the creation and use of records, and use a subsidiary development plan if there are major changes to be implemented
- Set and maintain standards by implementing new procedures, including obtaining feedback where the procedures do not match the desired levels of performance
- Highlight where non-compliance with the prescribed procedures is occurring and suggest a tightening of controls and adjustment to related procedures to remedy this.

The results of audits will be reported formally through the Information Governance Steering Group.

11. Dissemination and Implementation

This Policy will be disseminated to staff via the company's website/global e-mail/team brief/team leaders.

The Record Retention Periods appropriate to this Policy will be made available and accessible on the Company Intranet site and will be linked to this Policy.

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

All Company staff will be made aware of their personal and organisational responsibilities for record-keeping and record management through generic and specific training programmes and guidance materials, which will be regularly reviewed and updated.

The Records Manager will support staff in the records management process.

12. Monitoring Compliance with Effectiveness

This policy will be reviewed every two years (or sooner if new legislation, codes of practice or national standards are introduced).

The implementation and compliance with this Policy will be monitored by the Corporate Information Governance Group.

An implementation plan detailing the steps that will be taken to comply with the policy will contain delegated responsibilities & timeframes for compliance.

Quarterly records management reports will be provided to the Corporate Information Governance Group to monitor compliance.

Compliance with this policy will be monitored during the investigation of complaints or identified incidents or risks

This policy will also be monitored through supporting evidence to The Care Quality Commission Essential Standards Outcome 21 in the Registration Regulations and the Data Security and Protection (DSP) Toolkit.

13. Associated Documents

- Data Protection Policy
- Information Security Policy
- Information Governance Policy

14. References

In developing this policy the Company has had due regard to its legal requirements, the NHS Information Governance Agenda and best practice standards including, but not limited to:-

- Information Security Management: NHS Code of Practice
- ISO 27001 and 27002, the International Standards for Information Security
- ISO 27799: Health Informatics - Information Security Management in Health Using ISO-IEC 27002

- Records Management: NHS Code of Practice
- The legal and regulatory framework as set out within the NHS Information Governance: Guidance on Legal & Professional Requirements
- The NHS Information Governance Toolkit and its component requirements
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR).

Document Control

Date Approved: June 2026
Target Audience: All Serenta Homecare Staff
Review Date: June 2028
Author: Fran Beardsmore