

SESLHD POLICY COVER SHEET



Health
South Eastern Sydney
Local Health District

NAME OF DOCUMENT	Records Management
TYPE OF DOCUMENT	Policy
DOCUMENT NUMBER	SESLHDPD/196
DATE OF PUBLICATION	December 2023
RISK RATING	Medium
LEVEL OF EVIDENCE	National Safety and Quality Health Service Standards: Standard 1 – Clinical Governance
REVIEW DATE	December 2026
FORMER REFERENCE(S)	Area Pol-CGOV-07 SESIAHS PD 019
EXECUTIVE SPONSOR or EXECUTIVE CLINICAL SPONSOR	Director, Digital Health (CIO) as nominated Senior Responsible Officer for Corporate Records
AUTHOR	Records Management Coordinator Jocelyn.Bullard@health.nsw.gov.au
POSITION RESPONSIBLE FOR THE DOCUMENT	Manager Office of the Chief Executive
FUNCTIONAL GROUP(S)	Records Management – Corporate
KEY TERMS	Records Management
SUMMARY	SESLHD recognises that the keeping of records is both a Government mandate and a vital asset to the organisation. All records (paper based and electronic), including administrative, personnel, accounting and health records are to be managed in accordance with this policy, associated referenced documents and the NSW <i>State Records Act 1998</i> No 17.

COMPLIANCE WITH THIS DOCUMENT IS MANDATORY
This Policy is intellectual property of South Eastern Sydney Local Health District.
Policy content cannot be duplicated.

Feedback about this document can be sent to SESLHD-Policy@health.nsw.gov.au

1. POLICY STATEMENT






- That all employees, consultants and contactors of South Eastern Sydney Local Health District (SESLHD) are able to meet their legal obligations in regards to recordkeeping.
- This policy establishes a set of principles and objectives that underpins SESLHD's approach to records management and the conduct of certain recordkeeping practices.
- This policy will support District wide consistency in the management, creation, capture, access, storage and disposal of records, irrespective of format within SESLHD.
- This policy operates in conjunction with other recordkeeping policies, standards and guidance provided by State Records NSW.



2. RESPONSIBILITIES

- **Chief Executive** has ultimate responsibility and provides direction, support and resources for records management, to ensure compliance with the State Records Act 1998 no 17 and other relevant legislation.
[Section 10 of the State Records Act 1998](#) provides that:
The Chief Executive of each public office has a duty to ensure that the public office complies with the requirements of this Act and the regulations and that the requirements of this Act and the regulations with respect to State records that the public office is responsible for are complied with.
- **Director, Digital Health (CIO)** is responsible for promoting records management policies and strategies and advocates for sufficient resources to implement them. The Director, Digital Health (CIO) has a key role in representing records management interests at appropriate decision-making bodies and is SESLHD's **Senior Responsible Officer** for records management. The Director, Digital Health (CIO) is also responsible for ensuring the reliability, continuing operation of computerised systems that generate records and the development, implementation, and monitoring of information technology disaster recovery plans for these systems. Records, information and data management are identified and addressed in outsourced, cloud and similar service arrangements.
- **Director, Internal Audit** is responsible for routinely including records and information management monitoring and review on the SESLHD audit program.
- **Employees (including volunteers and contractors)** have a responsibility to create and effectively and routinely capture accurate records including work-related decisions made or actions taken and transactions of daily business in accordance with organisational policies and procedures. Employees (including volunteers and contractors) are responsible for ensuring the records they create are comprehensive, readily accessible, understandable, and usable.
All employees have recordkeeping responsibilities and obligations. For further information refer to NSW State Archives and Records advice: [Recordkeeping fundamentals – Your responsibilities in the NSW Public Sector](#).

- **Executive Services Records Coordinator** will provide advice to employees in relation to corporate records management.
- **External Service Providers** who have been contracted by SESLHD to fulfil an organisational function or to provide a service to the District and where it has been determined through contractual agreement that the records are the property of SESLHD, are required to return all documents / files to SESLHD.
- **Health Information Managers** will provide advice to employees in relation to health records management.
- **Managers, Team Leaders, Coordinators and Supervisors** in addition to their responsibilities as employees are also responsible for fostering and supporting a culture within their work group that promotes good record management practices and for incorporating records management strategies into district-wide planning. They must also ensure that any local procedures or protocols that are developed are consistent with SESLHD policy and procedure documents and State Records NSW standards.
- **Senior Responsible Officer** - The Chief Executive has delegated the role of Senior Responsible Officer for the oversight of Records Management to the **Director, Digital Health (CIO)** to ensure that SESLHD complies with legislative requirements for recordkeeping by establishing an ongoing organisation-wide records management program which is appropriate to the needs of SESLHD, aligns and supports SESLHD strategic plans, the organisational culture, legislative and technological environment and minimises exposure to risk.
- **SESLHD Health Records Steering Committee** is responsible strategic direction and leadership within the hospital and community setting in relation to the management of health care records and related systems including requirements in relation to national standards.
- **SESLHD Privacy Officers** and **Right to Information Officers** are responsible for ensuring compliance with Privacy and Government Information (Public Access) legislation with regards to access and release of information and documents.
- **System Administrators** are responsible for records management, maintenance, and operation of the records systems they administer as well as routinely auditing the system to ensure that there are no issues affecting information integrity, useability, or accessibility.
- **Tier 2 Directors and General Managers** in addition to their responsibilities as employees are ultimately responsible for ensuring a successful records and information management programs for their facility or service, including supporting and promotion of records and information management policies, procedures, standards, and guidelines.

3. REFERENCES

<p>Legislation</p> 	<ul style="list-style-type: none"> ▪ State Records Act 1998 No 17 ▪ Government Information (Public Access) Act 2009 No 52 ▪ Privacy and Personal Information Protection Act 1998 No 133 ▪ Health Records and Information Privacy Act 2002 No 71
<p>Standards</p> 	<ul style="list-style-type: none"> ▪ National Safety and Quality Health Service Standards 2021 Second edition ▪ Australian Standard AS/ISO 15489.1:2017 Information and documentation – Records Management Part 1: concepts and principles ▪ State Records NSW Standard on Records Management ▪ State Records NSW Standard on the physical storage of State records
<p>Framework</p> 	<ul style="list-style-type: none"> ▪ SESLHDHB/022 - SESLHD Corporate Records Management Framework
<p>Policies</p> 	<ul style="list-style-type: none"> ▪ SESLHD Policy Directive SESLHDPD/203 - Records management - retention periods ▪ SESLHD Policy Directive SESLHDPD/192 - Health Records (Paper based) Disaster Management ▪ NSW Health Policy Directive PD2020 046 - Electronic Information Security Policy
<p>Retention and Disposal</p>  <p>Authorities</p>	<ul style="list-style-type: none"> ▪ GDA17 Health Services, Public: Patient/Client records ▪ GDA 21 Health Services, Public: Administrative Records ▪ GA28 Administrative Records - Includes financial, accounting and personnel records ▪ GA45 Original or source records that have been copied

<p>Procedures</p> 	<ul style="list-style-type: none"> ▪ SESLHD Procedure SESLHDPR/220 – Records – destruction of ▪ SESLHD Procedure SESLHDPR/219 – Records – disaster management ▪ SESLHD Procedure SESLHDPR/192 – Health records (Paper based) disaster management ▪ SESLHD Procedure SESLHDPR/221 – Records – management of email ▪ SESLHD Procedure SESLHDPR/222 – Records – managing paper original or imaged records ▪ SESLHD Procedure SESLHDPR/218 – Records – storage and protection ▪ SESLHD Procedure SESLHDPR/336 – Documentation in the Health Care Record ▪ SESLHD Procedure SELSHDPR/292 – Hybrid Health Care Records Procedure ▪ Museums of History Procedure for transferring physical format records
<p>Guidelines and Business rules</p> 	<ul style="list-style-type: none"> ▪ NSW Health Business Classification Scheme (BCS) ▪ SESLHD Business rule - Content Manager T17/47292 ▪ SESLHD Business Rule - Content Manager and ePersonnel Files T18/62218
<p>Further Resources</p> 	<ul style="list-style-type: none"> ▪ State Records NSW

4. DEFINITIONS

Archive - records that have continuing value because of their legal, administrative, or historical value.

Local Health District - refers to South Eastern Sydney Local Health District as defined under Section 7(a) of the Health Services Act 1997 No 154.

Disposal - this includes consideration of the retention, deletion, or destruction of records in or from recordkeeping systems. They may also include the migration or transmission of records from current office space into low cost or archival storage.

Electronic record - are records where the information is communicated and maintained by means of electronic equipment.

Electronic record management - the convergence of the measures required to effectively collect, store, access, use and dispose of information with computing and telecommunications technologies and associated resources. It encompasses all resources required for the implementation of information technology, i.e. equipment, software, facilities and human resources.

Employee - for the purposes of this document, 'Employee' is defined as any person working in a part-time, casual, or full-time capacity within the Local Health District, including the Chief Executive Directors, Managers, Supervisors and Team Leaders, as well as volunteers, work-experience personnel, contractors, trainees and students.

File - files are a collection of documents on a specific subject, located within a file either in paper or electronic format, that show organisational activities through an identifiable sequence of transactions.

Health care record - a documented account of a person's health, illness or treatment in hard copy or electronic form.

Public Office - in the context of this Policy document public office means South Eastern Sydney Local Health District including all facilities and sites.

Records - recorded information, in any form, including data in computer systems, created, or received and maintained by an organisation or person in the transaction of business or the conduct of affairs and kept as evidence of such activity.

Recordkeeping - making and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information.

Records Management - the discipline and organisation function of managing records to meet operational business needs, accountability requirements and community expectations.

State Record - any record, made and kept, or received and kept, by any person in the course of the exercise of official functions in a public office, or for any purpose of a public office, or for the use of a public office. (State Records Act 1998.s.3 (1)).

State Archive - means a state record that the State Records Authority NSW has control of under the *State Records Act 1998*.

5. POLICY

SESLHD records management operations are to be carried out on a **devolved basis** in accordance with centrally approved policy and standards. **Each hospital, service or unit is responsible for making effective arrangements for managing the records relating to its functions, including the allocation of the necessary resources.**

The effective management of the hospital, service or unit records is one of the formal accountabilities of each manager and the implementation of an effective records management program is to be a key strategy considered during business planning.

SESLHD recognises the value of records and information as a strategic resource that is integral to good business and the daily operations of the Local Health District. As such, all employees (including volunteers and contractors) must create, capture and maintain the records of the Local Health District to support ongoing business activity and patient services, meeting accountability requirements, legislative requirements and community expectations. This includes implementing strategies to ensure records, information and data management are integrated into routine work processes, systems and services and carried out in accordance with authorised procedures.

All employees should ensure they are aware of the legislative, external and internal requirements listed under Section 3 References, which may affect records, information and data management practices associated with their role.

5.1 Creation of records

Records must be made

All employees are required to create records that adequately document the business activities in which they take part and to ensure that information and processing systems that support business activities create appropriate records as part of supporting those activities.

All employees must:

- Ensure records of any significant business conducted or decisions that are made including those made via the telephone or face to face are routinely captured. Significant business can include: providing advice, instructions or recommendations, giving permissions and consent, and making decisions, commitments or agreements. Employees should routinely document the reasons for decisions or recommendations that are made.
- Ensure someone has been delegated to make a record of meetings, whether minutes or a simple summary of decisions. Ensure that decisions are clearly recorded. Record any dissent by participants, circulate and sign or otherwise confirm the accuracy of the record.
- Ensure records regarding projects are created and copies of important research drafts submitted for comment or approval by others and drafts containing significant annotations.
- Ensure high volumes of records in email systems and on network drives are not accumulated. Save records to SESLHD's official recordkeeping systems where they can be properly stored and managed.

Records must be accurate

All employees must ensure accurate records are made at the time of or as soon as practicable after the event or transaction to which they relate.

Records must be authentic

All employees must ensure that records are routinely captured in the official recordkeeping systems and that appropriate metadata is created and captured or otherwise associated with records.

Records must have integrity

All employees must safeguard records from unauthorised access, alteration, deletion or destruction.

Records must be useable

All employees must ensure that records are linked to the business context and that the location of records is recorded and tracked to ensure they are accessible for as long as they are required.

Record creation, storage and archiving systems will be uniform across the Local Health District. Electronic systems for corporate and health care records may be different, however managing all records and information across all operating environments, including diverse system environments and physical locations is *mandatory*.

Responsibility rests with the creator of the records to ensure that the records are captured, managed, and maintained for as long as they are needed for business, legal requirements (including in accordance with current authorised records retention and disposal authorities), accountability and community expectations.

Corporate electronic document and records management system (eDRMS)

The primary eDRMS is Content Manager which is actively managed and maintained as authentic evidence of business activity, kept accessible to authorised users and records are disposed of in a managed, systematic, and auditable way.

While the eDRMS is SESLHD's preferred primary records system for all corporate administrative records, there are a number of databases and software applications which operate outside of the eDRMS that store records.

Employees should note that email folders, portable storage devices, local and share drives including Microsoft Teams one drive are not records management systems because they lack the required records management functionality.

Health Care Records The requirements for Health Care Records are clearly defined in [NSW Health Policy Directive PD2012_069 - Health Care Records – Documentation and Management](#). The principles reflect common law, legislative and ethical requirements. Each principle underpins local and state-wide policies related to health records management. Consolidated and updated state-wide policies can be found in the [Patient Matters Manual for Public Health Organisations](#).

5.2 Protection of records

Under the State Records Act 1998, the Local Health District records are State records. All employees must observe the requirements of SESLHD procedure [SESLHDPR/218 - Records Management – Storage and Protection](#). Records are to be stored only in authorised areas and facilities. Employees are to handle records sensibly and with care and respect to avoid damage to the records and to prolong their life. Employees must not alienate, relinquish control over, damage, alter or destroy records of the Local Health District without authorisation.

5.3 Access to records

SESLHD requires that records are protected from unauthorised or unlawful access, destruction, loss, deletion, or alteration.

- Employees are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period.
- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut completely down at the end of the workday.
- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.

- Passwords may not be shared or left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Upon disposal Restricted and/or Sensitive documents should be shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Lock away portable computing devices such as laptops and tablets.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer.
- All printers and fax machines should be cleared of papers as soon as they are printed to ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

5.4 Disposal and destruction of records

Employees may destroy or dispose of records of the Local Health District only in accordance with SESLHD policy [SESLHDPD/203 - Records Management – Retention Periods](#) and SESLHD procedure [SESLHDPR/220 - Records Management – Destruction of](#).

Guidelines concerning the disposal of health records are outlined in State Records NSW [General Retention and Disposal Authority GDA17 Patient Client Records](#). Guidelines concerning the disposal of Health Service Administrative records are outlined in State Records NSW [General Retention and Disposal Authority GDA21 Public Health administrative records](#). State Records NSW also provides guidelines on some aspects of normal administrative practice as outlined in the [State Records Act 1998 No. 17](#).

Employees who wish to initiate the disposal of records should seek advice from their Manager in relation to administrative records and the Health Records Manager in relation to Clinical Records. State Records NSW may be consulted for additional advice.

As outlined in SESLHD procedure [SESLHDPR/220 - Records management – Destruction of](#), approval should be obtained from the Chief Executive or delegated officer before records are destroyed.

5.5 High Risk records

High risk records are to be identified, managed, or mitigated by undertaking a risk assessment for each core business area and implementing appropriate control measures. If resources are limited, business areas should assess the levels of risk and allocate resources accordingly. For example, there are risks associated with particular record formats or categories, including:

- Records that are 'retain as state archives' are identified in general retention and disposal authorities by NSW State Archives and Records. They cannot be destroyed and should be transferred to the State Archives as soon as they are no longer needed in everyday business.
- digital records that have a retention period of over five years are likely to require preservation including migration, to ensure access over time.
- records that contain classified information need to be protected from unauthorised access.

5.6 Long term preservation of records

Digital

Digital preservation requires at risk records to be identified and necessary action to be taken to ensure the digital information is managed so that it can be accessed and used over time. For example, migration and conversion of records and information through system and service transitions.

Migration is the process of moving files to new media or computer platforms to maintain their value. Conversion entails changing files from one format from one to another and may involve moving from a proprietary format, such as Microsoft Word, to a non-proprietary one such as a plain text file or XML. To avoid losing data in the process initial tests and analysis should be performed to determine exactly what changes will occur and whether they are acceptable. With both migration and conversion, special attention must be paid to also maintaining the accessibility of any associated metadata.

Physical (paper)

Careful handling is the essential basic strategy for the long-term preservation of paper files:

- Ensure your hands are clean, free from food, grease, hand creams and use gloves when necessary.
- Take care when using pens near archival records because they can leave indelible marks on pages.
- Turn pages carefully, with two hands if necessary, to avoid tearing pages off the file pin.
- Do not use a wet finger to turn pages.
- If you need to bookmark a page in a file use a piece of clean white paper – avoid using 'post-it' notes and remove the 'bookmark' when finished.
- Do not use adhesive tape to repair tears. It will discolour, damage the paper and eventually fall off.
- Polyester, polyethylene or polypropylene plastic sleeves are very useful for placing torn or detached folios back on files and isolating photographs and other materials from adjoining file pages.
- File pins and other metal pins will eventually rust. Use stainless steel pins and clips or plastic clips to fasten files. Placing a piece of archival quality paper between the clip and the document will prevent damage to the paper.

5.7 Vital Records

Vital records are records, in any format, which contain information essential to the survival of an organisation. If a vital record is lost, damaged, destroyed or otherwise unavailable, the loss *is* a disaster, affecting critical operations. Vital records should be the main priorities for recovery and salvage efforts when a disaster occurs.

Tier 2 Directors and General Managers are to ensure vital records in their directorates and business units are identified, documented, and protected.

Protecting vital records

Preventive measures may include:

- Scanning and electronically registering the records in Content Manager and changing the record class from Corporate to Vital
- duplication and dispersal of vital records
- high levels of fire and security protection in storage containers and spaces
- storing backup copies off-site, and

- identifying and prioritising critical work in progress that may not be backed up or is sitting out on desks, in drawers, or on open shelving, and following procedures such as a 'clean desk policy' or additional safety measures.

Recovery and restoration procedures may include:

- the relocation of vital records to a secure site in the event of a disaster
- recommended handling and preservation techniques based on the media involved.

5.8 Disaster Management

Tier 2 Directors and General Managers have the responsibility to ensure that risk identification, analysis and assessment are carried out on a regular basis and that cost effective treatment methods are implemented to safeguard SESLHD's records and recordkeeping systems. Disaster management procedures are outlined as follows:

- [SESLHD Procedure SESLHDPD/219 – Records Management – Disaster Management](#)
- [SESLHD Procedure SESLHDPD/192 – Health Records \(paper based\) Disaster Management](#)

5.9 Decommissioning of Systems

Decommissioning is a process by which a business application (or system) is removed from use in an organisation. Decommissioning requires analysis of the data in the system, identifying the data, metadata and system documentation that must be brought forward and retained, and an accountable process for deletion of residual data in the system.

When systems are decommissioned, SESLHD staff must consider retention and disposal requirements for records and information held in the system.

5.10 Outsourced / Cloud Service arrangements

The Director, Digital Health (Chief Information Officer) is responsible for implementing a consistent and structured approach to risk assessments when considering outsourced ICT arrangements for SESLHD information. For all ICT outsourced or cloud service arrangements, the Director Digital Health (Chief Information Officer) must consider:

- the contextual risks specific to SESLHD and operating environment
- applicable NSW Government policy and legislation
- any possible complications arising from data being simultaneously subject to multiple legal jurisdictions.

5.11 Records required as State Archives

Under Part 4 of the *State Records Act 1998*, when SESLHD records deemed to be a State Archive become inactive or no longer in use for official purposes, SESLHD staff are required to routinely transfer all such records to the control of NSW State Archives and Records. Refer to State Records NSW Procedures for transferring custody of records as State Archives.

5.12 Monitoring Compliance

Directors, Managers, Team Leaders, Coordinators and Supervisors are required to monitor and review compliance with SESLHD policies and procedures, the *State Records Act 1998* No. 17 and associated standards and codes of best practice to ensure that they are implemented, accountable and meets the business needs.

- Directors, Managers, Team Leaders, Coordinators and Supervisors will cooperate and liaise with State Records NSW in relation to mandatory annual monitoring compliance surveys.
- Director, Internal Audit will routinely include records and information management monitoring and review on the SESLHD audit program.

6. DOCUMENTATION

As defined within SESLHD Records Management Procedures.

7. VERSION AND APPROVAL HISTORY

Date	Version No.	Author and approval notes
August 2002	0	Author: Area Records Management Committee - Approved by the Area Administration & Finance Committee 21 August 2002
October 2004	1	Re-formatted with minor changes approved by Area Records Officer and re-issued by Manager, Systems Integration.
September 2005	2	Minor changes made by Records Manager, Executive Support Unit following feedback from consultation with stakeholders. Approved by the Executive Management Committee 27 Sept 2005
March 2007	3	Manager, Systems Integration, minor changes to titles and updating references in Section 3.1
February 2011	4	Minor changes made by Records Manager Executive support Unit, updating references Formatting changes due to change to Local Health Network
September 2012	5	Formatting changes due to change to Local Health District
October 2012	5	Approved by DET
November 2012	6	Minor changes made by Manager Executive Services in consultation with CE.
October 2016	7	Major rewrite made by Records Management Coordinator, Executive Services
November 2016	7	Updates endorsed by Executive Sponsor
December 2016	7	Updates endorsed by District Executive Team
May 2018	7	Risk rating reviewed and updated – review dates to remain the same. Approved by Executive Sponsor.
May 2020	8	Minor changes made by Records Management Coordinator, Executive Services
May 2020	8	Minor review to update of terminology (eg Trim to Content Manager) and links. Endorsed by Executive Sponsor. Processed by Executive Services prior to publishing.
January 2023	9	Minor review by Records Management Coordinator, Executive Services. Changes include updating references and links.
March 2023	9	Approved by Executive Sponsor.
18 December 2023	9.1	Minor review to update Senior Responsible Officer for Records Management to Director Digital Health (CIO) and update broken hyperlinks.