

SESLHD PROCEDURE COVER SHEET



Health
South Eastern Sydney
Local Health District

NAME OF DOCUMENT	Records Management – Disaster Management
TYPE OF DOCUMENT	Procedure
DOCUMENT NUMBER	SESLHDPR/219
DATE OF PUBLICATION	July 2025
RISK RATING	Low
LEVEL OF EVIDENCE	National Safety and Quality Health Service Standards: Clinical Governance Standard NSW Legislation – <i>State Records Act 1998</i>
REVIEW DATE	July 2030
FORMER REFERENCE(S)	Area P-CGOV-21 – October 2004 SESIAHS PD 022
EXECUTIVE SPONSOR	Head, Office of the Chief Executive as nominated Senior Responsible Officer for Records, Information and Data
AUTHOR	Jocelyn Bullard Executive Services Corporate Records Management Coordinator Jocelyn.bullard@health.nsw.gov.au
POSITION RESPONSIBLE FOR THE DOCUMENT	Manager Executive Services
FUNCTIONAL GROUP(S)	Records Management – Corporate
KEY TERMS	Records Management; Disaster; vital records
SUMMARY	To outline the procedure for developing, implementing and maintaining an effective and efficient department-based Disaster Management Plan for records. The procedure focuses on the four recognised elements of disaster management: prevention and preparedness (pro-active) and response and recovery (reactive)

COMPLIANCE WITH THIS DOCUMENT IS MANDATORY

**This Procedure is intellectual property of South Eastern Sydney Local Health District.
Procedure content cannot be duplicated.**

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

1. POLICY STATEMENT

The Local Health District (LHD) has a responsibility to ensure all District Departments meet their responsibilities in regard to disaster management of records.

Under the *State Records Act 1998* (NSW), Part 2 Section 10, the Chief Executive has a duty to ensure that their public office complies with the requirements of the Act and the regulations with respect to State Records. Part 2 Section 11 states that “each public office must ensure the safe custody and proper preservation of the State Records that it has control of.”

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.

2. BACKGROUND

To outline the procedure for developing, implementing and maintaining an effective and efficient department-based Disaster Management Plan for records.

The Procedure focuses on the four recognised elements of disaster management: prevention and preparedness (pro-active) and response and recovery (reactive).

3. RESPONSIBILITIES

Chief Executive has ultimate responsibility with delegated responsibility to Head, Office of the Chief Executive as nominated Senior Responsible Officer for records, information and data.

4. DEFINITIONS

Disaster: Unexpected events with destructive consequences, including small and large scale events.

Disaster Management: Term given to strategies for the prevention, preparedness and response to disasters, and the recovery of operations following disasters.

Vital Records: Vital records are the cornerstone of an organisation’s ability to sustain operations and recover from catastrophic events. They are **irreplaceable documents** that are crucial for maintaining core functions and fulfilling legal and regulatory responsibilities.

These records:

- **Ensure business continuity:** Without them, an organisation cannot operate effectively or resume normal functions after a disaster.
- **Support re-establishment:** They are required to rebuild and restore essential services if all other records were destroyed.
- **Cannot be replaced:** Unlike other types of information, these records are **non-substitutable** - no duplicate or alternative source can provide them.

- **Include State Archives:** They also encompass documents required by law to be maintained as permanent records under state or national archival legislation.

Examples of vital records may include:

Type of Record	Description
Corporate charters	Legal documents that establish the existence of the organisation
Titles and deeds	Proofs of ownership of property or assets
Employee records	Essential data for payroll, pensions, and entitlements
Financial ledgers	Core financial transactions and obligations
Strategic plans & policies	Documents outlining operations, compliance, or crisis recovery procedures

Important records: those records which are not irreplaceable but could be reproduced only at considerable expense, time and labour.

Useful records: those records which, if lost, will cause some inconvenience but could be readily replaced.

Non-essential records: those records which are listed in disposal schedules for routine destruction.

5. PROCEDURE

Senior management 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.

The recommended methodology, based on that in Australian/New Zealand Standard, AS/NZS ISO 31000:2009 Risk Management, involves the following steps:

1. Establish the context
2. Identify the risks to records and recordkeeping systems
3. Analyse the risks in terms of probability and effect
4. Assess the risks in terms of acceptability and priorities for treatment
5. Treat the risks by identifying, evaluating and implementing options (this involves developing and implementing a counter disaster plan)
6. Monitoring and review

5.1 Prevention

The prevention phase should involve the:

- identification and assessment of risks to records and buildings and areas where records are stored, and
- identification and documentation of the important and vital records in the organisation.

Records Management – Disaster Management

SESLHDPR/219

Where cost effective methods can be found to eliminate or reduce risks, these should be implemented.

Each department must identify what is 'vital'. This should involve elements of business continuity and resumption planning strategies, as some vital records are essential in restoring critical functions. Organisational charts and related documentation should be used to identify functions that are vital to the organisation.

Risk audits should be applied to SESLHD's vital records to see whether they are adequately protected and accessible to staff that require them. Risk audits for vital records should also identify the impact on business activities, such as service delivery functions, legal liability and financial functions, if such records were lost or unrecoverable.

Once functions are identified, they must be analysed to determine what records are:

1. **vital records:** those records which are irreplaceable and mission-critical
2. **important records:** those records which are not irreplaceable but could be reproduced only at considerable expense, time and labour
3. **useful records:** those records which, if lost, will cause some inconvenience but could be readily replaced
4. **non-essential records:** those records which are listed in disposal schedules for routine destruction.

Electronic records might be vital as well and will need to be identified and planned for. Once identified, vital records must be listed. Lists should include:

- an identification number for each type of record
- the name of the area responsible for record series or electronic system containing vital information
- the title of the series or electronic recordkeeping system
- an indication as to why it is considered vital
- the record format
- all physical locations of originals and duplicates, and
- the frequency of update.

5.2 Preparedness

Where risks cannot be eliminated, they need to be managed. All Local Health District departments should establish and maintain a records management disaster management plan. This Plan should identify the most appropriate way to:

- initially respond to a disaster
- maintain business continuity during the disaster, or
- recover quickly after the disaster.

SESLHD PROCEDURE

Records Management – Disaster Management

SESLHDPR/219

The disaster recovery plan should also include:

- maintaining lists of materials and contacts that can be used in a disaster
- keeping recovery supplies on site
- testing and reviewing the plan, and
- training staff in the plan's use.

All potential risks to records, their possible causes and consequences should be identified. One of the most important ways to identify potential disasters is to conduct regular risk audits of the building and its surroundings.

Risk audits should also be applied to electronic records and their locations.

5.3 Response

Response includes the activities involved in putting the plan into action and getting together those resources that can assist agencies to protect or secure their assets from loss. It includes contacting the response and recovery team and relevant authorities, securing areas, issuing press releases and contacting recovery resources.

[Appendix 1](#) – Flow chart - Long Term Actions for a minor disaster.

5.4 Recovery

The final phase of disaster management is recovery, the activities associated with restoring resources and operations following a disaster so that normal operations can resume.

Detailed information on the four phases of Disaster Management for records are available from [State Records NSW Counter disaster reaction and recovery plan](#).

6. DOCUMENTATION

Disaster Management Team Checklist – [Appendix 2](#).

7. REFERENCES

- [State Records Act 1998 \(NSW\)](#)
- [State Records NSW Counter disaster reaction and recovery plan](#)
- [National Safety and Quality Health Service Standards – Clinical Governance](#)

8. VERSION AND APPROVAL HISTORY

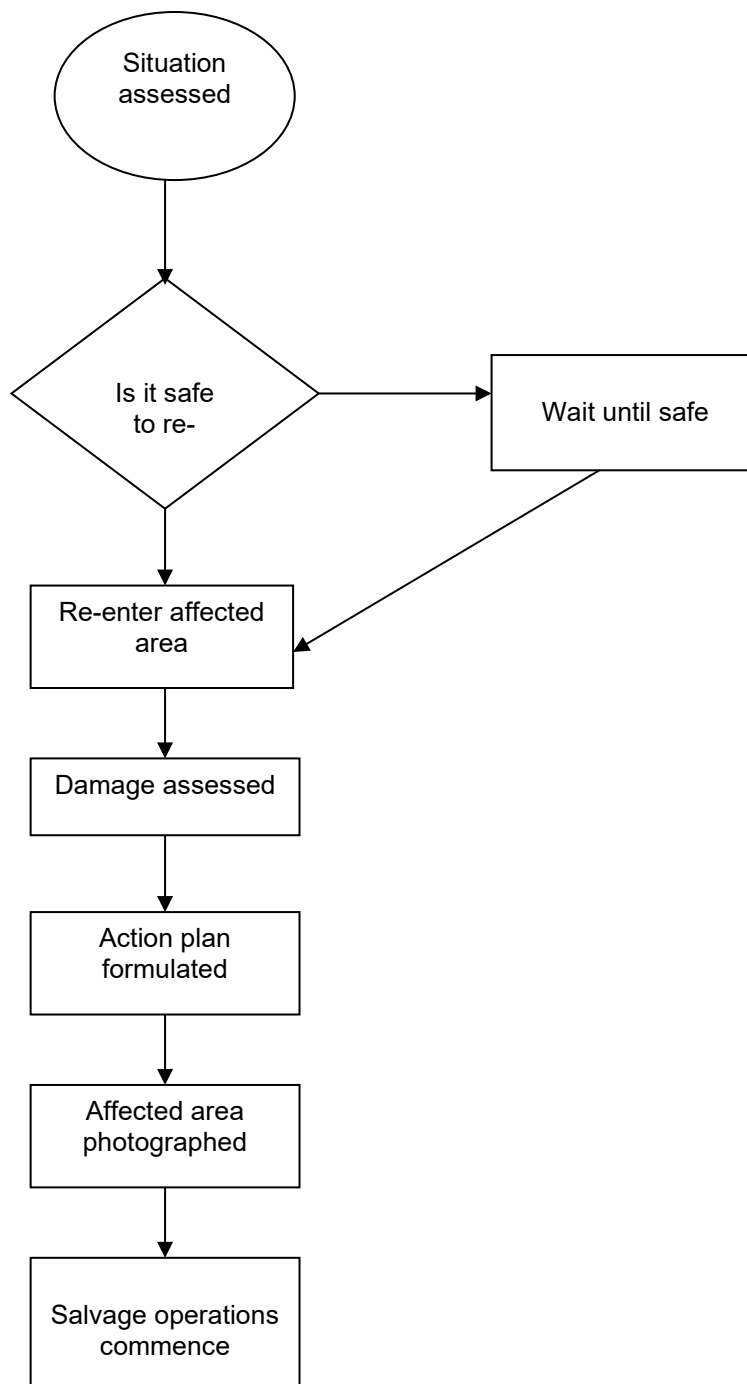
Date	Version	Version and approval notes
October 2004	0	Document previously prepared by Area Records Management Committee- not published- Reviewed in Oct 04 by Area Records Officer and re-formatted and released by the Manager Systems Integration.

Records Management – Disaster Management

SESLHDPR/219

September 2005	1	Minor changes made by Records Manager, Executive Support Unit following feedback from consultation with stakeholders. Approved by Area Executive Committee 27 September 2005
February 2011	2	Minor changed made by Records Manager, Executive Support Unit in consultation with Area Corporate Records Management Committee Formatting changes due to change to Local Health Network
October 2012	3	Changes made to LHD Approved by DET
November 2012	4	Minor changes made by Manager Executive Services in consultation with Chief Executive.
July 2016	5	Minor changes made by Records Coordinator to references and hyperlinks
July 2016	5	Updates endorsed by Executive Sponsor
May 2020	6	Minor changes made by Records Coordinator to references and hyperlinks and endorsed by Manager Executive Services on behalf of Executive Sponsor.
May 2020	6	Processed by Executive Services prior to publishing
18 December 2023	6.1	Minor changes to update Senior Responsible Officer for Records management to Director, Digital Health (CIO and update broken hyperlinks.
2 July 2025	6.2	Minor changes to update Senior Responsible Officer to Head, Office of the Chief Executive and definition of vital records update broken hyperlinks and reference to risk management standard. Minor changes to incorporate comments from Health Service Functional Area Coordinator HSFAC.

Appendix 1 - Long Term Actions for a minor disaster



SESLHD PROCEDURE

Records Management – Disaster Management

SESLHDPR/219

Appendix 2 – Disaster Management Team Checklist

1. Have you developed a project work plan and a strategic plan for the project?	<input type="checkbox"/> Yes <input type="checkbox"/> No
2. Have you arranged to report regularly to senior management?	<input type="checkbox"/> Yes <input type="checkbox"/> No
3. Have you informed all staff of the project?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Prevention - Records management practices	
4. Do you have current records inventories which list a record's function, format, location and use, and whether it is vital?	<input type="checkbox"/> Yes <input type="checkbox"/> No
5. Have you documented classification and retrieval systems so that files can be found easily?	<input type="checkbox"/> Yes <input type="checkbox"/> No
6. Have you documented retention and disposal schedules?	<input type="checkbox"/> Yes <input type="checkbox"/> No
7. Have you determined requirements for recordkeeping?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Vital records programs	
8. Have you identified your vital records in all record formats?	<input type="checkbox"/> Yes <input type="checkbox"/> No
9. Have you addressed actual and potential risks that could adversely affect vital records?	<input type="checkbox"/> Yes <input type="checkbox"/> No
10. Are vital records copied for backup protection and the copy stored at a different site to the original?	<input type="checkbox"/> Yes <input type="checkbox"/> No
11. Are vital records stored on or offsite in appropriate storage conditions and housings?	<input type="checkbox"/> Yes <input type="checkbox"/> No
12. Are vital records secured from unauthorised access?	<input type="checkbox"/> Yes <input type="checkbox"/> No
13. Do you have a vital records plan?	<input type="checkbox"/> Yes <input type="checkbox"/> No
14. Are there procedures to review and test the vital records program and manage the identification of new vital records based on the risk analysis?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Risk management	
15. Have the risks to records been addressed in organisation-wide risk assessments?	<input type="checkbox"/> Yes <input type="checkbox"/> No
16. Have you assessed the risks to records as part of your disaster management project?	<input type="checkbox"/> Yes <input type="checkbox"/> No
17. Have cost-effective risk treatment options been implemented?	<input type="checkbox"/> Yes <input type="checkbox"/> No
18. Are risk management strategies for records regularly reviewed to ensure they are effective?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Security	
19. Are the records unit work area and all records storage areas secure against unauthorised access?	<input type="checkbox"/> Yes <input type="checkbox"/> No

SESLHD PROCEDURE

Records Management – Disaster Management

SESLHDPR/219

20. Are there procedures and equipment for securing records not normally held in records storage areas?	<input type="checkbox"/> Yes <input type="checkbox"/> No
21. Do the procedures in Question 20 cover: a. the issue of records to/from agency staff b. removal or borrowing records from agency premises	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Yes <input type="checkbox"/> No
22. Do you have procedures to secure your electronic records from unauthorised access?	<input type="checkbox"/> Yes <input type="checkbox"/> No
23. Have you identified records which require special handling because they may contain confidential or valuable information?	<input type="checkbox"/> Yes <input type="checkbox"/> No
24. Are such records stored securely and flagged to indicate restricted access?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Business continuity/resumption planning	
25. Have the critical functions of your department been identified?	<input type="checkbox"/> Yes <input type="checkbox"/> No
26. Are the records to support these functions managed as part of your vital records program?	<input type="checkbox"/> Yes <input type="checkbox"/> No
27. Has your department identified and listed other business resources needed to perform critical functions (such as computer equipment)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
28. Has your department identified alternative sources for these business resources?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Disaster planning, response and recovery	
29. Does your department have a counter disaster plan for agency records based on the risk analysis?	<input type="checkbox"/> Yes <input type="checkbox"/> No