



Corporate Records Management Procedure

Contents

1. Purpose	2
2. Procedure	2
2.1 Training	2
2.2 Recordkeeping system	2
2.3 Creating records	3
2.4 Capturing and controlling records	6
2.5 Securing and protecting records	8
2.6 Accessing records	10
2.7 Disposing of records	11
2.8 Reporting	13
3. Roles and Responsibilities	14
4. Monitoring and Evaluation	14
4.1 Monitoring	14
4.2 Evaluation	14
5. Compliance	14
6. References	15
7. Definitions	15
8. Document Summary	18
9. Document Control	19
10. Approval	19
Appendix A: Legacy hard copy records management	20
Appendix B: Retention and disposal authorities	21
Appendix C: Folder management	23
Appendix D: Records Manager security model	25
Appendix E: Electronic transmission of corporate records	27
Appendix F: Monitoring	28

1. Purpose

The purpose of this procedure is to support the WA Country Health Service (WACHS) and all its employees to meet the requirements of the WACHS [Corporate Recordkeeping Compliance Policy](#).

2. Procedure

2.1 Training

Recordkeeping Awareness Training (RAT)

All WACHS employees must complete [Recordkeeping Awareness Training \(RAT\)](#) in the Learning Management System.

This is a mandatory requirement of the [Employment Policy Framework](#).

The current RAT course is common to all Health Service Providers (HSP) and the Department of Health. Completing this current course or having completed the previous WACHS version meets the requirement.

Records Manager training

All WACHS employees with corporate duties requiring access to Records Manager must complete WACHS-specific Records Manager training.

Limited read-only access to non-sensitive corporate records will be available until training is completed.

Due to the different implementation of the recordkeeping system in other HSP and the Department of Health, completing a WACHS-specific training course is required.

WACHS managers must ensure all new WACHS employees:

- understand the recordkeeping standards and processes of their business area as part of employee induction
- undertake corporate duties requiring access to Records Manager are enrolled in WACHS-specific Records Manager training.

2.2 Recordkeeping system

Records Manager

The recordkeeping system approved for the use of keeping corporate records is Records Manager, also known as TRIM. It is an electronic document and records management system (EDRMS).

All WACHS employees with corporate duties must keep corporate records in Records Manager.

The electronic record in Records Manager is the single source of truth.

All WACHS employees who share corporate records in collaboration applications such as SharePoint, Microsoft Teams or One Drive must ensure the:

- corporate record shared has its source in Records Manager
- original record in Records Manager is updated with any changes.

Legacy records

Hard copy records management is not supported for corporate records, except for legacy records.

All WACHS employees must keep legacy hard copy records for the life span of the records until eventual destruction, transfer or permanent retention (see [Appendix A: Legacy hard copy records management](#) for further guidance).

Migration

Shared drives and email systems are not authorised for the keeping of corporate records.

WACHS managers must:

- ensure that their business area steadily migrates corporate records currently kept in shared drives or email systems to Records Manager beginning with:
 - any current, in use records
 - the previous year's records
 - significant, sensitive or high-risk records, and
- have corporate records which have met the minimum retention requirements authorised for disposal (see [Disposing of records](#) for further guidance).

2.3 Creating records

Record of your work

All WACHS employees must create a corporate record, or ensure a corporate record is created, whenever there is a business activity, process or transaction such as:

- a decision is reached
- a transaction is made
- a customer is communicated with.

Records may be in any format such as emails, spreadsheets, Portable Document Formats (PDFs), databases, photographs, maps, audio or video recordings, text messages from mobile phones or social media posts.

If you answer yes to one or more of the following questions, a record should be created.

- Does the matter relate to my work?
- Did I write, receive or send this in the course of my work?
- Is action required?
- Is this something I have used to do my work or to reach a decision?
- Will I need this information again?

- Will someone else need this information at some stage?

See the [State Records Office of Western Australia \(SRO\) - Records Management Advice - Recordkeeping Responsibilities and You](#) for further guidance.

Ephemeral records

Ephemeral records are “those with only short-term value to an organisation, as they contain little or no ongoing administrative, fiscal, legal, evidential or historical value”.
[General Disposal Authority for State Government Information \(DA 2013-017/1\)](#)

All WACHS employees may:

- not keep ephemeral records in the recordkeeping system; examples of ephemeral records include:
 - printouts from Records Manager or a line-of-business system
 - duplicate or exact copies of records captured in Records Manager
 - external publications
- keep ephemeral records alongside corporate records in Records Manager if that would be beneficial to WACHS employees.

All WACHS employees must:

- take care assessing the content of ephemeral records that they do not contain unique information of ongoing value to the organisation. In which case they are corporate records
- keep corporate records in Records Manager
- securely destroy ephemeral records without further authorisation once no longer of use.

Receive records

WACHS does not have a single point of entry for the receipt of hard copy or electronic records. Mail management is a distributed responsibility.

All WACHS employees receiving a corporate record must:

- capture the record, or ensure that it is captured, to Records Manager
- distribute the electronic record, or ensure that it is distributed, to WACHS employees requiring it to do their work.

Hard copy records management is not supported for corporate records, except for legacy records. However, it is likely WACHS will continue to receive some hard copy records.

All WACHS employees must:

- create and whenever possible receive electronic records that are born digital such as emails, PDF or Microsoft Word files rather than hard copies
- request outside organisations communicate with WACHS in this way rather than through the post
- digitise, by scanning, any hard copies received.

Scanning

Digitising, or scanning, corporate records must be completed in a way that results in the digitised electronic record being able to stand in place of the hard copy source record.

All WACHS employees scanning corporate records must:

- complete scanning in compliance with the requirements of the [SRO - Specification for Digitisation of State Records](#)
- set up scanner or multi-function device to scan:
 - at 300dpi
 - original size
 - with auto-colour detection
 - with optical character recognition (OCR) so most text is searchable
- perform initial quality check while scanning to ensure:
 - all pages are scanned
 - pages are in order
 - all content is as legible as that of the hard copy
 - re-scan if necessary
- capture to Records Manager as soon as practical after digitisation (see [Capturing and controlling records](#) for further guidance)
- write the Records Manager record number on the hard copy
- place the hard copy aside in a box or file
- treat the digitised version as the corporate record, once it is in Records Manager
- take any further action on the digitised electronic record, not the hard copy; actions may include:
 - making notes
 - signing or authorising
 - making changes
- treat the hard copy as a source record and manage until disposal (see [Disposing of records](#) for further guidance).

Create records

All WACHS employees with corporate duties must:

- create corporate records such as writing documents or email correspondence
- ensure corporate records are created of all business activities, processes or transactions that do not directly result in a record such as creating a meeting agenda and minutes or a file note.

Emails

Emails sent or received by a WACHS employee as part of their work are corporate records to be captured in Records Manager, not kept within an email system.

All WACHS employees must:

- keep corporate records in the form of emails in Records Manager
- restore emails from 'archiving solutions' such as Enterprise Vault before capturing in Records Manager, failure to do so will result in a 'stub' without the full text of the email being available.

Electronic documents

Electronic documents created or received by a WACHS employee as part of their work are corporate records to be captured in Records Manager, not kept in shared drives or collaboration applications.

All WACHS employees must:

- keep corporate records in the form of electronic documents in Records Manager
- not compress electronic documents in 'archive' files such as .zip or .rar files. Doing so will result in the corporate records not being searchable, updateable or accessible for the full life span of the records
- not protect electronic documents with passwords. Doing so will result in the corporate record not being available to WACHS employees requiring the record to do their work.

Websites

Websites and website content created by a WACHS employee as part of their work are corporate records to be captured in Records Manager.

WACHS managers responsible for a website or website section must:

- ensure that their business area keeps corporate records of the website and website content in Records Manager including:
 - purpose of the site whether informational or transactional
 - published information
 - changes and updates to the website information.

Social media

Social media posts created or received by a WACHS employee as part of their work are corporate records to be captured in Records Manager.

WACHS managers responsible for social media content must ensure that their business area keeps corporate records in Records Manager in compliance with the WACHS [Social Media Policy](#) which states: "It is the responsibility of the responsible business unit to record post content, comments and private messages."

The WACHS Communications team must keep corporate records in Records Manager in compliance with the WACHS [Social Media Policy](#) which states: "The Communications team is responsible for recording analytical data, available via Facebook Business Manager. It is recommended that analytical data be collected at least one month from the date of the post."

2.4 Capturing and controlling records

Business processes

All WACHS employees must ensure they engage in verifiable business processes that result in the capture of corporate records in Records Manager.

Capturing records

All WACHS employees with corporate duties must:

- capture corporate records in Records Manager as close as possible to the activity recorded or at a clear point in the conversation such as:
 - when a decision is made
 - when a milestone is reached
 - when a piece of information is introduced
- register corporate records in Records Manager.

For each record registered Records Manager will generate the following metadata:

- Creator: the WACHS employee logged into the computer, and therefore into Records Manager, with their HE number and password.
- Date created: date and time the file was created in its native application. For example, when a Microsoft Word document was created on a computer desktop or when an email was sent.
- Date registered: date and time the record, in whatever format, is registered in Records Manager.

All WACHS employees registering a corporate record in Records Manager must, for each record:

- select the following metadata:
 - Record type such as Email or eDocument
 - Regional Classification Prefix such as Email - GF or eDoc - CO.
 - Format (Document) either Electronic or Scanned
 - Folder the record will be contained in
- give each record a clear and unique title; the title should:
 - use consistent naming conventions
 - use naming conventions of your business area
 - give a clear idea of what the record is without having to open it
 - contain terms likely to be searched on
 - use dates at the start of the title in reverse order YYYY-MM-DD
 - use unique identifiers to easily distinguish between similar records.

Controlling records

All WACHS employees registering a corporate record in Records Manager must, for each record:

- select the correct folder to contain it in:
 - Collected in a folder with other records relating to the same business activity, process or transaction
 - Organised by date
- create a new folder if an appropriate one does not already exist.

WACHS managers must:

- ensure that their business area creates folders:
 - in the most appropriate section of the classification structure

- that keep separate operational records and a limited number of strategic records
- that are organised per year in most cases. Exceptions may include multi-year projects or contracts with a term greater than one year
- ensure that their business area closes folders:
 - At the end of the calendar or financial year in most cases.

Classification structures and the folders within them are linked to default security and access as well as disposal authorities.

See [Appendix C: Folder management](#) for further guidance.

2.5 Securing and protecting records

Records Manager security

Records Manager is available only within the Health network.

The Manager Records Management must ensure Records Manager software and server is maintained in compliance with [MP 0067/17 Information Security Policy](#).

Records Manager log-in is unique to each WACHS employee using HE number and password log-in to your physical or virtual computer.

All WACHS employees must keep passwords individual and private in compliance with [MP 0067/17 Information Security Policy](#).

The Records Manager security model is made up of security level and access controls.

WACHS Records Services must maintain Records Manager:

- security levels applied to both positions and records
- access controls applied to records to limit accessibility of sensitive information.

User security

WACHS Records Services must:

- provide WACHS employees who have completed training a security level in Records Manager based on the employee's position
- provide WACHS employees who have completed training accessibility to sensitive records based on the employee's position having reason and permission to access sensitive information as part of their work
- in consultation with business areas, maintain membership of access control groups to limit accessibility of sensitive information.

WACHS managers must:

- ensure that their business area engages in consultation with WACHS Records Services to maintain membership of access control groups to limit accessibility of sensitive information
- ensure that changes in their business area are communicated to WACHS Records Services including:

- a new WACHS employee with corporate duties requiring access to Records Manager
- change of position of a WACHS employee in compliance with [WACHS Cessation of Employment Policy](#)
- an employee leaving WACHS employment, including transfer to another HSP or Department of Health, in compliance with WACHS [Cessation of Employment Policy](#)
- change in line of reporting
- participation in cross-business groups, for example committees or projects, requiring changes to record accessibility.

Employees changing position or leaving WACHS employment must ensure all relevant records from the position they are leaving are in Records Manager to ensure retention of business knowledge and intellectual property in compliance with WACHS [Cessation of Employment Policy](#).

Information classification

Records are a form of information and the same classification rules apply to them as in the WACHS [Information Classification and Handling Policy](#).

All WACHS employees registering a corporate record in Records Manager must, for each record:

- assess the information classification of the record as either Official or Official: Sensitive; examples of sensitive information include:
 - sensitive personal information including health information of clients or employees
 - commercial in confidence information
 - Cabinet in confidence information
 - legal privilege information.
- manage any Commonwealth Security Classified information in accordance with the relevant provision(s) of applicable inter-jurisdiction agreement(s).

Security level

All WACHS employees registering a corporate record in Records Manager must, for each record, contain the record in a folder with security level proportionate to the sensitivity of the information the record contains:

- Protected (Internal Use) security level for information classified Official.
- Confidential security level for information classified Official: Sensitive.

The security level of records in Records Manager is by default taken from the folder they are saved in.

The security level of folders in Records Manager is by default taken from the classification structure they are created in.

All WACHS employees registering, accessing, using or receiving a corporate record in Records Manager must, for each record:

- ensure the record is contained in a folder with security and access controls proportionate to the sensitivity of the information the record contains
- request security and access control changes if appropriate folders are unavailable.

See [Appendix D: Records Manager security model](#) for further guidance.

Hard copy storage

All WACHS employees must ensure legacy hard copy records are stored in such a way as to:

- protect the records from unauthorised access or theft
- minimise risk of damage from vermin and natural disaster such as fire, water and mould.

2.6 Accessing records

Accessibility

All WACHS employees must ensure:

- ready accessibility for other WACHS employees to non-sensitive corporate records in Records Manager
- corporate records containing sensitive information have accessibility restricted to WACHS employees who need to access these records to do their work. Including the work of supervising, coordinating and directing the work of others
- accessibility restrictions are based on position, group or business area membership rather than on individual persons, except where this is strictly necessary such as individual members of recruitment panels or individual decision makers for integrity investigations.

WACHS Records Services must:

- in consultation with business areas restrict accessibility of sensitive corporate records in Records Manager to positions, groups or business areas, or in a limited number of cases individuals.
- include line of reporting up to and including the WACHS Chief Executive in accessibility restrictions, unless there is a specific reason not to.

Access

All WACHS employees must access corporate records:

- that they have reason and permission to
- Only for the purpose of their work.

Use

Corporate records are an organisational asset and should be used to further WACHS' core purposes and strategic goals.

All WACHS employees must:

- refer to relevant existing corporate records when making decisions or researching subjects
- edit existing records when there is an update or change to be made thereby ensuring version control.

Share

All WACHS employees must share:

- corporate records with and distribute corporate records to persons with reason and permission to access these records
- links to records in Records Manager with internal parties, rather than distributing uncontrolled copies.

See [Appendix E: Electronic transmission of corporate records](#) for further guidance.

2.7 Disposing of records

“Disposal” encompasses both destruction of time expired records and transfer of records to permanent archives.

Destruction of temporary records

All WACHS employees must:

- retain corporate records, including records no longer in use, for the time period specified by an approved disposal authority. See [Appendix B: Retention and disposal authorities](#) for further guidance
- only dispose of records authorised for disposal.

WACHS managers must review time expired records of their business area and either endorse disposal or provide a reason to retain longer than the minimum retention period because the records are:

- significant or historical
- currently referenced
- required for review.

WACHS Executive Directors must, in accordance with the WACHS [Authorisation Schedule](#) authorise disposal of time expired corporate records endorsed by WACHS managers.

WACHS Chief Financial Officer (CFO) must, in accordance with the WACHS [Authorisation Schedule](#) authorise disposal of time expired financial records endorsed by WACHS Managers.

Any destruction of corporate records without this authorisation is illegal and may be subject to a \$10,000 fine per section 78(7) of the [State Records Act 2000](#).

Destruction methods

Records authorised for destruction are to be completely and securely destroyed so no information is recoverable.

All WACHS employees taking part in destruction of corporate records must either ensure hard copy records are:

- shredded or placed in a secure destruction bin onsite by a WACHS employee and that this employee certifies complete and secure destruction has occurred
- shredded or pulped by a secure destruction company operating under common use arrangement [Storage, Retrieval, Destruction and Digitisation of Paper and Electronic Records CUAREC2015](#). The company will provide a certificate of destruction for these services.

Other methods of destruction of hard copy records, such as burning or burying, are not allowed.

Photographic film and other non-paper hard copy records are to be completely and securely destroyed by methods appropriate to the material and similar to shredding.

WACHS Records Services must:

- destroy electronic records in Records Manager so that no information from the electronic file (for example the document or the email) is recoverable
- ensure metadata including an audit trail of creation, use and destruction is retained.

Archiving of State archive records

Significant records are not to be destroyed at the end of the retention period required by an approved disposal authority. They are to be transferred to the State Archives when this organisation can accept transfers as required by the *State Records Act 2000*.

Authorisation to transfer records to the State Archives follows the same process as authorisation of destruction of temporary records.

State archives may have a restricted access period during which they are only accessible to authorised WACHS employees or through Freedom of Information (FOI) requests. After this period the State archives are open access.

All WACHS employees must attempt, as far as current resources allow, to store hard copy State archive records in WACHS' possession in compliance with [SRO Guideline - Archival Storage Specification](#).

WACHS Records Services must regularly convert electronic records in Records Manager that are State archives to long-term file formats.

Disposal program

WACHS managers and Executive Directors must review, endorse or authorise disposal reports in a timely manner.

WACHS Records Services must:

- prepare disposal reports of corporate records in Records Manager for both electronic and legacy hard copy records
- distribute disposal reports for endorsement by managers of the relevant business areas and authorisation by the relevant Executive Director
- distribute disposal reports annually:
 - financial records after the end of each financial year
 - other corporate records after the end of each calendar year.

Destruction of source records

Hard copy records that have been digitised and captured to Records Manager, known as source records, are able to be destroyed if they meet certain requirements.

All WACHS employees must:

- perform quality assurance that the digitised electronic record in Records Manager is of the same quality as the source record and can take its place
- retain the source record for six months after capture to Records Manager.
- retain high-volume transactional source records for the period of time determined by the responsible business area:
 - source records of invoices, which are high-volume transactional records, are to be retained one month after payment.

WACHS employees must not dispose of any source records:

- that do not meet these requirements
- that are State archives from before the year 2000
- for which the physical format is important to understanding or appreciating the record.

In these cases, the original hard copy record must be retained although a digitised electronic access copy may also be created.

2.8 Reporting

Audit logs

Actions taken on all records in Records Manager are auditable including the actions of registering, viewing, editing, emailing and printing of records.

Auditing and reporting

The Manager Records Management must:

- regularly conduct audits and reports of compliance with the [Corporate Recordkeeping Compliance Policy](#) by the methods and to the schedule detailed in [Appendix F: Monitoring](#) below
- provide results of audits and reports to the WACHS Executive.

WACHS managers must ensure that their business area:

- participates in auditing activities when selected
- takes follow up actions to improve recordkeeping compliance if auditing and reporting identifies any issues.

These requirements are supported by Help Guides and further information available via the WACHS [Records Services](#) intranet section.

3. Roles and Responsibilities

All WACHS employees are responsible for keeping records, or ensuring they engage in verifiable business processes that result in keeping records, in compliance with the WACHS [Recordkeeping Plan](#), the [Corporate Recordkeeping Compliance Policy](#) and this procedure.

All staff are required to work within policies and guidelines to make sure that WACHS is a safe, equitable and positive place to be.

4. Monitoring and Evaluation

4.1 Monitoring

Monitoring of ongoing compliance with the requirements of the [Corporate Recordkeeping Compliance Policy](#) and this procedure is carried out by the reporting and auditing methods and according to the schedule detailed in [Appendix F: Monitoring](#) below.

The Manager Records Management is responsible for this monitoring and for reporting the results to the WACHS Executive.

4.2 Evaluation

Evaluation of this procedure is conducted against the [State Records Office Recordkeeping Plan Self-Evaluation Checklist](#) at least every five years or whenever a significant change is identified.

The Manager Records Management is responsible for this evaluation.

5. Compliance

This procedure is a mandatory requirement under the [State Records Act 2000](#).

Failure to comply with this procedure may constitute a breach of the WA Health Code of Conduct (Code). The Code is part of the [Integrity Policy Framework](#) issued pursuant to Section 26 of the [Health Services Act 2016](#) and is binding on all WACHS staff which for this purpose includes trainees, students, volunteers, researchers, contractors for service (including all visiting health professionals and agency staff) and persons delivering training or education within WACHS.

6. References

[State Records Office - Records Management Advice - Recordkeeping Responsibilities and You](#)

7. Definitions

Terms used in this procedure are defined in the Corporate Recordkeeping Compliance Policy in addition to the following.

Term	Definition
Accessibility	The ability to access a record due to security and access controls allowing of access, though the record may not in fact be accessed by any person in any way.
Access	Making use of accessibility to actually access a record. Examples of accessing a record include viewing, transmitting or downloading.
Capture	The process to capture records and information into a recordkeeping system that will support its use, management and preservation over time. This may involve digitising, migrating or encapsulating records and information. Source: National Archives of Australia - Capturing information
Classification structure	Tool for linking records to the context of their creation in a systematic arrangement of business activities according to logically structured conventions, methods and procedural rules supporting security, accessibility and retention and disposal. Source: AS ISO 15489 Information and documentation – Records management – Concepts and principles
Distributed responsibility	A single or several definite locations, positions or business areas do not exist to complete an activity. All WACHS employees must assume the responsibility according to local processes.
Folder	A container in Records Manager to collect records such as documents, emails and sub-folders of similar business activities, processes and transactions. Each WACHS region has its own first level folder record type.
Legacy records	Hard copy corporate records created outside of the currently approved electronic recordkeeping system that must be managed for the full life span of the record.
Metadata	Data that describes records including structural metadata describing the relationship between records such as folder or format, administrative metadata used to manage a record such as access controls and descriptive metadata such as title. Source: SRO - Records Management Advice - Metadata and Discoverability
Non-sensitive corporate record	A record of WACHS business activities, processes or transactions that does not contain sensitive information.

	A record containing information which is classified Official in terms of the Western Australian Information Classification Policy - Business Impact Levels Tool
Recordkeeping Awareness Training (RAT)	The online course that informs each Health employee about good recordkeeping practices and explains their responsibilities in managing records under the <i>State Records Act 2000</i> . Accessible via the Learning Management System. It is a mandatory, once only requirement of the Employment Policy Framework to complete this course.
Register (a record)	The process to capture an electronic or digitised record to the approved recordkeeping system Records Manager to support the record's use, management and preservation in accordance with WACHS Recordkeeping Plan. Involves a WACHS employee selecting metadata as well as system generated metadata.
Sensitive corporate record	A record of WACHS business activities, processes or transactions that contains sensitive information. A record containing information which is classified Official: Sensitive in terms of the Western Australian Information Classification Policy - Business Impact Levels Tool
Significant record	<p>"The criteria for determining which records are Significant are that the activity:</p> <ul style="list-style-type: none"> • Substantially impacts / affects the obligations, responsibilities or liabilities of the State or the agency. • Substantially impacts / affects the whole-of-government function. • Substantially impacts / affects the agency's business, structure or policy. • Substantially impacts / affects the implementation or development of legislation or government policy. • Sets a legal or substantive precedent. • Generates / involves substantial community or public interest, debate or controversy. • Involves / affects property (land, infrastructure, structures, buildings or items) considered to have cultural, Aboriginal, environmental or heritage significance. • Concerns / affects the long term environmental impact on State land, waters and air. • Led or substantially contributed to a major investigation or formal inquiry. • Involves innovative, unique or precedent-setting practices, techniques or methods." <p>Source: General Disposal Authority for State Government Information (DA 2013-017/1)</p>
Source record	Any record in an analogue format (e.g. paper, film, photograph) from which a reproduction in digital format has been created. Source: SRO - Glossary of Terms

State archive record	A record required to be transferred to the State Archives and kept permanently as part of the history of Western Australia because of its significance.
State Archives	The organisation created by the <i>State Records Act 2000</i> to permanently keep and maintain access to State archive records transferred from government organisations such as WACHS.
Temporary record	A record which is not a State archive record and which must be retained for the time period specified by an approved disposal authority, authorised for destruction by a WACHS delegated authority and securely destroyed.
Time expired record	A temporary record which has been retained for the time period specified by an approved disposal authority and is now due to be authorised for destruction by a WACHS delegated authority and securely destroyed.
Transfer	A record permanently leaving WACHS' custody and being received by another organisation who will maintain the record for the remaining life span of the record, including permanent retention. Including transfer of State archive records from WACHS to the State Archives as required by section 32 of the <i>State Records Act 2000</i> .
WACHS-specific Records Manager training	A training course, maintained by the Manager Records Management, setting out the basics of how Records Manager is used at WACHS to capture and manage corporate records.

8. Document Summary

Coverage	WACHS-wide
Audience	All WACHS Employees
Records Management	Non Clinical: Corporate Recordkeeping Compliance Policy
Related Legislation	Public Sector Management Act 1994 (WA) State Records Act 2000 (WA)
Related Mandatory Policies / Frameworks	Employment Policy Framework Information Management Policy Framework MP 0067/17 Information Security Policy
Related WACHS Policy Documents	Cessation of Employment Policy Corporate Recordkeeping Compliance Policy Information Classification and Handling Policy Social Media Policy
Other Related Documents	General Disposal Authority for State Government Information (DA 2013-017/1) SRO Recordkeeping Plan Self-Evaluation Checklist SRO Specification for Digitisation of State Records WACHS Authorisation Schedule WACHS Recordkeeping Plan
Related Forms	Nil
Related Training Packages	Recordkeeping Awareness Training (RAT) WACHS Records Manager training
Aboriginal Health Impact Statement Declaration (ISD)	ISD Record ID: 2275
National Safety and Quality Health Service (NSQHS) Standards	1.07
Aged Care Quality Standards	8
National Standards for Mental Health Services	8.4

9. Document Control

Version	Published date	Current from	Summary of changes
1.00	1 June 2023	1 June 2023	New procedure.

10. Approval

Policy Owner	Executive Director Business Services
Co-approver	N/A
Contact	Manager Records Management
Business Unit	Records & TRIM Services
EDRMS #	ED-CO-23-206932

Copyright to this material is vested in the State of Western Australia unless otherwise indicated. Apart from any fair dealing for the purposes of private study, research, criticism or review, as permitted under the provisions of the Copyright Act 1968, no part may be reproduced or re-used for any purposes whatsoever without written permission of the State of Western Australia.

This document can be made available in alternative formats on request.

Appendix A: Legacy hard copy records management

Hard copy records management is not supported for corporate records, except for legacy records.

WACHS employees are to, where practical, digitise hard copy records and keep and dispose of the source records.

Where this is not practical, WACHS employees must keep the legacy hard copy records according to the following instructions:

- Sort records according to similarity and consecutive date range
- Store records in compliant 'archive' cartons sourced from an approved offsite records storage company.
- Identify each individual carton with a unique barcode.
- List the content and date range of each carton and provide the listing to WACHS Records Services.
- Lodge cartons to offsite storage with an approved supplier.
- Securely destroy legacy hard copy records when authorised.

Appendix B: Retention and disposal authorities

The State Records Commission has approved several disposal authorities for WACHS use.

These consolidate information from a full range of legislation, regulations and guidelines on how long we must keep different records.

Any records to be destroyed must not only meet these minimum retention requirements but be reviewed by the responsible business area and authorised by a Tier 3 officer, in accordance with the WACHS [Authorisation Schedule](#).

Retention and disposal requirements apply to both electronic and legacy hard copy records.

Disposal authorities approved for WACHS use include:

- [General Disposal Authority for Source Records \(RD 2016002\)](#)
- [General Disposal Authority for State Government Information \(DA 2013-017/1\)](#)
- [Patient Information Retention and Disposal Schedule for the WA health system \(PIRDS\) \(DA 2019-008\)](#)
- [Sector Disposal Authority for Health Services \(DA 2017-020\)](#)
- [Ad Hoc Disposal Authority - COVID-19 Health and Vaccination Information \(DA 2021-010\)](#)
- [Sector Disposal Authority for Mental Health Services \(DA 2021-012\)](#)
- [General Retention and Disposal Authority for Incidents and Allegations of Child Abuse or Neglect \(DA 2020-003\)](#)

The format of disposal authorities is usually as in the below example taken from the [General Disposal Authority for State Government Information \(DA 2013-017/1\)](#).

Number	Function / Activity	Description	Disposal Action	Custody
74.1	PROCEDURES	<ul style="list-style-type: none"> • Procedures developed and approved by the agency which apply to its core business operations or activities, for internal (agency) use or external (client) use. • Procedures developed by the agency for whole-of government use. Records include proposals, consultation and comment, major drafts and approved final version.	Required as State archives	Retain 5 years after procedures are superseded, then transfer to the SRO.
74.3	PROCEDURES	Externally produced procedures used by the agency in the conduct of its business or administration. Includes whole-of-government procedures developed by a central or other government agencies, or other external sources.	Destroy	Retain 2 years after superseded, then destroy.
Explanation of field: Reference number	Explanation of field: Title of function or activity	Explanation of field: Description of function or activity and the records it creates	Explanation of field: Final outcome of the record's life span whether State archive or destroyed	Explanation of field: How long it must remain in WACHS custody before disposal

Appendix C: Folder management

Classification structure

In Records Manager, records are classified and organised according to business functions and related activities which generate the records. The classification structure links records to the business function they document, independent of any organisational or administrative structure. The structure is adjusted when WACHS responsibilities change.

Broad to Narrow Structure:

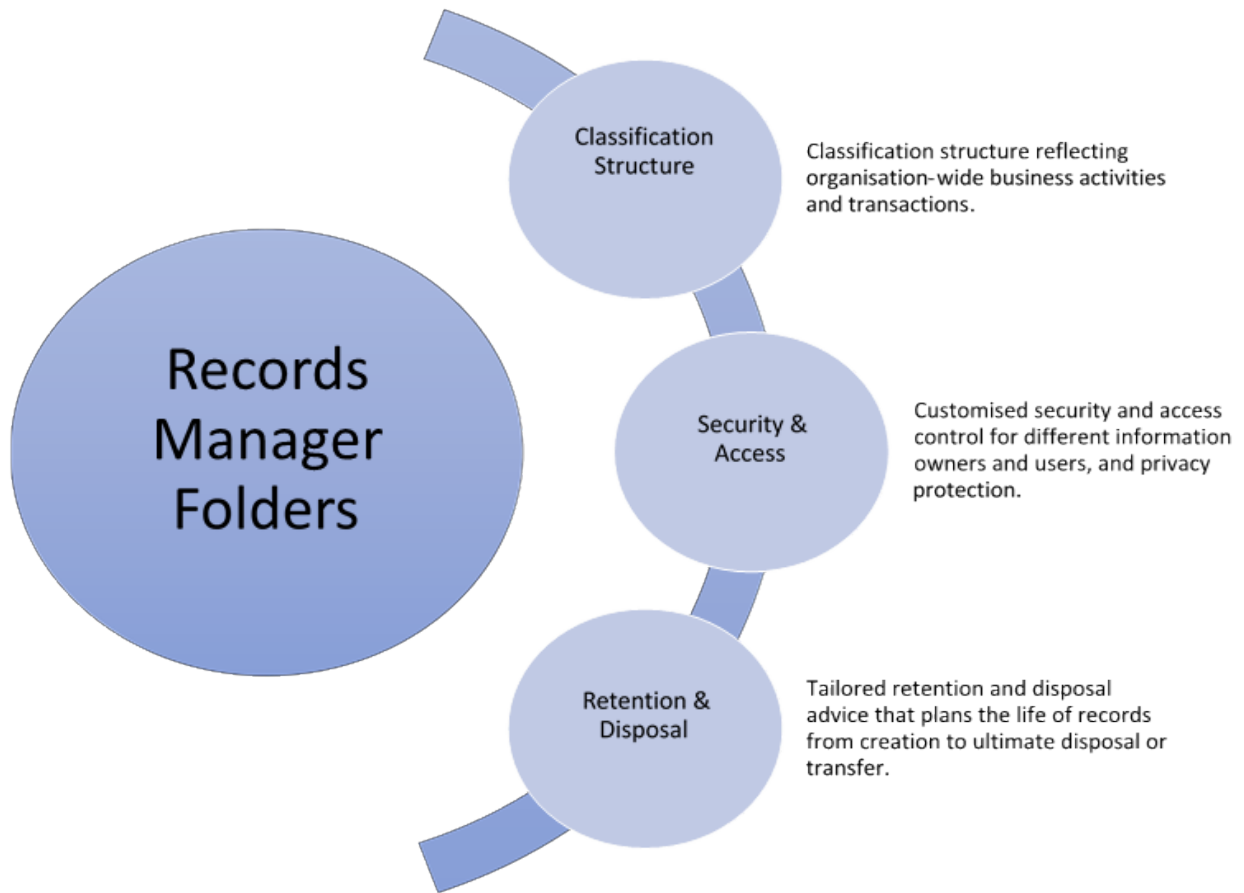
- 1st level term Function: Group of activities that reflect a major responsibility or function.
- 2nd level term Activity: Major tasks, area of service or operation, performed as part of a function.
- 3rd level term Subject: Topic, transaction or work process, program or project, etc. associated with a business activity. Folders are created at this level.

Folders

A Records Manager folder is a container for business records. Unlike a folder in a personal or shared drive, it has recordkeeping functionality to enable WACHS to effectively manage records while they are in use and until such time as they can be legally disposed of, i.e. either destroyed or transferred to the State archive collection.

Folders should contain business records that are:

- findable and readable
- safe from unauthorised access, alteration and deletion
- adequately described, and linked to a relevant business function and activity
- meaningful because the links ensure the context in which the records were created and used is apparent.



Appendix D: Records Manager security model

Information classification

The Records Manager security and access model aligns to the requirements of the [Western Australian Information Classification Policy](#), MP 0146/20 [Information Classification Policy](#) and [WACHS Information Classification and Handling Policy](#).

All information is classified as Official or Official: Sensitive based on the consequences should that information be compromised.

Any Commonwealth Security Classified information is to be managed in accordance with the relevant provision(s) of applicable inter-jurisdiction agreement(s).

User security

- All users completing [Recordkeeping Awareness Training \(RAT\)](#) and Records Manager training are given security and access to records based on their position.
- Each position in Records Manager has a security level. It may also be a member of an access group and/or have a security caveat.
- Log-in to Records Manager is HE number dependent and can only be done from within the Health network.
- Regardless of security or accessibility records must only be accessed by WACHS employees to do their job.

Security level

- All records in Records Manager receive a security level at registration into the system.
- The security level is taken from the folder, which in turn takes its security level from the classification structure.
- The default security level for all records is **Protected (Internal Use)** which matches the information classification **Official**.
- Classification structures likely to contain sensitive information have a security level of **Confidential** which matches the information classification **Official: Sensitive**.

Access controls

- Records with **Protected (Internal Use)** security level are open to WACHS employees to access for the purpose of doing their jobs.
- Records with **Confidential** security level may have access controls applied to further restrict accessibility to particular groups or positions.

- In a limited number of cases (for example, recruitment panels or integrity investigation decision makers) access controls may include restricting accessibility to individuals. However, access controls are usually position based.
- Classification structures classified with **Confidential** security level likely to contain information requiring access controls have access restricted to an access group or groups.
- Access groups containing business areas, positions and cross-business groups (for example, committee membership) are applied for common, repeatable record access control needs.

Security caveats

- A limited number of security caveats may be applied to records classified Official: Sensitive, in addition to security level Confidential. These are:
 - Cabinet in confidence
 - Commercial in confidence
 - Legal privilege
 - Personal information: Employee
 - Personal information: Patient
- They may be applied in addition to, or instead of an access control.

Responsibilities

All WACHS employees are responsible for:

- assessing the information classification of a corporate record, based on the consequences should that record be compromised as detailed in the [Western Australian Information Classification Policy - Business Impact Levels Tool](#)
- when capturing a record to Records Manager selecting a Records Manager folder, within a classification structure with security level and access controls proportionate to the sensitivity of the information the record contains.
- subsequently, it is the responsibility of WACHS employees accessing records to cause to be rectified any discrepancy between information sensitivity and record security level and access controls.

Appendix E: Electronic transmission of corporate records

WACHS employees are to share and distribute corporate records to persons with reason and permission to access these records.

WACHS employees must keep corporate records in Records Manager and transmit them by the secure methods detailed below.

Transmission within WACHS

Links to corporate records, rather than uncontrolled copies, are to be transmitted between WACHS employees to ensure the security and integrity of both sensitive and non-sensitive records. Approved methods for transmission within WACHS are:

- Records Manager reference – Send mail function – attach a reference file which when followed will take the receiver to the original record in Records Manager
- Records Manager hyperlink – Create Open in RM Hyperlink function – copy and paste a hyperlink which when followed will take the receiver to the original record in Records Manager
- Read only hyperlink – Create ‘Read Only’ (view) Hyperlink function – copy and paste a hyperlink which when followed will open the original document or email.

Accessibility of corporate records transmitted by these methods is determined by the security and access control settings of the original records in Records Manager.

WACHS employees must not use less secure methods of transmitting corporate records that bypass the security and integrity controls within Records Manager.

External transmission

Non-sensitive corporate records may be transmitted by email to external parties with reason and permission to access these records.

Sensitive corporate records must be transmitted by secure means authorised by the MP 0067/17 [Information Security Policy](#). Authorised systems for transmission of sensitive corporate records are:

- [My File eXchange \(or MyFX\)](#) which is available for ad hoc use, and as an on demand self-registration based service to send and receive large files, sensitive and confidential information both inside and outside of the WA health system network.
- [My File Transfer \(or MyFT\)](#) which is available to enable regular use, and/or ongoing business process integrated file transfer requirements, to send and receive large files, sensitive and confidential information both inside and outside of the WA health system network. Interested staff can apply for MyFT access via the HFN-030 form. Note that a license fee applies to this use.

This procedure supersedes the Electronic Transmission of Documents Procedure.

Appendix F: Monitoring

Monitoring of the [Corporate Recordkeeping Compliance Policy](#) and this procedure using the following methods and schedule is the responsibility of the Manager Records Management.

Policy section	Policy statement	Monitoring method	Compliance pass	Compliance fail	Schedule
2.1	Create records	Report – Records registered and edited	User registered three or more documents and three or more emails in Records Manager.	User registered fewer than three documents and/or fewer than three emails in Records Manager.	Quarterly
		Audit – Business process	All records of a known business process with clear documentary products are easily discoverable by colleague.	All records of a known business process with clear documentary products are not able to be easily discovered by colleague.	Quarterly. Two business processes per year, checked twice six months apart.
2.2	Capture and control records	Report – Records registered and edited	User edited three or more records in Records Manager.	User edited fewer than three records in Records Manager.	Quarterly
		Audit – Sampled	A sample of 24 records are assessed as being contained within a Classification Structure matching the business activity of the records sampled.	A sample of 24 records are assessed as being contained within a Classification Structure that does not match the business activity of the records sampled.	Quarterly

Policy section	Policy statement	Monitoring method	Compliance pass	Compliance fail	Schedule
2.3	Secure and protect records	Audit - Sampled	A sample of twelve Confidential and twelve Protected security records are assessed as having security proportional to the sensitivity of the information they contain.	A sample of twelve Confidential security records includes records assessed as being Official in Information Classification terms and/or a sample of twelve Protected security records includes records assessed as being Official: Sensitive in Information Classification terms.	Quarterly
2.4	Access records	Audit – Business process	Records of an identified business activity are confirmed by the responsible business area as having been accessed by persons in positions who need to access the records to do their job.	Records of an identified business activity are flagged by the responsible business area as having been accessed by persons not in positions who need to access the records to do their job.	Quarterly. Two business processes per year, checked twice six months apart.
2.5	Dispose of records	Report – Disposed of records	Number of records disposed of equals number of records authorised for disposal.	Number of records disposed of is not equal to number of records authorised for disposal.	Yearly
		Audit – Sample of source records	Sample of scanned electronic records compared to source paper records meets SRO digitisation standard.	Sample of scanned electronic records compared to source paper records does not meet SRO digitisation standard.	Twice a year