ACT Government | ACT Health

POLICY DOCUMENT

Records Management Policy

Document number	**AHDPD-09:2022**
Effective date	09 August 2022
Review date	09 August 2027
Author branch	Office of the Chief Information Officer, Digital Solutions Division
Endorsed by	Digital Committee
Audience	ACT Health staff
Version number	1.0

Contents

Policy Statement

Excellent recordkeeping is critical to the ACT Health Directorate's (ACTHD) corporate governance and operational efficiency, provides essential evidence of business activities and transactions, and demonstrates accountability and transparency in ACTHD's decision-making processes.

Records must be captured and retained in the corporate recordkeeping system, Objective, or the functional business system.

Records must not be captured and retained on OneDrive, network shared drives or computer hard drives, MS Outlook or temporary storage media such as USB devices.

Purpose

The purpose of this policy is to provide the direction for the management of records, to guide the creation, maintenance, storage and disposal of ACTHD records and identify staff responsibilities in creating full and accurate records in accordance with all relevant legislation and regulatory requirements. ACTHD is committed to establishing and maintaining records management practices that meet its business needs, accountability requirements and stakeholder expectations.

Excellent records management practices will assist ACTHD to achieve organisational accountability, improve productivity and reduce risks by ensuring privacy is protected. Trusted information that is well-described, stored in approved locations and accessible to staff when needed, is essential to ensuring ACTHD can provide evidence of decisions, service delivery, when action was taken and by whom.

Policy principles

These principles underpin how records will be managed within ACTHD. They establish our values and approach to information, its use and ongoing management throughout. The creation, capture and management of records are integral parts of conducting business, in any context.

1. Records, regardless of form or structure, are authoritative evidence of business when they possess the characteristics of authenticity, reliability, integrity and useability.
2. Metadata describes a record and is a component of a records. Metadata describes and chronicles the context, content and structure of the records, as well as their management through time.
3. Decisions regarding the creation, capture and management of records are based on the analysis and risk assessment of business activities, in their business, legal, regulatory and societal contexts.

4. Systems for managing records, regardless of their degree of automation, enable the application of records controls and the execution of processes for creating, capturing and managing records. They depend on the defined policies, responsibilities, monitoring and evaluation, and training in order to meet identified records requirements.

The above principles align with the international standard, ISO 15489.1: 2017 Records Management, Part 1: Concepts and Principles.

Scope

This policy applies to all administrative records from the time of creation or capture and covers:

- all aspects of ACTHD's business operations
- all types and formats of records created to support business activities
- business applications used to create, manage and store records, including business systems, databases, email, voice and instant messaging, websites and social media applications
- organisations and businesses, including their employees, to which ACTHD has outsourced its functions or activities, including associated recordkeeping responsibilities.

The policy will be supported by procedures that will enable an understanding of how records are:

- Created, collected and captured
- Organised, accessed and secured
- Governed by corporate rules and captured in authorised systems
- Used appropriately, accessible and protected as required, and
- Defensibly disposed.

Ownership

All records generated by full-time, part-time staff, casual staff, volunteers, consultants and /or contractors as part of their duties are Territory records and belong to the ACT Government and not to individual employees in ACTHD. ACTHD is the custodian of all records created.

Exclusions

Excluded from this policy are ACT Health clinical records.

Roles and Responsibilities

Position	Responsibility
Every employee	All staff must adhere to ACT Health's Records Management policy, procedures and standards in maintaining records as required within their duties and to the *Territory Records* Act *2002*. Staff must understand the recordkeeping requirements and responsibilities specified within this policy and how they apply to their role. Staff are responsible for the creation and management of records in regard to the work they perform on behalf of the organisation. Staff must routinely create full and accurate records of work activities including records of all substantive decisions and actions. Staff must ensure records are captured into the appropriate system so that they are accessible and appropriately secured as needed. Staff will be held accountable for unauthorised access to information. Staff must not destroy records without the authorisation from ACTHD's Chief Information Officer, except through the appropriate application of Normal Administrative Practices (NAP) of the *Territory Records Act 2002* – (further information below). Staff must undertake annual records management training as required
Director-General	The Director-General is ultimately responsible for the management of records, promotes compliance with this policy, supports and fosters a culture of good recordkeeping in the organisation, and ensures the Records Management Program is adequately resourced.
Chief Information Officer (CIO)	Develops policy, strategy, resourcing and systems to ensure the successful operation of approved records systems; Approves additions to the systems of record, compliant with standards, to be available to manage records and information; Owner of the Records management program, policy and supporting procedures; Oversees the records management program; Coordinates compliance of systems against the Territory Records Office (TRO) standards for all records; Authorising the disposal of records; Reports to the Director-General on records management.

Position	Responsibility
Digital Committee	Reports to ACT Health Executive Board on records management matters
Director Records Management	The Director Records Management is responsible for implementing and monitoring recordkeeping legislative and best practice requirements across ACTHD. Providing input into records management business plans. Identification of records management requirements, The development, implementation and periodic review of the policy and procedures to ensure currency with best practice/standards. Reporting to the CIO on records management issues.
Digital Solutions Division (DSD) staff	DSD staff are responsible for maintaining the technology for business systems, including appropriate system accessibility, security and back-ups in accordance with ICT policies.
CMTEDD Digital Records Support Team	Maintaining and administering the Electronic Document and Records Management Systems Provision of technical and functional support and advice Ensuring systems are updated where there are changes to configurations, such as, business functions and activities in the WhoG thesaurus and changes to records authorities.
The Agency Security Advisor	The Agency Security Advisor provides advice on security policy and guidelines associated with the management of records
Managers and Supervisors	Managers are ultimately responsible for ensuring that all records produced by their area are captured, maintained and accessibly stored in the Objective, EDRMS, in accordance with this policy. Ensuring that staff, consultants and / or contractors under their responsibility are made aware of their records management obligations and what information resources and training is available to them. Advise the Director Records Management of any changes in the business environment, such as restructures. Ensure that all staff under their responsibility undertake annual records management training. Ensure that record and information management responsibilities are expressed in worker role descriptions, performance management plans

Position	Responsibility
Volunteers, contractors, consultants and service providers	Volunteers, contract staff, consultants and service providers must create and manage records in accordance with this policy and supporting procedures Undertake necessary training

Requirements

Creation and capture

ACTHD has a responsibility under the ACT Government's legislative framework and standards issued the Territory Records Office to create and maintain full and accurate records of business. Records created or received must be captured into the corporate recordkeeping system, Objective, and described and classified according to ACTHD standards, procedures and business rules.

All employees must ensure that guidance is followed to ensure the creation and capture of records of activities, decisions and actions made while undertaking ACTHD business to:

- Explain why decisions or actions have been made or taken which impact upon individuals or organisations
- Enable current and future employees to take appropriate action and make well informed decisions
- Protect individuals or organisations affected by decisions or actions
- Enable an authorised person to examine the conduct of ACT Health business, and
- Protect the legal, financial and other rights of ACT Health staff and stakeholders.

Records created, received or discovered which contain information that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage will be appropriately managed, protected and made accessible if needed.

Guidance is provided in the records management procedures on the capture and management of records.

Storage and preservation

Digital recordkeeping

The underpinning concept of the records capture process is that records that are born digital should stay digital. Where hardcopy documents are received, they must be digitised and captured in Objective as soon as possible after receipt.

To ensure digital records remain accessible and useable for as long as required, records must be captured into systems where:

- Sufficient metadata can be captured around the records so they can be understood, that is:
    - the records have context such as who created it, when and for what purpose
    - the history and use of the records can be viewed
    - Security status and rights or restrictions on access are linked to records
- The metadata is persistently linked to the records;
- Audit trails track actions taken on the records;
- The records are protected from unauthorised access, alteration, removal, deletion or destruction; and
- Records of long-term value are securely preserved in formats that will be accessible over time.

The following characteristics are essential in considering the status of documents as records and minimum requirements for systems for recordkeeping:

Records must be	Systems must provide the following minimum metadata	Systems must have the following functionality	Recordkeeping processes
•Complete and unaltered •Adequate •Accurate and trustworthy •Authentic •Findable and readable •Secure from unauthorized access, alteration and deletion.	•Date of creation •Creator •Title •Unique Identifier •Business function/activity •Creating Application (where applicable) •Record Type (e.g. letter, memo, report, contract , schematic, blog, or locally defined types) •Management / audit history •Disposal information, e.g. records authority, disposal class ID, disposal action, disposal trigger date, disposal action due. •Use history	•Capture read only versions of digital records •Retrieve and present digital records in human readable form •Restrict or permit access to records by specified individuals or groups •Capture and manage the minimum required recordkeeping metadata. •Manage the creation, registration, classification, access, preservation and disposal of records, incorporating version control •Provide audit history, retaining metadata on disposal of records in alignment with approved records authorities	•Creation and capture •Linking records to business context •Linking records to people, agents and relationships between records (contained, aggregation, contained by) •Applying or changing access rules •Secure storage •Measures for continued useablity •Migration and conversion •Disposition including destruction and transfer

Figure 1: Digital recordkeeping requirements

Electronic storage facilities, such as shared network drives, local computer drives, USBs, CD ROMS etc. are temporary storage solutions which do not meet the requirements for records management. Shared network drives are only to be used for information of an ephemeral nature, graphics, linked spreadsheets etc. Further guidance is provided in the records management procedures.

Digitisation

As hardcopy documents are received by ACTHD, they must be digitised and captured in the EDRMS, Objective. As part of a business process the scanned image becomes the official record which will be used in the transaction of business.

Digitisation projects are retrospective or project-based digitisation of existing sets of non-digital records to enhance accessibility, maximise re-use or for preservation purposes. In digitisation projects, the action is already completed and was undertaken on the hardcopy records. Digitisation projects may be undertaken to facilitate access to records that have been transferred to the Territory Records Office.

Digitisation projects must be authorised by the Chief Information Officer.

The Territory Records Office provides guidance on the technical specifications for digitisation. Further detail can be found in the record management procedures.

Physical records

ACTHD retains many physical records created prior to the transition to digital recordkeeping.

Physical records are stored in ACT Health's storage facility. The Records Management team coordinates the storage and retrieval of physical records. Requirements for managing physical records are detailed in the records management procedures.

Physical records are maintained in accordance with the Territory Records Office Guideline, Principle 5: Protect Principle.

Retention and disposal

Disposal of records and information, in any format, or held in any location, system or application must be:

- Approved by the Territory Records Office by authorised disposal actions in relevant records authorities and support ACTHD procedures, and
- Approved by the business owner of the records and the Chief Information Officer.

Records required for retention as Territory Archives and those that can be destroyed on expiry of the appropriate disposal sentence are identified in whole of government and sector specific records disposal authorities.

Only records that have been appraised and identified in conjunction with records disposal authorities approved by the Director of Territory Records and endorsed by the Chief Information Officer as allowable for destruction will be destroyed.

Records authorised for destruction must be done by secure means. This means that processes will be in place to ensure the irreversible destruction of digital and physical records.

All system migration or decommissioning of ACT Health business systems or applications must ensure that authorised disposal actions are satisfied for any stored records. After successful migration from one system to another, the destruction of information and

records is permitted upon satisfaction that the migrated information is functionally equivalent to the source record for business, legal and archival purposes. Guidance is provided by the Territory Records Office on system decommissioning, refer to Records Advice, Decommissioning Business Systems, 2019.

Normal administrative practice

Records can be disposed of outside of the above under the Normal Administrative Practice (NAP) provisions of the *Territory Records Act 2002*. These records are short term, facilitative or ephemeral in nature and are not identified in the relevant records authorities.

Staff must not destroy information or records outside of the above requirements.

Records that must be retained, even if the authorised disposal action in a relevant records authority has been satisfied, are those:

- Likely to be required for a pending or anticipated, inquiry or legal proceeding;
- Relating to an access request submitted under FOI, for example, and
- Identified in a disposal freeze imposed by the TRO, such as records pertaining to the subject of a Royal Commission.

Other than for records retained based on the three dot points above, should the business owner of a record decline to authorise destruction of a record after it is due for destruction, the business owner's cost centre will be liable for the full cost of storing and maintaining the records. The Chief Information Officer will provide an annual report to the Director-General and Chief Finance Officer on all such retentions and charges.

For further information refer to the Records Management Procedures, Normal Administrative Practice.

Protection of records

Security classification of records has been implemented in the EDRMS, Objective. All records must be assigned an appropriate label. The following labels are available:

Term	Definition	Examples
For Official Use Only	This marking is to be used on information when its compromise may cause limited damage to national security, ACT Government directorates, commercial entities or members of the public.	Tender responses Correspondence outlining contractual requirements
Sensitive	This marking is to be used on information where the: • secrecy provisions of enactments may apply; and/or	• Committee records that have not been approved for publication (i.e., in-camera evidence, minutes of private

Term	Definition	Examples
	• the disclosure of which may be limited or prohibited under legislation.	meetings, draft reports). • Private advice provided to members.
Sensitive: Legal	This marking is used to identify information that is subject to legal professional privilege.	Correspondence seeking or receiving advice from any legal professional body, including the ACT Government Solicitor.
Sensitive: Personal	This marking is used for information that contains a fact or opinion, whether true or not, about an individual or an individual who is reasonably identifiable. This marking should be applied to all sensitive personal information as defined under the *Information Privacy Act 2014* and personal health information under the *Health Records (Privacy and Access) Act 1997*. Staff handling Sensitive: Personal information should also be aware of their obligations under the Privacy Policy.	Personnel records
Sensitive: Cabinet	This marking is to be applied to: • any document including but not limited to business lists, minutes, submissions, and memoranda that has been submitted or proposed to be submitted to Cabinet. • official records of Cabinet. • any other information that would reveal the deliberations or decisions of Cabinet, or matters submitted, or proposed to be submitted to Cabinet. Additional handling requirements for Cabinet information are outlined in the ACT Government Cabinet Handbook.	• Cabinet submissions • Budget submissions and business cases

Access

Public access

Under the *Freedom of Information Act 2016*, members of the public have the right to apply for access to and, in the case of personal information amendment of information assets held

by ACTHD. The *Freedom of Information Act 2016* applies to all information and records controlled by ACTHD, regardless of the format or system in which it is stored. FOI requests are coordinated by the FOI Team.

Note: this does not relate to Clinical/Patient records.

Information sharing

Records should only ever be made available to other ACT Government Directorates, Agencies, Institutions or Taskforces, private contractors and non-government organisations representing or contracted out by ACT Government or ACT Health such as legal firm, auditor in response to a formal request, an established process or procedure, a regulatory requirement or other established obligation or condition.

Where information and records need to shared this can be done by using the endorsed corporate solution (Kiteworks) to ensure a secure environment for collaboration and sharing with third parties.

Arrangements external parties

Contracts or agreements with external parties where ACTHD has outsourced any function or activity, or with whom ACTHD has entered into any service arrangements, must include records and information management provisions. These must include:

- records management responsibilities of the contractor, and
- clarity around the custody and ownership of records.

This will ensure compliance with our legislative obligations relating to the management and use of our records and minimise risks associated with the external storage of records and information, and ACTHD's right to access information held by the contractors.

Continuous improvement and monitoring

The Records Management team will undertake monthly performance monitoring against the records management program and policy as part of the Monitoring and Compliance Program. Results are reported to the Chief Information Officer for reporting to the Digital Committee.

ACTHD will also report regularly to the TRO.

Records Management

Authorised recordkeeping system

ACT Health's authorised and compliant EDRMS is Objective. Records Management will ensure that the recordkeeping system is measured and monitored to ensure that the identification and retrieval of information remains consistent and meets the needs of the Records Management Program and business operations.

The following functional business systems are endorsed for the capture and storage of specific records, information and data:

- JIRA (digital solutions division service request catalogue)
- HR21 (employee self-service for leave, pay, position occupancy)
- HRIMS (learning management system)
- IAM (system and building access requests)
- One Gov Service Centre (forms for non-standard leave,
- Oracle ERP/FMIS (financial reporting)
- Riskman (incident and risk management)
- Converga/APIAS (invoice processing)

Any system that captures records must have the ability to manage the following processes, as a minimum:

- be capable of collecting all information and records related to a transaction, matter or activity, to ensure the records are full and accurate;
- be capable of capturing content, structure and context of the record, assigning business classification terms and retention actions;
- provide adequate and compliant storage of records;
- provide protection of record integrity and authenticity;
- ensure the security of records;
- be readily accessible to staff who need to use the records contained within the system, provided no legislative restrictions exist, for as long as the record is needed;
- undertake the disposal of records in accordance with the *Territory Records Act 2002* and standards made under that Act;
- ensure the recoverability of records in the event of a disaster; and
- ensure the availability of records in a useable format through technology changes and migration and can be imported / exported without loss of content and metadata.

Evaluation

Appropriate strategies, processes, applications and tools that ensure records of business activities are made and kept will be continually monitored to:

- support the effective management of information and records;
- continually advance strategic priorities, and
- meet client needs and community expectations.

Outcome Measures	Method	Responsibility
Compliance with the requirements of the *Territory Records Act 2002* and the Territory Records (Records and	Reporting to the TRO on the ACT Health records management program	Territory Records Office

Outcome Measures	Method	Responsibility
Information Governance) Standard 2022		
Records Management has established key performance indicators which are reported to the CIO on a regular basis, and available on request.	Records management monitoring program has been implemented Records management practices will be subject to periodic internal audits, the TRO or the ACT Government Auditor-General or others, as endorsed by the Director-General of ACT Health	Digital Committee
ACT Health staff are capturing records in the corporate recordkeeping system, Objective	Records management monitoring program has been implemented Capture of records, file titling will be monitored and remediation activities undertaken as required. Training for all staff is mandatory	Internal Audit Managers & Supervisors
The Records Management (RM) Team provide professional services that support business need and provide services that facilitate the creation of full and accurate records	Records management monitoring program has been implemented Internal audit conducted as required. Service level catalogues outline RM service provision and responsibilities of the business teams. RM Team submits an annual work plan detailing work packages that will meet compliance, business need and provide value for money.	CIO

References and Related Documents

References

- AS ISO 15489-1:2016 - Information and documentation — Records management — Part 1: Concepts and principles
- SA/SNZ TR ISO 26122:2008 – Work Process Analysis for Recordkeeping
- AS: 5044-2010 - AGLS Metadata Standard.
- AS/NZS 5478:2015 Recordkeeping Metadata Property Reference Set.

- ISO: 16175-1:2020 - Information and documentation — Processes and functional requirements for software for managing records — Part 1: Functional requirements and associated guidance for any applications that manage digital records
- The Territory Records Office Standard and Guidelines for Records and Information Governance

Legislation

- *Territory Records Act 2002*
- *Dangerous Substances Act 2004*
- *Freedom of Information Act 2016*
- *Evidence Act 2011*
- *Information Privacy Act 2014*
- *Health Records (Privacy and Access) Act 1997*
- *Electronic Transactions Act 2001*
- *Financial Management Act 1996*
- *Medicines, Poisons and Therapeutic Goods Act 2008*
- *Public Sector Management Act 1994*
- *Radiation Protection Act 2006*
- *Work Health and Safety Act 2011*
- *Working with Vulnerable People (Background Checking) Act 2011*

Supporting Documents

A range of policies relevant to the management of records must be applied alongside this policy, including:

- ACT Government's Open Government Policy
- ACTPS Digital Records Policy
- ACT Government Policy on the Selection and Implementation of Electronic Document and Record Management System (EDRMS) Capabilities

Definitions

Term	Definition
Clinical Record	Also referred to as a "Health Record"
Business classification scheme (BCS)	A conceptual representation of the business functions and activities performed by an organisation. Represented as a hierarchical scheme for identifying and defining the functions, activities and transactions an agency performs in the conduct of its business, and the relationships between them. Also referred to as a "Thesaurus".
Digital Record	A record that is communicated and maintained in a digital format. Same as an electronic record.
Disposal	A range of processes associated with implementing decisions such as retention, damage or alteration, deletion or destruction of records. Disposal may also include the migration or transmission of records between systems, and the transfer of custody or ownership of records. Disposal of a record, includes the deletion or destruction of the record from a recordkeeping system.
Electronic document and records management system (EDRMS), Objective	Objective is the corporate recordkeeping system for ACT Health. Objective is designed to capture, manage and protect business information in order to ensure access to authoritative records and meet governance and regulatory compliance obligations.
Freedom of Information (FOI)	Freedom of information provides citizens the right to request government information.
Functional Business System	A functional business system is a system that captures, creates and stores a specific type of information, such as financial, service requests or risk reporting. This information is usually entered into the system in a formatted and structured method.
Health Record	Means any record, or any part of a record: (a) held by a health service provider and containing personal information; or (b) containing personal health information
Metadata	Structured descriptive data that must be captured in a recordkeeping system to enable a record to be understood, verified, managed and used. It is data

Term	Definition
	describing context, content and structure of records and their management over time.
Normal Administrative Practice (NAP)	A process that allows agencies to destroy certain types of low value and short-term information in the normal course of business.
Records	Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business (AS ISO 15489)
Records Management	The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records (AS ISO 15489).
Records Management Program	A records management program is implemented in ACT Health in compliance with section 16 of the Territory Records Act 2002. The program is documented which describes the means by which ACT Health will manage its records. The program is approved by the agency's Principal Officer (Director-General).
Territory Records Office (TRO)	The Territory Records Office assists Territory agencies to meet their records management requirements. The Territory Records Office is responsible for the implementation of the *Territory Records Act 2002* and the regulation of recordkeeping across the ACT Government.

Version Control

Version	Date	Comments
0.5	15/07/2022	Consultation draft
1.0	8/8/2022	Updated and finalised draft

Disclaimer: *This document has been developed by the ACT Health Directorate specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at his or her own risk and the ACT Health Directorate assumes no responsibility whatsoever.*