



ACT
Government

ACT Health

Records Management Program (RMP)

Document number	AHDPD-02-2022
Effective date	25 March 2022
Review date	01 January 2027
Author branch	Office of the Chief Information Officer, Digital Solutions Division
Endorsed by	Digital Committee
Audience	ACT Health
Version number	1.0

Contents

Introduction	1
Compliance	1
Responsible Senior Manager	1
Relationship with the Director of Territory Records	1
Records management framework	1
Principles	1
Principle 1: Strategy	1
Principle 2: Capability	2
Principle 3: Assess	3
Principle 4: Describe	4
Principle 5: Protect.....	4
Principle 6: Retain	6
Principle 7: Access.....	8
Implementation, compliance and reporting.....	9
Availability for public inspection.....	9
Review	10
Authorisation	11
Version Control	12

Introduction

The *Territory Records Act 2002* obliges the Director-General, ACT Health to ensure the organisation and its staff comply with the *Territory Records Act 2002*. This includes the development, approval and implementation of this Records Management Program (RMP).

Compliance

This RMP addresses all elements set out in section 16 of the *Territory Records Act 2002* and meets the requirements set out in the Standard for Records, Information and Data released by the Director of Territory Records.

Responsible Senior Manager

The Chief Information Officer (CIO) is the Executive in charge of records and information management, including the implementation and regular review of this RMP. A key responsibility includes:

- Implementation and regular review of this RMP.
- Ensuring all staff, volunteers, consultants, contractors and outsourced providers comply with the policy and procedures for records, information and data management.

Relationship with the Director of Territory Records

The Director of Territory Records:

- oversees the administration of the *Territory Records Act 2002*;
- provides an advisory and compliance-monitoring service;
- may provide reports to the relevant Minister on records;
- provides/oversees information and data management capabilities; and
- issues notifiable instruments (standards) that relate to the management of records, information and data.

Therefore, arrangements are in place to liaise with the Director of Territory Records for:

- examining the operations of the RMP and compliance with the *Territory Records Act 2002*
- advising on the outsourcing of any aspect of records, information and data management responsibilities
- requesting assistance, advice and training in relation to records, information and data management
- reporting on compliance with the *Territory Records Act 2002*, the RMP, and records, information and data management capabilities
- resolving disputes regarding compliance with the *Territory Records Act 2002* and the RMP.

Records management framework

ACT Health Records Management Program Framework

Program Principles

Strategy, Capability, Assess, Describe, Protect, Retain, Access - Principles to ensure records management practices support open & accountable government & records are managed & preserved

Capabilities

- Skilled records management resources
- Corporate recordkeeping system, Objective
- Whole of Government tools – business classification scheme, records authorities
- Digital preservation
- Training and communication.



Requirements

- Territory Records Act
- Territory Records Office (TRO)
- TRO implementation guidelines
- TRO Agency self assessment checklist
- Best practice international standards

Governance

- Digital Committee
- Strategy and planning
- Records management program, Record management policy and procedures
- Roles and responsibilities
- Annual work plans
- Performance monitoring & compliance
- Internal audits

Principles

The ACT Government’s Standard for Records and Information Governance outlines Records Management best to encourage open and accountable government by ensuring that Territory records are managed and preserved in accessible formats to meet business requirements and community expectations.

To achieve this, the following section outlines the seven principles from the standard, the intent of the principles and the requirements implemented to meet those principles. The seven principles are:

1. Strategy
2. Capability
3. Assess
4. Describe
5. Protect
6. Retain
7. Access

Principle 1: Strategy

Recordkeeping must be planned, rather than ad hoc or reactive. Strategic management for recordkeeping processes allows organisations to set and understand their recordkeeping objectives, manage risk, and plan for and respond to change. Particularly in the digital environment, records will not be created and captured if they are not actively considered and planned for.

Organisations must strategically manage records, information and data by following guidelines for:

- developing a Records Management Program; and
- developing and promulgating a Records and Information Governance Policy and supporting procedures and guidelines.

Requirements, Strategy and Governance

ACT Health will strategically manage business records by ensuring:

- a RMP is developed
- a records management policy is developed and communicated to all staff

The RMP is approved and published on the ACT Health website.

The Records Management Policy is approved and published on the ACT Health website.

The Program and Policy have been communicated and introduced to staff through a training and awareness program.

<ul style="list-style-type: none"> the program and policy are supported by procedures and guidelines 	<p>Records Management Procedures support the implementation of the RMP and policy. These procedures are available to staff through the ACT Health Intranet.</p> <p>The Digital Committee has a remit to provide strategic oversight of records management. The Digital Committee reports to the ACT Health Executive Board.</p>
---	---

Principle 2: Capability

Recordkeeping strategies and processes cannot be effectively implemented if they are not supported by appropriate resources, including skilled staff, adequate systems and tools, and funding.

Organisations must establish and maintain appropriate records and information governance capabilities by following guidelines for:

- identifying and providing financial, human and other resources for records and information governance;
- planning for and measuring the performance of records and information governance activities; and
- reviewing and improving performance to meet the changing requirements of government business.

Requirements, Capability assessment and maturity development	
<p>ACT Health will ensure records management capability is established and maintained by:</p> <ul style="list-style-type: none"> identifying and providing financial, human and other resources for records, information and data management; planning for and measuring the performance of records, information and data management activities; and reviewing and improving performance to meet the changing requirements of government business 	<p>The Director-General, ACT Health, in association with the Chief Information Officer (CIO), will report annually to the Director of Territory Records on its records, information and data management capabilities using the Compliance Checklist Tool provided by the Territory Records Office or as required by the Annual Report Directions.</p> <p>A monitoring and compliance program is in place to monitor records management performance, systems and processes, identify corrective actions, and plan for improvements.</p> <p>Annual plans are developed and implemented to build capability-maturity. Annual plans are based on calendar year and include planned initiatives for implementation.</p> <p>Mandatory training for all staff in ACT Health on recordkeeping obligations.</p> <p>An appropriately resourced and supported Records Management Team provides skilled resources to support ACT Health in records management.</p> <p>A Service catalogue details the provision of services and expectations.</p>

Principle 3: Assess

Recordkeeping systems and processes may be misdirected or inadequate if the organisation does not assess and understand its recordkeeping requirements. This includes understanding its needs to create, describe, protect, retain and provide access to records.

Organisations must assess their records and information governance requirements by following guidelines for:

- establishing processes for identifying the records they need to create and keep, including by supporting 'records by design' approaches to business systems development;
- ascertaining the significance of their records and the risks that are addressed by, or arise from, their creation and management
- managing records in accordance with their significance, risk and other relevant factors.

Requirements, Capturing and managing full and accurate records

ACT Health will assess records by following guidelines for:

- establishing processes for identifying the records, information and data they need to create and keep;
- creating and managing full and accurate records;
- ascertaining the significance of their records, information and data; and
- managing records, information and data in accordance with their significance and other factors.

ACT Health works with the Territory Records Office to develop Records Disposal Schedules that identify the records ACT Health must create to make and keep full and accurate records of its activities.

ACT Health is committed to processes for identifying its records and their significance that are accountable, consistent, objective, comprehensive, contextualised and documented.

The following support the requirement to create full and accurate records of ACT Health's activities:

- Records management procedures provide detailed guidance to staff on the creation and management of ACT Health records.
- Guidance is provided to business teams on the corporate recordkeeping system, Objective.
- All ACT Health policies and standard operating procedures have a records management component to identify what records are required to be created and where they will be stored.
- The corporate recordkeeping system, Objective, is the official store for administrative records.
- The secondary recordkeeping system HP TRIM continues to be supported for the management of short term legacy paper records.
- A system register has been developed by the Digital Solutions Division as an index with information outlining relationships between business systems, business owners and the records contained in the systems. Recordkeeping metadata requirements are outlined and linked from this system register.

Requirements, Capturing and managing full and accurate records

- An information asset register has been developed to identify high value / high risk records supporting regulatory functions.

Principle 4: Describe

Records cannot be reliable, retrievable or understood if they are not adequately described. This involves capturing and preserving metadata about the record's creation, content, business context and use.

Organisations must deliberately control records, information and data by following guidelines for:

- ensuring appropriate and sufficient descriptive elements are incorporated into the systems that manage records; and
- ensuring the descriptive elements are managed appropriately so that authenticity, usability and reliability of the records are protected.

Requirements, Metadata management

ACT Health will control records by ensuring:

- appropriate and sufficient descriptive elements are incorporated into the systems managing records, information and data; and
- the descriptive elements are managed appropriately so the authenticity, usability and reliability of the records, information and data are protected.

ACT Health complies with recordkeeping metadata standards endorsed by the Territory Records Office. ACT Health uses the Whole of Government Recordkeeping Thesaurus to classify its records, according to the business functions and activities they represent. Requirements to capture metadata for ACT Health's records are contained in standard operating procedures for its business activities and in the following specific procedures:

- Records management procedures, and
- User guides for the corporate recordkeeping system, Objective.

Ongoing review and associated quality assurance processes of the capture of records in the Objective system includes a review of file titling and the capture of metadata on files, folders and documents.

Principle 5: Protect

To ensure their ongoing reliability, usability and integrity, and to protect the legitimate interests of records creators, user and subjects, records need to be protected from inappropriate access, alteration or disposal.

Organisations must manage the appropriate storage and preservation of records by following guidelines for:

- identifying the protection requirements for their records; and
- ensuring appropriate protection measures are in place.

Requirements, Protecting records

ACT Health will manage the appropriate storage and preservation of records, information and data by following guidelines for:

- identifying their records, information and data protection requirements; and
- ensuring appropriate protection measures are in place.

Arrangements are in place to protect records, information and data. This includes ensuring the continued appropriate access to records, information and data for as long as they are required to be kept in accordance with the *Territory Records Act 2002* (as defined by records disposal authorities). This includes the identification of endorsed locations for records storage, both in hard copy and digital form.

Physical records

- Records are stored in facilities in conditions that will ensure the records will not unduly deteriorate or be affected by pests or extremes of temperature.
- Storage facilities are securely protected with a range of measures that meet protective security requirements.
- Shelving, equipment and containers used for storing records are secure, accessible and protected from deterioration.

Digital records

Security in the corporate recordkeeping systems, Objective, is open by default. Records are protected by:

- Provision of a secure working space for each Branch/Division;
- Personnel records have necessary restrictions to protect staff;
- Security clearance at the level of Negative Vetting Level 1 is required for staff and contractors with elevated access rights to business systems;
- Security classifications are implemented;
- Sharing of information with external stakeholders is undertaken using Objective Connect which is rated to Protected to ensure records and information are shared securely;
- Guidance is provided in the records management procedures and user guidance for Objective, and
- A Data Breach Policy is in place.

Arrangements are in place to protect records, information and data in the custody of volunteers, consultants,

Requirements, Protecting records

contractors and outsourced providers to ensure the assets are returned or managed in accordance with the *Territory Records Act 2002*. This is done by:

- Clauses in contracts to provide direction on requirements for the management of ACT Health records, and
- Exit procedures for staff, contractors and volunteers to ensure records are managed appropriately. This requires sign off from Records Management Team.

The preservation of high value / high risk records is addressed through the following:

- Digitisation project for records requiring long term preservation such as Retain as Territory Archive (RTA) records;
- Migrating records from CD ROM, floppy disc and USB devices to Objective;
- Migrating records from shared drives to Objective,
- Migrating digital records from HP CM to Objective where appropriate; and
- Using PDF/A as the preferred format for the preservation of electronic records.

Guidance is provided to staff in the records management procedures.

Principle 6: Retain

Records cannot fulfil their functions of protecting rights and entitlements and preserving business and community memory if they are not retained for as long as those requirements remain. At the same time, recordkeeping processes will be inefficient if records are retained for longer than they needed to support business and community purposes.

Organisations must identify the retention requirements of their records by following guidelines for:

- assessing which of their records must be retained in perpetuity;
- assessing which of their records are eligible for destruction; and
- ensuring destruction of records is managed appropriately, in accordance with legislative and security requirements.

Requirements, Records disposal arrangements

ACT Health will identify the retention requirements of records, information and data by following guidelines for:

- assessing which of their records, information and data must be retained in perpetuity;
- assessing which of their records, information and data are eligible for destruction; and
- ensuring destruction of records, information and data is managed appropriately, in accordance with legislative and security requirements.

The following Records Disposal Schedules are authorised for use in the agency:

Schedule name	Date Effective	Instrument No
Finance and Treasury Management Records	27 February 2017	NI2017-83
Government and Stakeholder Relations Records	27 February 2017	NI2017-84
Health Treatment and Care	8 December 2017	NI2017-629
Human Resources Records	27 February 2017	NI2017-79
Information and Communications Technology Records	27 February 2017	NI2017-85
Patient Services Administration	24 December 2013	NI2013-590
Population Health Care Management & Control	8 May 2009	NI2009-209
Property Equipment and Fleet Records	27 February 2017	NI2017-86
Public Health Protection	29 March 2019	NI2019-161
Records and Information Management Records	27 February 2017	NI2017-87
Solicitor and Legal Services Records	27 February 2017	NI2017-88
Converted or Digitised Source Records	21 July 2020	NI2020-435
Strategy and Governance Records	27 February 2017	NI2017-89
Student Management	14 October 2016	NI2016-568

Requirements, Records disposal arrangements

	Training and Tertiary Education Records	7 July 2015	NI2015-363
	Preserving records containing information that may allow people to establish links with their Aboriginal and Torres Strait Islander heritage	25 March 2011	NI2011-162
	Protection of records relevant to the Royal Commission into Institutional Responses to Child Sexual Abuse	1 February 2013	NI2013-42

Records may only be destroyed in accordance with one of the above schedules or accepted normal administrative practice. Normal administrative practice for ACT Health is defined in the records management procedures and reinforced through training.

Additional arrangements are in place to protect records, information and data that may allow people to establish links with their Aboriginal or Torres Strait Islander heritage, and for records, information and data that are to be retained in perpetuity for cultural and historical purposes.

The organisation's arrangements for the authorisation of the disposal of records, information and data, and for their proper destruction, are outlined in the records management policy, procedures and additional guidance developed for business units to support relocations and rationalisation of records.

Principle 7: Access

Records cannot fulfil their purpose if they remain inaccessible.

Organisations must support the access to and openness of records, information and data by following guidelines for:

- encouraging open access of records, both across government and publicly;
- ensuring records can be found, accessed, used and re-used when appropriate; and
- enabling appropriate public access.

Requirements, Public access to records, information and data

ACT Health will support access and openness of records by following guidelines for:

- encouraging openness of records, information and data;
- ensuring records, information and data can be found, accessed, used and re-used when appropriate; and
- enabling appropriate public access.

Arrangements are in place to provide public access to records, information and data under the authority of the *Territory Records Act 2002*. These arrangements also allow for the exemption of certain information, data and record assets, and the regular review of the exemption (as defined by section 28 of the *Territory Records Act 2002*).

The organisation’s arrangements for providing public access to records, information and data are contained in records management procedures. Public access for ACT Health is administered by the Territory Records Office, Heritage Library.

Implementation, compliance and reporting

Arrangements are in place to implement this RMP , through the business planning process.

To monitor compliance with the RMP, performance measures for records, information and data management activities have been established and include:

- information, data and records are created or captured in a full and accurate way and in endorsed locations
- information, data and records are appropriately managed for as long as required
- ACTPS Territory Recordkeeping metadata requirements are implemented
- capability improvement measures are planned and implemented.

Quarterly/monthly/weekly reports on records and information management activities are provided to the Chief Information Officer by the Director, Records Management.

Availability for public inspection

Arrangements are in place to ensure this RMP is available for inspection by the public free of charge through publication on the ACT Health website (www.health.act.gov.au).

Review

A review of this RMP will be undertaken at least every five years or as required. Reviews may result in the replacement or amendment of this RMP.

Authorisation

In accordance with the *Territory Records Act 2002*, and as Director-General of the ACT Health Directorate, I:

- appoint the Chief Information Officer (Executive Group Manager, Digital Solutions Division) as the responsible senior executive for records management
- authorise this RMP
- certify that this RMP addresses all elements contained within section 16 of the *Territory Records Act 2002*
- certify that this RMP meets all the requirements set out in the Standard for Records, Information and Data released by the Director of Territory Records.

This RMP provides a framework to ensure records, information and data management requirements are met. The records, information and data management framework includes:

- Territory Records Act 2002
- Standard for Records, Information and Data released by the Director of Territory Records
- other applicable legislation and standards
- other applicable policies
- other administrative directions of the ACT Government and broader ACT public service
- RMP (this document)
- records, information and data management policy, procedures and architecture register for business systems.

This RMP and associated policies and information applies to the ACT Health Directorate as well as the ACT Local Hospital Network (LHN).

The Records Management Policy can be accessed from the ACT Health website.

I authorise the appropriate resourcing of this RMP, which includes the:

- promulgation of this RMP and the associated framework to all staff, volunteers, consultants, contractors and outsourced providers
- appropriate management of records, information and data
- annual assessment of records, information and data management capabilities
- planning for, and continual improvement of, records, information and data management capabilities.

Rebecca Cross
Director-General, ACT Health Directorate

February 2022

Version Control

Version	Date	Comments
0.1	06/12/2021	Initial draft
0.2	17/12/2021	Amendments and update into AHD template
0.3	22/12/2021	Minor amendments
0.4	03/01/2022	Minor amendments
0.5	17/01/2022	Minor amendments – draft to go out for consultation
0.6		ACTHD-wide consultation

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.*