POLICY DOCUMENT

ACT Government | ACT Health

Data Accountabilities Policy and Procedure

‘Data Custodian Policy and Procedure’

Document number	AHDPD-02:2023
Effective date	10 August 2023
Review date	10 August 2024
Author branch	Data Analytics Branch
Endorsed by	Executive Board (Operational)
Audience	All staff and contractors
Version number	1.0

Contents

Policy Statement

ACT Health Directorate (ACTHD) and Canberra Health Services (CHS) collect, generate and store large amounts of data and information to fulfil their administrative, clinical and public health roles. This includes information about those who access their services. To administer and provide coordinated health care services in the ACT, some data are shared between these two organisations.

The establishment of strong data governance processes assists in building trust with the community that their personal and health-related data are safely stored, and responsibly and ethically accessed and utilised by authorised ACTHD and CHS users. One of the key mechanisms to ensure the safe and ethical use of reliable and trustworthy data is the establishment of accountable data roles within an organisation, such as data custodians. Establishment of accountable roles also maximises efficiencies by minimising duplication of effort in the maintenance of data and establishing a recognised contact point for enquiries.

Those within ACTHD and CHS who use data and information for performance or other reporting, to support funding allocations, to inform clinical or health system policy decision-making, or to provide patient care, must be able to trust that data are fit-for-purpose or that any data quality issues are well documented. Data stewards, for example, play a critical role in these data management functions.

ACTHD and CHS have an obligation to assign accountable and responsible data roles to ensure safe and appropriate data access, use and management across the data lifecycle - from creation or acquisition, to storage, use, disclosure, and destruction or archiving.

Purpose

The purpose of this policy is to promote accountability for data governance and responsibility for data management practices by defining key data roles across ACTHD and CHS. As much data are shared between these two organisations, a clear understanding and acceptance of these roles and responsibilities will help strengthen a consistent approach to data governance.

This policy aligns with requirements as outlined in the ACT Government Data Governance and Management Framework.[1] The policy components of this document have been agreed by ACTHD and CHS. This ensures there is a consistent and shared foundation for data accountabilities across organisations, although the associated procedural processes may differ.

[1] ACT Government Data Governance and Management Framework

Scope

This policy and procedure is applicable to all ACTHD workers, including permanent, temporary, and casual employees, students, external contractors, consultants, and volunteers. These workers are required to comply with all obligations in relation to data and information privacy, protection and management as directed in relevant legislation and policies.

This document covers all data or digital information held by ACTHD and CHS including clinical, business and operational information that is shared between these organisations. It also covers all data and information held solely by ACTHD. It includes data or information acquired from external sources or provided by external data custodians that is accessible through ACTHD or CHS IT systems.

This policy and procedure encompasses information stored in any format, including unit record or aggregate data. It includes collections of business and health information where sound and accountable data practices are required.

Data managed on corporate platforms such as Chris21, HRIMS, KRONOS and similar are not subject to the data governance requirements specified in this policy. All efforts to align data governance standards will be undertaken but these collections may be subject to organisation-specific policies.

Context

Data ecosystem

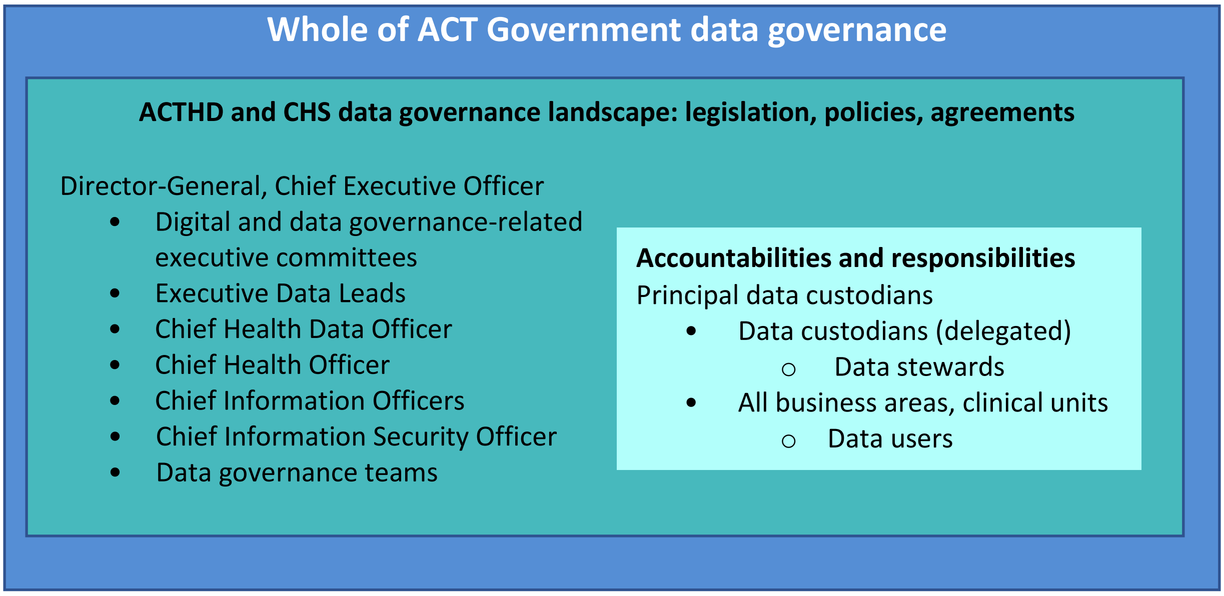
The ACTHD and CHS data ecosystem comprises several data and information assets, both physical and digital, held by these organisations to meet business needs. ACTHD holds a central data repository of clinical and other administrative and performance data collected across organisations subject to specific use cases mandated by legal instruments, agreements and reporting obligations. CHS has locally held data and repositories that are not managed by the ACTHD repository administrators, but which are aligned and consistent with data infrastructure managed by ACTHD.

Data are stored in repositories within ACTHD and CHS using a systems-based approach. ACTHD are the IT administrators for both the Digital Health Record system configuration and the Territory-wide data repository. The repository is one of several for the public health system that are supported by/in conjunction with Digital, Data and Technology Solutions (Territory-wide government data) administrators.

Governance framework

At ACTHD and CHS, there is a federated data operating model, where a central data governance body within each organisation coordinates data governance and enables the relevant business areas to manage data locally. This approach allows business areas to assume responsibility for the data and information they collect or manage. Agreed reporting metrics and definitions are used across ACTHD and CHS to ensure reporting has a consistent approach across and within organisations.

Data-related executive-level committees provide oversight and advice to those who are accountable for the security and safe, ethical and appropriate use of data. **Figure 1** below represents the ACTHD and CHS data governance landscape.



Whole of ACT Government data governance

ACTHD and CHS data governance landscape: legislation, policies, agreements

Director-General, Chief Executive Officer

- Digital and data governance-related executive committees
- Executive Data Leads
- Chief Health Data Officer
- Chief Health Officer
- Chief Information Officers
- Chief Information Security Officer
- Data governance teams

Accountabilities and responsibilities

Principal data custodians

- Data custodians (delegated)
  - Data stewards
- All business areas, clinical units
  - Data users

Figure 1: ACTHD and CHS data governance, including key accountable and responsible roles.

Legislative and policy context

Certain Commonwealth and ACT legislation and policies (ACT Government and ACTHD) prescribe and shape data governance and management arrangements. Legislation specifies who is permitted to access data and information and for what purposes. For example, the *Health Records (Privacy and Access) Act 1997* (ACT) outlines certain purposes for which personal health information can be accessed. Key legislation and policies that affect how data and information is governed and managed are outlined in **Table 1**.

Certain agreements or contracts may also exist that define how data and information can be used.

Table 1: Key legislation and policies

Key ACT legislation
Epidemiological Studies (Confidentiality) Act 1992
Health Act 1993
Health Records (Privacy and Access) Act 1997
Information Privacy Act 2014
Medicines, Poisons and Therapeutic Goods Act 2008
Public Health Act 1997
Territory Records Act 2002
Transplantation and Anatomy Act 1978
Relevant Commonwealth legislation
Privacy Act 1988
Data Availability and Transparency Act 2022
Health Care Identifiers Act 2010
My Health Records Act 2012
Policies and procedures
Proactive release of data (Open Data) Policy
ACT Health Directorate Information Privacy Policy
Data Breach Policy and Procedure
ACT Health Protective Security Policy
ACT Government Protective Security Policy Framework
ACT Conflict of Interest Procedure

Accountable and responsible roles

Data roles

This policy mandates that data roles must be formally assigned for all datasets or holdings within scope and sets out the responsibilities for protecting the confidentiality, integrity and availability of data. Key accountable and responsible roles, their definitions and the scope of the roles are outlined below.

Principal Data Custodians

Within ACTHD and CHS, the Director-General or Chief Executive Officer have overall accountability for all data and information collected or acquired by their organisation. These officers hold the role of Principal Data Custodian.

Executive Data Lead

The Executive Data Lead in each organisation is accountable for information assets, data sharing arrangements, governance decisions, establishing and implementing a data strategy and fostering a positive data culture for each entity's data holdings.

At ACTHD, the Executive Data Lead is the Executive Group Manager, Policy Partnerships and Programs Division.

At CHS, the Executive Data Lead is the Chief Information Officer, Executive Branch Manager, eHealth and Informatics Division.

Chief Health Data Officer

The central data governance body at ACTHD is overseen by the Chief Health Data Officer (CHDO). The below points reflect data governance functions facilitated by and for ACTHD by the CHDO to enable business areas to operate in a coordinated and effective manner, with support being provided, as required, to CHS or other directorates including:

- the provision of data governance-related advice, education, and in-service training
- knowledge and implementation of data governance best practices
- overseeing the allocation of accountabilities and responsibilities, including the functions of data custodians and stewards
- promoting the use of data and information for the purpose of improving health outcomes
- promoting the use of data and information for research
- working with experts within the organisations on priority data management improvements or projects such as establishing a data catalogue
- overseeing the development of policies and procedures for implementation across all business areas
- ensuring the establishment of data quality standards and data dictionaries
- coordinating metadata management across ACTHD and CHS
- identifying common gaps in governance and management practices at ACTHD and CHS and collaborating on prioritising actions
- working with data officers to ensure they understand their accountabilities and responsibilities
- ensuring the accuracy of accountable and responsible roles as documented in a central data catalogue.

At ACTHD, the CHDO reports to the Executive Group Manager in the Policy, Partnerships and Programs Division (ACTHD Executive Data Lead). The CHDO is the Executive Branch Manager for the Data Analytics Branch.

Chief Information Officer

The ACTHD Chief Information Officer provides high-level leadership, management and strategic advice in relation to performance reporting and technology capabilities across ACTHD.

At CHS, the Chief Information Officer provides strategic leadership, governance oversight, advice and management to the data and information collected, managed, released and reported by CHS. This includes endorsement of the technical architecture, data integrity, definitions, mapping, security and extraction of data from the core systems to the data repositories by the IT data storage providers, and access to data in the CHS data repository.

Data custodians

Data custodians are accountable for data governance decisions for assigned data or data sets and for authorising and facilitating safe data access, use and sharing. This role ensures maintenance of data privacy and confidentiality in consultation with the relevant Chief Information Officer and the Chief Information Security Officer (also known as the Agency Security Executive as defined under the ACT Government Data Governance and Management Framework).

Data custodians (and any others identified in organisation policies) are to be advised of any data breaches that are relevant to the datasets or holdings for which they are accountable and may be required to assist with the management of these breaches through participation in a data breach response team, or as directed by the Executive Data Lead. In addition, data custodians:

- have a business-level understanding of the information for which they are accountable
- have a sound knowledge of the legislation that is applicable to the information managed, including permitted uses
- have knowledge of any memoranda of understanding, contracts or other agreements that define permitted purposes for information use
- liaise with data users and other affected parties when making significant changes to datasets or information management practices
- approve any revisions to information, in accordance with business rules and with supporting documentation
- work closely with data stewards and application managers or business owners, to ensure that the information within their scope of accountability is adequately protected and meets business needs
- ensure that data governance complies with all relevant national, ACT Government, ACTHD or other relevant frameworks, policies and procedures.

Refer to the *Data Disclosure Policy* (available on the ACTHD Policy Register) that provides information for data custodians to consider when assessing a request for data for disclosure to internal or external recipients.

Data custodians and their contact details must be recorded in the central data catalogue hosted by the CHDO. Each organisation must ensure that the central data catalogue contains up-to-date information about data custodian allocations.

Data stewards

For the data or data sets assigned to them, data stewards are responsible for operational data management and decisions, including but not restricted to:

- metadata management
- maintaining data dictionaries
- ensuring data quality
- the utilisation of data standards.

Refer to the *Data Quality Policy and Procedure* (available on the ACTHD Policy Register) that provides information for data stewards and other staff about data quality and data quality statements.

Where data issues affect ACTHD and CHS, the management approach should be collectively agreed. This is to be governed through the appropriate committee.

In addition, data stewards:

- have a comprehensive understanding of the data or information for which they are responsible
- ensure that data management complies with all relevant ACT Government or organisation policies and procedures
- ensure all documentation relating to the information is current and stored in the enterprise records management system
- monitor and maintain records of access, use and disclosure
- maintain the validity of any contractual arrangements
- undertake other tasks as directed by the data custodian.

Data stewards work closely with the relevant data custodian and application managers or business owners.

Data stewards and their contact details must be recorded in the central data catalogue hosted by the CHDO. Each organisation must ensure that the central data catalogue contains up-to-date information about data steward allocations.

Application managers

Applications can be software or a device that provides a specific function or service that when implemented together, supports one or more related business processes. Application managers are responsible for management, enhancement, integration, and retirement of an application that hosts one or more datasets.

It is the application manager's responsibility to ensure new or changes to existing software/devices are reviewed by ACTHD and CHS to reduce the risk of duplication.

Application managers and their contact details must be recorded in the central data catalogue managed by the CHDO. Application managers must ensure that the CHDO is provided with up-to-date information about application manager allocations for recording in the central data catalogue.

Business owners

Business owners ensure applications meet business outcomes and create value for government and the community. Business owners work closely with data stewards and custodians.

Business owners and their contact details must be recorded in the central data catalogue managed by the CHDO. Business owners must ensure that the CHDO is provided with up-to-date information about business owner allocations for recording in the central data catalogue.

Data ownership

Data ownership is a complex issue and data collected or held by government does not grant ownership or proprietary rights, except in limited cases.[2] The data owner is usually the data provider – an individual, business or other entity providing information to another party.

Data users

Data users within ACTHD and CHS are all staff, students on placement,[3] contractors or volunteers. Data users must ensure they understand their obligations around the safe and appropriate use of enterprise information as outlined in policies and procedures.

Technical and security roles

Agency Security Executive

The ACTHD Chief Information Security Officer is the Agency Security Executive for ACTHD. The Chief Information Security Officer reports to the ACTHD Chief Information Officer and approves protective security programs for ACTHD, as defined by the *ACT Health Protective Security Policy*. The role is responsible for the management of information security vision, policy and implementation; the conduct of risk-based assessments, security awareness and identity access management; protective and cyber security matters; management of system customisation and environment configuration; and maintenance of identity and access management and security systems.

The Executive Branch Manager, Health Infrastructure Support Services is the Agency Security Executive for CHS. The CHS Chief Information Officer leads the advice and recommendations to the CHS Agency Security Executive.

Assigning custodians and stewards

Given the data and information ecosystem structure, data custodian and steward accountabilities and responsibilities are assigned to specified data use cases, regarding:

- the collection for the use of treating a patient and delivering clinical care
- patient administration, records management, appointments and on-going management of patient data and information for both clinical and administrative users
- ACT Government or Australian Government reporting requirements – including performance reporting, reports to support funding arrangements and other activity-based reporting
- data sharing, including:
    - ad hoc data requests from external researchers including Commonwealth and jurisdictional government departments, or external education partners (under a defined agreement)
    - regular approved data submissions such as to the NSW Centre for Health Record Linkage; Australian Institute of Health and Welfare for inclusion in national registries such as, but not limited to, the Australian Cancer Database, National Death Index,

[2] *ACT Government, 2020, Data Governance and Management Policy Framework*

[3] Excluding students on work experience or otherwise not subject to specified agreement (including MOU's)

Perinatal Data Collection, National Disability Data Asset, National Integrated Health Services Information Analysis Asset or National Minimum Datasets

- with contracted care providers, including but not limited to, Winnunga Nimmityjah Aboriginal Health Service or non-government organisations
- other approved data sharing initiatives.

Data custodians

Data custodians must hold a senior role within their organisation. Where the data contains information from ACTHD and CHS, data custodians are assigned by agreement between these organisations. As the digital landscape changes and the data governance function at ACTHD matures, the process of assigning data custodians where data are shared between ACTHD and CHS may be reviewed and amended.

Delegating custodian accountability

Where data custodians are defined under legislation, such as the role of the Chief Health Officer under the *Medicines, Poisons and Therapeutic Goods Act 2008* (ACT) or the *Public Health Act 1997* (ACT), data custodian (including Principal Data Custodian) accountability functions can be delegated or transferred to other officers using formal delegation instruments.

Unless authorised in legislation, a delegated function cannot be sub-delegated. A delegation 'survives' even if the person who made the delegation departs the organisation – the delegation can continue to be relied upon until revoked or varied.

Section 20 of the *Public Sector Management Act 1994* (ACT) expressly enables a Director-General of an ACT government administrative unit to delegate and sub-delegate to a public employee.

Persons acting in a role (such as an acting Director-General) are empowered to delegate functions, and to vary or revoke existing delegations.

Where further assistance with the proper construction and execution of delegations is required, contact the ACT Government Solicitor through ACT Health Governance and Risk: ACTHealth.GovernanceandRisk@act.gov.au

Where legislation does not specify data custodian arrangements, a Principal Data Custodian may authorise custodian roles to other suitable senior officers.

The relevant Principal Data Custodian must approve all custodian delegations. Relevant Chief Executive Officers must approve data custodian delegations at CHS.

While a data custodian may delegate some or all their responsibilities for the data in their care, they cannot delegate their accountability for the integrity, quality and currency, accuracy and accessibility of the data and information.

Delegations may be subject to conditions or limitations.

All approvals and delegations must be in writing and recorded in the enterprise records management system. A copy of the document/instrument must be retained by both the person making the delegation and the person who has been delegated the function.

A delegation template can be found at **Appendix 1.**

Data stewards

Where the data contains information from ACTHD and CHS, data stewards are assigned by agreement. Their appointment must be approved by the relevant data custodian. Data stewards must hold at least a SOGC or equivalent level role within their organisation. As the digital landscape changes and the data governance function at ACTHD matures, the process of assigning data stewards may be reviewed and amended.

Conflicts of Interest

Conflicts of interest arise in situations where a public officer is placed in a position where their duty to act independently, ethically and without prejudice may be, or appear to be, compromised by self-interest or a relationship with a third party. Data custodians and stewards must declare any conflict of interest in accordance with the *Public Sector Management Act 1994*.

Where a data custodian is aware of a conflict of interest, the custodian must complete a 'Conflict of interest declaration form' in line with their organisation's procedure. This form must be submitted to the Principal Data Custodian for consideration.

Where a conflict of interest situation involves the data steward, the steward must complete the *Conflict of Interest Declaration* form attached to the *ACT Conflict of Interest Procedure* and submit it for consideration to the data custodian.

Version Control

Version	Date	Comments
V0.1	October 2022	Data Strategy and Governance. Appending ACTHD procedural components to Data Working Group agreed policy (3 November 2022). Other minor changes
V0.2	March 2023	ACTGS advice
V 1.0	July 2023	Consultation and EGM PPP feedback

Glossary

Term	Definition
Application	Software functions and services implemented together to support one or more related business processes.
Data	Raw, cleaned, or processed material of information.[4] It may be numerical (quantitative), descriptive (qualitative), visual or tactile. It may be held in any format or media.[5]
Data holding	An aggregation of datasets in a specific repository.
Dataset	A cohesive set of data with measurable value that is designed to address a specific set of business needs.
Information	Data in context.[6] Any collection of data that is processed, analysed, interpreted, classified or communicated in order to serve a useful purpose, present fact(s) or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form (Office of the Australian Information Commissioner (OAIC), 2013).

[4] *DAMA-DMBOK Data Management Body of Knowledge*, 2nd edition, p. 20
[5] ACT Government Data Governance and Management Guide, August 2020, p. 117
[6] ACT Government Data Governance and Management Guide, August 2020, p. 117

Appendix 1

Data custodian delegation template

Date	
Data holding / use case	
Organisation (Please circle):	ACTHD / CHS
Action to be taken (Please circle):	• Register new delegation • Change or transfer of delegation • Removal of delegation
Current data custodian	Name:
	Role:
Staff member to be assigned delegation	Name:
	Role:
	Signed:
Relevant Delegation	
Identify any specific limitations or restrictions applicable	
Have you read, understood and accepted the responsibilities outlined in the *Data Accountabilities Policy and Procedure*?	Yes/No
Has a conflict of interest been identified? (Please circle)	Yes/No **If Yes:** Please contact your relevant Data Custodian and complete relevant Declaration/s.
Approved by relevant Principal Data Custodian (including acknowledgement of receipt and approval of any conflicts of interest declarations, as applicable):	Name:
	Role:
	Signed:
	Date:
Received by ACTHD Chief Health Data Officer	Name:
	Signed:
	Date:
Filed into the enterprise records management system?	Yes/No