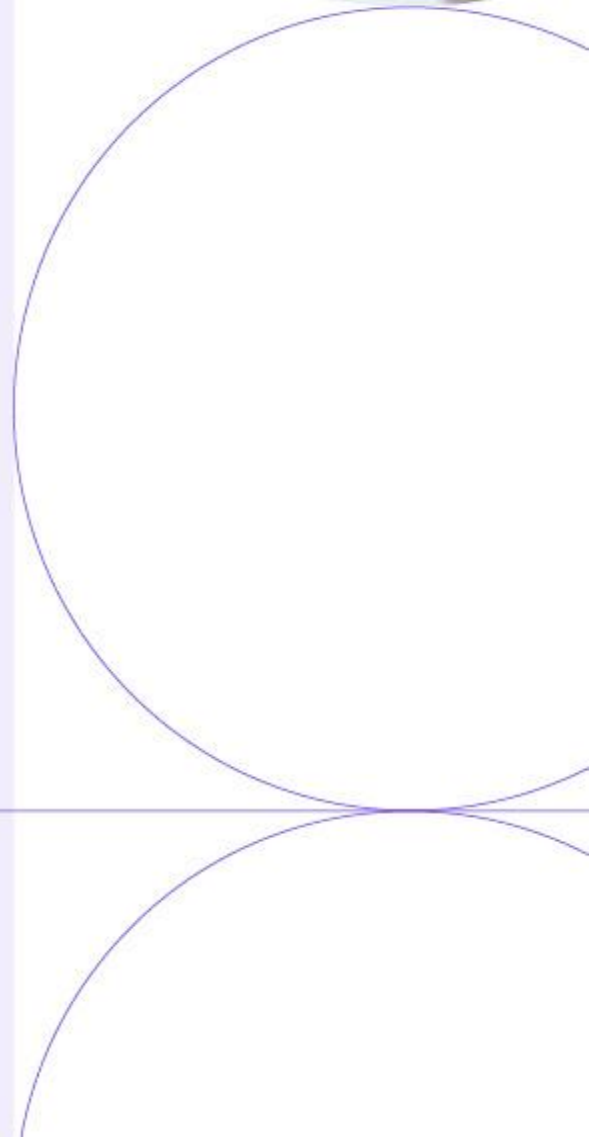


Policy Document

Data Access Policy

Document number AHDPD-07:2023
Effective date June 2025
Author Policy, Partnerships and
Programs Division /
Data Analytics Branch
Version number 2.0



Acknowledgement of Country

The Health and Community Services Directorate acknowledges the Ngunnawal people as traditional custodians of the ACT and recognise any other people or families with connection to the lands of the ACT and region.

We respect the Aboriginal and Torres Strait Islander people, particularly our Aboriginal and Torres Strait Islander staff, and their continuing culture and contribution they make to the Canberra region and the life of our city.

© Australian Capital Territory, Canberra

Disclaimer: This document has been developed by the Health and Community Services 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 Health and Community Services Directorate assumes no responsibility whatsoever.

Material in this publication may be reproduced provided due acknowledgement is made.

Produced by the Health and Community Services Directorate. Enquiries about this publication should be directed to the Health and Community Services Directorate.

GPO Box 158, Canberra City 2601

act.gov.au

Telephone: Access Canberra – 13 22 81

If you are deaf, or have a hearing or speech impairment, and need the telephone typewriter (TTY) service, please phone 13 36 77 and ask for 13 22 81.

For speak and listen users, please phone 1300 555 727.

For more information on these services, contact us through the National Relay Service:
www.accesshub.gov.au.

If English is not your first language and you require a translating and interpreting service, please telephone Access Canberra on 13 22 81.

Contents

Introduction	4
Purpose	4
Scope	4
Legislative and policy context.....	5
Access criteria.....	5
Need to know	5
Security clearance	6
Skills and training	6
Data custodian approval	6
Mode of access and storage	7
Service agreements.....	7
Roles and Responsibilities	8
Glossary.....	8
Review Date	9
Version Control.....	9

Introduction

Data held by the Health and Community Services Directorate (HCSD) are a valuable resource. Among its many uses, data records and informs clinical care, enables government reporting, justifies funding and is the foundational tool for clinical and health system research and evaluation.

Certain legislation prescribes the purposes for which data held by the HCSD can be accessed and used. Furthermore, the Australian community expects that any information provided by them to the government will be managed lawfully and be safe from unauthorised access. Where personal information (including sensitive information) and personal health information (see Glossary) held by an organisation is accessed or disclosed without authorisation (or is lost), a data breach has occurred. This may lead to harm to affected individuals or organisations and erodes public trust.¹

Purpose

This policy defines the conditions for data access that are necessary to ensure that only authorised data users with an approved need-to-know access data stored on HCSD servers.

Scope

This policy applies to all data held or hosted by the HCSD, including data provided by external data custodians, that are accessible through HCSD IT systems or infrastructure.

This policy applies to data access requests made by HCSD workers, including permanent, temporary and casual employees. These personnel are required to comply with all obligations in relation to data privacy, protection, and management as directed in relevant legislation, policies or procedures.

This policy provides additional guidelines to provide access to external contractors, consultants, students, and volunteers, in exceptional circumstances.

This policy does not apply to data requests made by external parties. All external data request must go through the Data Analytics Branch (ACTHealthDABCoordination@act.gov.au). These requests will be assessed on a case-by-case basis in consultation with relevant data custodian.

There are two components to controlling data access:

1. Policy controls that define the conditions for access and the required authorisations.
2. IT access provisioning: IT-enabled physical access to the data once the necessary authorisations are in place; IT safeguards that restrict access to unauthorised users; IT systems that track and audit access; and privileged access arrangements.

The IT provisioning of access (component 2 above) is managed under other arrangements as directed by the Chief Information Officer and is not addressed in this policy.

¹ Office of the Australian Information Commissioner [Part 1: Data breaches and the Australian Privacy Act — OAIC](#)

Legislative and policy context

Legislation that constrains how data can be used includes the *Health Records (Privacy and Access) Act 1997* (ACT) and the *Information Privacy Act 2014* (ACT). The *Health Records (Privacy and Access) Act 1997* (ACT), for example, outlines certain purposes for which personal health information can be used and disclosed.

The *ACT Government Standard for Records and Information Governance*² describes seven principles and minimum standards for records management in the ACT that supports the *Territory Records Act 2002* (ACT). This includes the 'access' principle that requires organisations to make data findable and accessible for use when appropriate.

The ACT Health *Data Breach Policy and Procedure* provides information regarding the management of unauthorised access (and disclosure) of personal information and personal health information.

The ACT Health *Protective Security Policy* defines obligations to protect the information HCSD holds and for it to be accessed only by those with a need-to-know.

The *Data Accountabilities Policy and Procedure* defines the roles of the data custodian.

Access criteria

There are four policy controls that need to be met prior to requesting access to data:

1. The person requesting access has an approved need-to-know (i.e. where there is an operational requirement for access³).
2. Where required by the data custodian, the access requestor holds the required Australian Government Security Vetting Agency clearance.
3. The requestor has the requisite skills and training to safely utilise and manage the data.
4. The data custodian has assessed that the purpose for which the data is to be used is permitted under legislation or any other relevant agreements or constraints.

Need to know

Those requesting access to data (access requestors) must only seek access where it is required to undertake approved tasks – i.e. there is a need-to-know. Data access use cases which demonstrate a need-to-know include:

- the provision of clinical care
- administration to support the delivery of clinical care

² *ACT Government Standard for Records and Information Governance*

³ *Protective Security Policy Framework Policy 9: Access to information*

- ACT Government or Australian Government reporting – including performance reporting, reports to support funding arrangements and other activity-based reporting
- facilitating research or evaluations conducted by:
 - Australian Government and jurisdictional government departments, under a defined data sharing agreement, or in accordance with ethics committee approvals
 - external agencies, such as universities, under a defined data sharing agreement
 - HCSD for authorised internal projects.
- 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 the Australian Cancer Database, National Death Index, or Perinatal Data Collection, National Disability Data Asset, National Health Data Hub and National minimum data sets.
- to support strategic procurement activities (including access for contractors/consultants)
- other initiatives approved by the data custodian.

Prior to seeking data custodian approval, a senior line manager must approve access after confirming that the access requestor has a business need-to-know. Approval is required from a Director or higher-level officer.

Security clearance

For HCSD staff requiring access to data, a valid Australian Government Security Vetting Agency clearance at the clearance level stipulated by the data custodian may be required.

Skills and training

Access conditions may include requirements for users to possess certain technical skills. Data custodians may require requestors to complete additional training to ensure safe data access, utilisation and output management. As training requirements may vary for different use cases and may change over time, check with the relevant data custodian.

Data custodian approval

Once the access requestor's manager has approved access; the requestor has obtained the required security clearance; and any necessary training has been completed, data custodians must review the request to ensure that the purposes for access and use are permitted under relevant legislation.

Generally, any information which is personal information may only be used for the purposes for which it was collected from the individual (except with the consent of the person or in other defined circumstances). The *Health Records (Privacy and Access) Act 1997 (ACT)* only permits uses and disclosures of personal health information for identified (or re-identifiable) individuals for limited purposes - for example, to permit sharing of information within the treating team for a patient for a particular episode of care.

Agreements or contracts may also exist that define how data can be accessed and used. It is the responsibility of data custodians to have knowledge of these agreements and to ensure that any agreements, memoranda of understanding or other contracts are recorded in the enterprise records management system (Objective).

Once all approvals, including data custodian approval, have been obtained, IT administrators can provision access in accordance with relevant IT policies and procedures.

Mode of access and storage

Enabling direct access to data where feasible minimises risks associated with release, including the security of data during transfer, version control issues, re-identification risks, unauthorised access or on-disclosure (including loss of data), control of outputs, and monitoring file and output destruction at project completion.

To minimise risks associated with data transfer, enable direct access to data where feasible.

Identifiable or potentially re-identifiable data must not be stored on desktops, personal drives, external drives or non-ACT Government computers. These types of data are to be stored on IT managed systems or in locations stipulated by the data custodian.

Photographing unit record data is prohibited.

Where unit record (micro) data can be downloaded from HCSD servers, the Principal Data Custodian, data custodian, Chief Health Data Officer, Chief Information Officer or Chief Information

Identifiable or re-identifiable data or extracts must not be stored on desktops, personal drives, external drives or non-ACT Government computers.

Security Officer may mandate additional data access or storage constraints.

Non-employee access

Where an external (third) party has been contracted to provide a service requiring access to HCSD data, this process is initiated through a procurement process. These services may be provided by a consultant or consultancy, or a contractor. Refer to the [Health Procurement and Assets Sharepoint page](#) for additional information and support. All procurements valued over \$5,000 must be registered on the [Procurement Register](#).

Service agreements

Service agreements allow HCSD (as an ACT Government directorate) to purchase services from a consultant/contractor and include requirements around how Territory information must be used. Refer to the *Procurement Policy* and *Procurement Procedure* on the [Policy Register](#) for advice on managing consultant or contractor arrangements. The relevant data custodian should approve any service agreements. Assistance with procurement is available at: healthprocurement@act.gov.au.

Where data are accessed by a consultant, contractor, student, or volunteer, a data custodian may apply special conditions. Additional safeguards that may be imposed by data custodians may include:

- confidentiality deeds that:
 - might be relevant if sensitive data needs to be accessed or disclosed

- can be requested from the ACT Government Solicitor by contacting the ACT Health outposted officer from ACT Government Solicitor or contacting ACT Health Governance and Risk ACTHealth.GovernanceandRisk@act.gov.au.
- provision of direct access to the data (HCSD on-premises), rather than providing a copy of an extract of the data, particularly where access to identified or potentially re-identifiable data is necessary. This limits risks associated with version control, unauthorised access or on-disclosure (including loss of data), control of outputs, and monitoring file destruction.
- obtaining ethics committee or site-specific approvals. Contact the Centre for Health and Medical Research for guidance: ethics@act.gov.au.

restrictions on publications or presentations. Where providing direct access to HCSD data is not

Where consultants or third parties require identified or potentially re-identifiable data, consider enabling direct access to the data.

feasible and consultants or contractors are to be supplied with a data extract (i.e. the data are disclosed or shared), refer to the *Data Disclosure Policy* for guidance which can be found on the ACT Health Policy Register.

Roles and Responsibilities

Position	Responsibility
Access requestors	Adherence to this and related policies and procedures.
Data custodians	Accountable for data governance decisions for assigned data or data holdings and authorising and facilitating safe data access, use and sharing.
Managers, executive staff	Approval that access is necessary to fulfil business role.

Glossary

Term	Definition
Consumer – as defined in the <i>Health Records (Privacy and Access) Act 1997 (ACT)</i>	An individual who uses, or has used, a health service.
Personal health information – as defined in the <i>Health Records (Privacy and Access) Act 1997 (ACT)</i>	Personal health information, of a consumer, means any personal information, whether or not recorded in a health record— (a) relating to the health, an illness or a disability of the consumer; or (b) collected by a health service provider in relation to the health, an illness or a disability of the consumer.

Term	Definition
Personal information – as defined in the <u><i>Information Privacy Act 2014 (ACT)</i></u>	Information or an opinion about an identified individual, or an individual who is reasonably identifiable— (i) whether the information or opinion is true or not; and (ii) whether the information or opinion is recorded in a material form or not; but (b) does not include personal health information about the individual.
Sensitive information – as defined in the <u><i>Information Privacy Act 2014 (ACT)</i></u>	Sensitive information, in relation to an individual, means personal information that is— (a) about the individual’s— (i) racial or ethnic origin; or (ii) political opinions; or (iii) membership of a political association; or (iv) religious beliefs or affiliations; or (v) philosophical beliefs; or (vi) membership of a professional or trade association; or (vii) membership of a trade union; or (viii) sexual orientation or practices; or (ix) criminal record; or (b) genetic information about the individual; or (c) biometric information about the individual that is to be used for the purpose of automated biometric verification or biometric identification; or (d) a biometric template that relates to the individual.

Review Date

The next review of this document is due by 30 June 2026.

Version Control

Version	Date	Comments
V0.1	August 2022	Data Strategy and Governance, Data Analytics Branch
V 0.2	September 2022	Digital Solutions Division
V0.3	January 2023	Procurement, Governance and Risk
V0.4	March 2023	Action DSD comments
V0.5	March 2023	Legal Policy review
V1.0	June 2023	ACTHD consultation feedback
V1.1	July 2024	ACTHD annual review
V1.2	September 2024	Revise review date and footer
V2.0	June 2025	ACTHD annual review

