ACT Government | ACT Health

POLICY DOCUMENT

# Data Disclosure Policy

| | |
|---|---|
| **Document number** | **AHDPD-05:2023** |
| **Effective date** | 1 September 2023 |
| **Review date** | 1 September 2024 |
| **Author branch** | Data Analytics Branch |
| **Endorsed by** | Executive Board (Operational) |
| **Audience** | All staff and contractors |
| **Version number** | V 1.0 |

# Contents

# Policy Statement

Data held by organisations, including ACT Health Directorate (ACTHD), are a valuable resource. Where data held by ACTHD are findable, accessible, interoperable and reusable (FAIR)[1], and can be safely disclosed (made available to others), there are opportunities for researchers, policy makers, service providers, planners, innovators and others outside ACTHD to utilise this information to improve the health and wellbeing of the ACT community. Benefits can include the provision of health, welfare and education services that better meet community needs and improved responses to natural disasters.

Commonwealth initiatives to support and promote safe data sharing between government agencies or the private sector are outlined in the *Australian Data Strategy*[2] and include the implementation of the *Data Availability and Transparency Act 2022* (Cwth) and enhancing data integration infrastructure and systems within Australia. The ACT Government is signatory to the Data and Digital Ministers' *Intergovernmental Agreement on data sharing between Commonwealth and State and Territory governments*, where parties agree to share data where it can be done securely, safely, lawfully and ethically.

In the ACT, the *Proactive Release of Data (Open Data) Policy*[3] promotes a 'disclosure as default' commitment to make available data that is of public interest. The ACT Government has also developed a framework that promotes and supports a consistent and standardised approach to data sharing across the Territory.

Australians trust and expect that information about them that is provided to the government (including ACTHD) will be safe from unauthorised access or disclosure.[4] As such, where data are disclosed to others, organisations have an ethical and legal responsibility to ensure that the data are managed in a way that protects the privacy and confidentiality of data providers (an individual, business or other entity providing information to another party[5]) captured within a particular release.

At ACTHD, all internal (within the ACT Government) and external data movements that involve the disclosure of personal health information (as defined under the *Health Records (Privacy and Access) Act 1997* (ACT)) about individuals (whether identifiable or re-identifiable) must be permitted by law and be accompanied by a valid data sharing agreement. Refer to the Glossary for definitions of personal information (including sensitive information) and personal health information.

1 Australian Research Data Commons
2 Department of the Prime Minister and Cabinet. 2021. *Australian Data Strategy*
3 ACT Government. 2015. *Proactive Release of Data (Open Data) Policy*
4 OAIC Australian Community Attitudes to Privacy Survey 2020
5 Australian Bureau of Statistics Glossary

# Purpose

This policy describes the rationale for:

- undertaking a disclosure risk assessment – applying the data sharing principles to data requests
- applying safeguards or protections to mitigate disclosure risks prior to making data available to others
- implementing data sharing agreements.

This policy applies to all internal (ACT Government) or external data disclosures. The policy may also need to be applied where data are transferred between ACTHD and Canberra Health Services aside from business-as-usual exchanges of information covered by standing agreements or memoranda of understanding, as the transfer of identifiable or potentially re-identifiable data may constitute a disclosure requiring a data sharing agreement.

This policy is a resource to assist data custodians to decide whether to approve a request for data while ensuring that legal requirements are met, and data providers' privacy and confidentiality are protected.

**This policy is a resource to assist data custodians to decide whether to approve a request for data while ensuring that legal requirements are met, and data providers' privacy and confidentiality are protected.**

The implementation of this policy also aims to provide the ACT community with reassurances that data held by ACTHD that is about them is disclosed ethically, responsibly and as permitted under legislation.

# Scope

This policy applies to all ACTHD workers, including permanent, temporary, and casual employees, external contractors, consultants, students and volunteers. ACTHD workers are required to comply with all obligations in relation to privacy and data protection as directed in relevant legislation, agreements, policies and procedures.

This policy covers all data held by ACTHD. It includes data acquired from external sources or provided to ACTHD by external data custodians that are accessible through ACTHD IT systems and infrastructure.

## Out of scope

This policy does not:

- consider data access arrangements for ACTHD staff who are required to extract information from ACTHD IT servers to facilitate release or sharing to approved data requestors. These arrangements are described in the *Data Access Policy.*
- address the specific statistical controls that may need to be applied to data prior to its disclosure to protect privacy and confidentiality. These techniques are addressed in the *Statistical Disclosure Controls Policy and Procedure.*
- prescribe the mechanisms to be used to safely transfer data from ACTHD servers to an internal or external data recipient. These are addressed in the *Transferring Confidential Information Policy and Procedure.*
- consider disclosures under the *Freedom of Information Act 2016* (ACT).

This policy does not apply to data sharing that is:

- a legal requirement – such as information required by an ACT or other court. The protocol for providing data to ACT Courts is described elsewhere.[6]
- required under legislation.

This policy does not:

- overrule any data sharing agreements such as intergovernmental agreements
- address the sale of ACT Government data or any procurement processes. Refer to the *Data Access Policy* that outlines arrangements for the provision of data to consultants/contractors under the procurement process.

# Modes of disclosure

Under certain conditions, data held by ACTHD can be disclosed, through sharing or release, to authorised recipients. Data are:

- **shared** where they are made 'available to another agency, organisation or person under agreed conditions.'
    - This could include **closed data** – data (that may include unit record data [microdata][7] or identifiable data) that are disclosed to secure networks for access by authorised users.[8]

**DATA SHARING EXAMPLES**

Unit record data are utilised by analysts within a secure network, such as the Australian Bureau of Statistics' DataLab.

ACTHD unit record data is provided to the Centre for Health Record Linkage for inclusion in the Master Linkage Key.

6 *Protocol for the release of data relating to the operations of the ACT Courts*.
7 Australian Bureau of Statistics Glossary
8 ACT Government. Data Sharing Policy, 2022.

- **released** where they are 'made publicly available with no or few restrictions on who may access the data and what they may do with it'.[9]
    - An example is the ACT Open Data Portal. In this setting, data custodians cannot control who accesses the data or how the data will be used.

**DATA RELEASE EXAMPLES**

The Australian Bureau of Statistics' Data Cubes – 'Ageing Population', 'Cultural Diversity', 'Educational Qualifications'.

Australian Institute of Health and Welfare – 'Adoptions Australia', 'General Record of Incidence of Mortality'.

Data.gov.au datasets – 'Taxation Statistics', 'Disaster Events'.

# Context

## Legislative setting

In the ACT, there is legislation that defines personal information (*Information Privacy Act 2014* (ACT)) and personal health information (*Health Records (Privacy and Access) Act 1997* (ACT)) and how that information is to be protected, and how it can be used and disclosed (refer to Glossary).

The *Information Privacy Act 2014* (ACT) contains 13 Territory Privacy Principles that set out standards, rights and obligations for the collection, use, disclosure, storage, access, and correction of personal information. There are 12 Health Privacy Principles in the *Health Records (Privacy and Access) Act 1997* (ACT). Health Privacy Principle 10 states that 'a record keeper … must not disclose personal health information about a consumer from the record to an entity other than the consumer' unless under certain conditions (**Appendix A**).[10]

Other legislation, such as the *Public Health Act 1997* (ACT) also stipulates how information can be used or disclosed. The *Australian Immunisation Register Act 2015* (Cwth) states it is an offence to record, disclose or otherwise use information within the Register unless for purposes prescribed by the Act.

Section 9(2)(d) of the *Public Sector Management Act 1994* (ACT) states that a public servant must not 'without lawful authority, disclose confidential information gained through the public servant's job'.

Data custodians should have knowledge of any legislation that is relevant to the data for which they are accountable.

The unauthorised disclosure of certain information can constitute a criminal offence where the maximum penalty includes the possibility of a term of imprisonment.

9 Department of the Prime Minister and Cabinet. *Best practice guide to applying data sharing principles.* 2019

10 *Health Records (Privacy and Access) Act 1997* (ACT)

**Data custodians should have knowledge of any legislation that is relevant to the data for which they are accountable.**

## Policy setting

ACTHD is signatory to the ACT Government Data Sharing Memorandum of Understanding (MoU) with other participating ACT Government directorates that states that directorates have a 'responsibility to share' data. The MoU confirms that ACTHD agrees to use 'best efforts' to share data responsibly and sets out the general terms for data sharing between ACT Government parties.

The responsibility to disclose data under this policy:

- is not a legal requirement
- requires best endeavours to disclose within existing resources and infrastructure
- does not override any legal or other constraints that restrict disclosure
- does not override a data custodian's data request risk assessment.

To facilitate a consistent approach to data disclosure across the Territory, this ACTHD policy is consistent with the *ACT Government Data Sharing Policy*.

This policy should be read in conjunction with the *Data Accountabilities Policy and Procedure*. In that policy, **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.

The *Data Quality Policy and Procedure* states that where data quality issues are not known or are unable to be communicated to the data user, it is recommended that those data should not be disclosed. At ACTHD, for the data or data sets assigned to them, the *Data Accountabilities Policy and Procedure* prescribes that **data stewards** are responsible for data management activities including metadata management; maintaining data dictionaries; ensuring data quality; and the utilisation of data standards.

**Where data quality issues are not known or are unable to be communicated to the data user, it is recommended that those data should not be disclosed.**

The *Statistical Disclosure Controls Policy and Procedure* and the *Transferring Confidential Information Policy and Procedure,* respectively, define how data may need to be managed to make it safe prior to disclosure, and how authorised data disclosures are to be safely digitally transmitted to internal or external recipients.

When assessing a data disclosure, it is important to consider liaising with the Aboriginal and Torres Strait Islander Health Partnerships team where the data are about, or may affect, Aboriginal or Torres Strait Islander people.

A data breach occurs where personal information is accessed or disclosed without authorisation, or is lost. As such, where personal information or personal health information have been disclosed outside this policy, a data breach may have occurred and should be reported as outlined in the *Data Breach Policy and Procedure.*

**Where personal information or personal health information have been disclosed outside this policy, a data breach may have occurred and should be reported.**

## DATA Scheme

The *Data Availability and Transparency Act 2022* (Cwth) is underpinned by the DATA Scheme. Regulated by the National Data Commissioner, data sharing under the DATA Scheme occurs where the request aims to improve the delivery of government services, inform government policies and programs, or supports research and development.[11]

The DATA Scheme provides another pathway to request ACTHD data and for ACTHD to request data from external data custodians. *Dataplace* is the platform developed to manage DATA Scheme requests and support Scheme administration.

Visit the Office of the National Data Commissioner's website for details about the DATA Scheme and how to request data or manage requests for ACTHD data.

# Background

## The problem

The Australian Bureau of Statistics defines **confidentiality** as 'protecting the secrecy and privacy of information collected from individuals and organisations and ensuring that no data are released in a manner likely to enable their identification'.[12]

There are two main types of identification risks[13] that can occur following disclosure:

1. **Identity disclosure**:
    - **Direct identification**: Where a data release contains direct identifier/s that establishes the identity of a person, group or organisation.
    - **Indirect identification**: Where 'the identity of a person, group or organisation is disclosed due to a unique combination of characteristics (that are not direct identifiers) in a dataset'.
        - An example is a celebrity identified from data containing age, sex, occupation and income.

11 Office of the National Data Commissioner *Introducing the Data Scheme.*
12 Australian Bureau of Statistics Glossary
13 Australian Bureau of Statistics Glossary

Identification can be:

- **Spontaneous**: This is a non-deliberate identification. It can occur where there are individuals with a rare characteristic within the data. An example would be a 99-year-old man who lives in a rural postcode.
- **Deliberate:** Where the data recipient crossmatches or links unique characteristics that are common to the released data and other information such as that found on the internet or already held; or tries to identify a record that contains specific characteristics known to that person.

2. **Attribute disclosure** occurs where 'previously unknown information is revealed about an individual, group or organisation (without necessarily formally re-identifying them)'.[14]
    - For example, if an income bracket for all women aged 60 to 65 years living in a small geographic area were reported, then the income for any woman of that age living in that area would be known to an outsider.

Section 18 of the *Information Privacy Act 2014* (ACT) states that personal information is **de-identified** if 'the information is no longer about an identifiable individual or an individual who is reasonably identifiable'.

To maintain confidentiality, agencies including ACTHD, must ensure that identifiable information about data providers,[15]:

- is not disclosed publicly
- is only provided to authorised individuals who have a 'need-to-know' and as permitted by law
- cannot be used to re-identify a data provider or organisation
- is securely stored.

# Data Sharing Principles

The Five Safes framework is the internationally recognised disclosure risk management standard[16,17] that is used to assess risk associated with disclosing confidential or sensitive data.[18] The Data Sharing Principles reflect the Five Safes Framework. The DATA Scheme also utilises the Data Sharing Principles to facilitate safe, consistent and efficient data sharing.[19]

14 Australian Bureau of Statistics Glossary
15 ACT Health Protective Security Policy Framework, DGD17-013
16 Department of the Prime Minister and Cabinet. *Best practice guide to applying data sharing principles.* 2019.
17 Ritchie F. *The 'Five Safes': a framework for planning, designing and evaluating data access solutions.* UK: University of the West of England; No date.
18 Fives Safes Org. *The Five Safes. Effective decision-making for data and risk management*. No date.
19 Office of the National Data Commissioner *Introducing the Data Scheme.*

The assessment of disclosure risk is subjective. Applying the Data Sharing Principles to a data request is a tool to assist data custodian decision making. It does not:[20]

- provide empirical formulae upon which to base risk assessment decision-making
- prescribe how the decision whether or not to disclose is made
- define an organisation's attitude to risk or risk tolerance.

As the decision about whether to disclose data is complex, the Five Safes framework (Data Sharing Principles) enables risk to be considered across five simpler domains: People, Projects, Settings, Data and Outputs.

Data custodians should use the Data Sharing Principles to conduct data request disclosure risk assessments. To help preserve the privacy and confidentiality of data providers, each Data Sharing Principle is associated with several safeguards, protections or controls. The application of these controls should be considered by data custodians prior to any disclosure.

**Use the Data Sharing Principles to conduct data request disclosure risk assessments.**

# Project Principle

## Are the proposed uses of the data appropriate, ethical and lawful?

This principle considers whether the data are to be shared for a purpose that delivers a public benefit. In the ACT, public benefit projects are those that:

- inform improved policy design
- support research and evaluation
- inform improved service planning and delivery
- support the recommendation of a Royal Commission, inquest, or inquiry
- inform improved reporting activities and relevant government functions
- support improved public safety outcomes, or
- support either the creation or improved delivery of a Wellbeing Indicator.

Data custodians should consider whether publicly available data already exists that will meet the requestor's needs. In addition, the data custodian should be satisfied that:

- any project proposal is methodologically rigorous and statistically robust
- the data are available and will sufficiently address the requestor's needs
- the data can be disclosed or used as prescribed in relevant legislation or other agreements and contracts (see Legislative Considerations below)
- data providers have consented to the disclosure, or other mechanisms for legal disclosure exist

20 Desai T Ritchie F Welpton R. Five Safes: designing data access for research. Bristol UK: University of the West of England, Faculty of Business and Law, 2016.

- where relevant, the project has been approved by a National Health and Medical Research Council-accredited human research ethics committee (and that approval is currently valid) (see Ethical Considerations below)
- additional approvals are not required from other data custodians.

Aside from open data releases (where this principle cannot be assessed), where a data request does not meet Project Principle requirements, the data should not be disclosed, and no further Data Sharing Principles need to be assessed.

**Where a data request does not meet Project Principle requirements, the data should not be disclosed, and no further Data Sharing Principles need to be assessed.**

## Legislative Considerations

**Table 1** provides examples of ACT and Commonwealth legislation that deal with disclosure of information about individuals or other entities.

**Table 1:** Key ACT and Commonwealth legislation that deals with disclosure of information about individuals or other entities.

| **Key ACT legislation** |
|---|
| ***Health Records (Privacy and Access) Act 1997*** |
| The *Health Records (Privacy and Access) Act 1997* (ACT) (**Health Privacy Principle 9 and 10**) 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.<br>Refer to **Appendix A** which details the constraints for the use and disclosure of identified or identifiable records containing personal health information. |
| ***Information Privacy Act 2014*** |
| This Act states that if an agency holds personal information that was collected for a particular purpose, that information cannot be disclosed for another purpose unless the individual has consented to the disclosure, or under limited other circumstances. |
| ***Public Health Act 1997*** |
| Within this Act, it is an offence to disclose the name of the person, laboratory or hospital associated with a disease notification; or, to disclose information that may identify a person with, or who may have, a notifiable condition, unless under certain circumstances. |
| **Key Commonwealth legislation prescribing disclosure constraints** |
| ***Privacy Act 1988*** |
| Australian Privacy Principle 6 deals with the use or disclosure of personal information (including sensitive information, health information, credit information, employee record information and tax file number information). This principle states personal information that was collected for a particular purpose must not be disclosed for a secondary purpose without the consent of the individual, or unless other certain circumstances apply. |

Other ACT legislation that may influence data custodian disclosure decisions includes:

- *Blood Donation (Transmittable Diseases) Act 1985*
- *Drugs of Dependence Act 1989*
- *Epidemiological Studies (Confidentiality) Act 1992*
- *Food Act 2001*
- *Gene Technology (GM Crop Moratorium) Act 2004*
- *Health Act 1993*
- *Medicines, Poisons and Therapeutic Goods Act 2008*
- *Public Health Act 1997; Public Health Regulation 2000*
- *Public Sector Management Act 1994*
- *Radiation Protection Act 2006*
- *Transplantation and Anatomy Act 1978*

### Ethical Considerations

Requests for information may require approval from the ACT Health Human Research Ethics Committee and other National Health and Medical Research Council accredited ethics committees.

Projects that require ethics committee approval include, but are not limited to:

- any research project involving the use and disclosure of personal information or personal health information
- projects involving data integration
- any request that the data custodian considers high risk or requiring ethics approval.

Please contact the ACT Health Human Research Ethics Committee executive office for advice if you are uncertain whether a project requires approval: research.governance@act.gov.au

## People Principle

### Who is accessing the data?

### Do the users have the right knowledge, skills, and motivations to appropriately use the data?

When considering this principle, the data custodian assesses whether those requesting access have the appropriate skills to properly analyse and interpret the data. This may include reviewing their qualifications, experience and organisational affiliations. Can the data users be trusted to use the data appropriately? Does the requesting team have sufficient expertise across all areas of the project such as subject matter, biostatistical or data integration expertise?

Other considerations can include an assessment of conflicts of interest for those accessing the data or sponsoring the project; or whether the institution hosting the requested data has adequate data breach management processes in place or can be trusted to manage a data sharing agreement.

# Setting Principle

## Where will the disclosed data be stored and accessed?

## Is the access environment safe and secure?

This principle involves consideration of how the disclosed data will be transferred to the data recipient. The *Transferring Confidential Information Policy and Procedure* prescribes how secure file transfer protocol software must be used to safely transmit confidential data to internal or external recipients.

Once disclosed to the new storage or access location, data custodians should consider whether the data will be physically secure and protected from cyber threats. Will the data be safe from unauthorised access and re-identification? Can the data be subjected to audits? Are there clear responsibilities for data management and governance? How will the data be destroyed at project completion?

To protect the confidentiality of potentially re-identifiable unit record data, data custodians should consider whether the data storage and access environment needs to be closed or controlled (such as the Australian Bureau of Statistics' DataLab or the Sax Institute's Secure Unified Research Environment), and whether user training is required.

**To protect potentially re-identifiable unit record data, data custodians should consider whether the data storage and access environment needs to be controlled.**

# Data Principle

## What data are requested?

## Is there a potential that data providers can be identified?

As part of the assessment for the Data Principle, custodians should establish the full extent of the data requested from all custodians, to help gauge re-identification risks. The more data that are requested across all data custodians, the greater the re-identification risk.

The *Statistical Disclosure Controls Policy and Procedure* defines how data may need to be managed prior to disclosure to protect the confidentiality of data providers and manage re-identification risks.

For data that will be posted on open data websites, *very strong* statistical controls will need to be applied prior to release.

**For open data, very strong statistical controls need to be applied prior to release.**

To help ensure data requestors understand the data they are receiving, include a data quality statement for each extract along with metadata that includes a data dictionary that describes each of the variables. Refer to the *Data Quality Policy and Procedure* for assistance with preparing data quality statements and the data quality statement template.

## Output Principle

### How will findings be used or reported?

### Will statistical outputs ensure confidentiality?

Assessment of this principle by the data custodian involves consideration of any artefacts that will be created, such as reports, dashboards, publications or linkages with other data. Processes for the release of outputs should be considered with regard to the *Freedom of Information Act 2016* (ACT), the *Territory Records Act 2002* (ACT) or other relevant legislation.

Will the data in outputs have been sufficiently managed to prevent re-identification or attribute disclosure? Data custodians may choose to impose restrictions such as the requirement for any findings or reports to be approved prior to publication (**rules-based restriction**); or they may take a **principles-based** approach to restrictions where, for example, outputs are permitted where they meet certain criteria stipulated by the data custodian (such as ethical standards).

# Data sharing agreements

At ACTHD, all internal (within the ACT Government) and external data movements that involve the disclosure of personal health information (as defined under the *Health Records (Privacy and Access) Act 1997* (ACT)) about identifiable (or re-identifiable) individuals must be accompanied by a valid data sharing agreement and must be permitted by law. Additional agreements may also be implemented, such as Service Agreements or Collaboration Deeds.

**At ACTHD, all data movements that involve the disclosure of personal health information about identifiable (or re-identifiable) individuals must be accompanied by a valid data sharing agreement and be permitted by law.**

The ACT Government has developed two data sharing agreement templates that incorporate data custodian assessments of disclosure risk using the Data Sharing Principles. These agreements also document the parties to the agreement, variations, and any limitations or constraints applicable to the disclosure.

Use the ***ACT Health Internal Data Sharing Agreement Template*** to record and assess each of the Data Sharing Principles and establish risk safeguards that need to be implemented, where data are to be disclosed to other ACT Government directorates.

Use the ***ACT Health External Data sharing Agreement Template*** to record and assess each of the Data Sharing Principles and establish risk safeguards that need to be implemented, where data are to be disclosed to agencies external to the ACT Government.

Internal and external data sharing agreement templates can be found on the Data Strategy and Governance Sharepoint site.

For all data requests, Internal and External data sharing agreements are to be approved by data custodian/s following a disclosure risk assessment against the Data Sharing Principles.

**For all data requests, data sharing agreements are to be approved by the data custodian following a disclosure risk assessment against the Data Sharing Principles.**

As ACTHD is signatory to the ACT Government Data Sharing MoU, a summary of each data sharing agreement is to be lodged on the ACT Government online public data sharing schedule. This process is designed to promote transparency around data sharing and open government practices.

Completed data sharing agreements, and any other records relevant to the request must be filed in the enterprise records management system (Objective).

# Assessing the adequacy of safeguards

To help preserve the privacy and confidentiality of data providers, each Data Sharing Principle is associated with several safeguards, protections or controls. The application of these controls should be considered by data custodians prior to any disclosure.

When data custodians consider a data sharing request, the challenge is to maximise the utility of the data for the requester by providing them with quality data that are fit-for-purpose to meet the data requestor's needs, while maintaining the confidentiality of those data. The more controls that are put in place to protect privacy and confidentiality, the less utility (or usefulness) there may be for the data user.[21]

As all disclosure is associated with some risk, data custodians must consider whether the public benefits that could arise from the disclosure are greater than any associated residual risks. If the combined protections afforded by the safeguards outlined in the data sharing agreement are insufficient to protect confidentiality, then the data should not be disclosed.[22, 23]

**If the combined protections afforded by the safeguards are insufficient to protect confidentiality, then the data should not be disclosed.**

21 Australian Bureau of Statistics. Five Safes framework. 2021.
22 Office of the National Data Commissioner, *Sharing Data Safely,* 2019
23 Australian Bureau of Statistics. Five Safes framework. 2021.

# Using the data sharing principles

Not all Data Sharing Principles may need to be assessed for each data request. **Figure 1** illustrates the **minimum** level of control that should be assessed for each disclosure type (open data, aggregated data and unit record data).

**Not all Data Sharing Principles may need to be assessed for each data request. This will depend on the nature of the data that is proposed for disclosure.**

The magnitude of safeguards that need to be applied will depend on the nature of the data that is proposed for disclosure. For example, for:

- **open data releases,** it is not possible to know or assess how the released data will be used (Project Principle); who will be accessing the information (People Principle); where it will be accessed or stored (Setting Principle); or how outputs or artefacts will be reported or published (Outputs Principle).
    - **Very strong statistical controls** need to be applied prior to open data releases (Data Principle). Refer to the *Statistical Disclosure Controls Policy and Procedure.*

- **aggregate data** sharing or release requires, **at a minimum,** data custodians to be assured of the purposes for which the data are to be used (Project Principle), and to apply statistical controls to protect the confidentiality of data providers (Data Principle) prior to disclosure.

- **unit record data:**
    - **All** Data Sharing Principles are to be assessed to ascertain whether the sharing is within acceptable risk limits, and that these risks do not outweigh intended public benefits. Strong controls or safeguards need to be in place for the Project, People, Setting and Data Principles.
    - The **Setting Principle** is a very strong mechanism to protect privacy and confidentiality. Data custodians should consider only transferring unit record data, potentially re-identifiable data or identifiable data to the secure networks and settings below (**closed data**):
        - Australian government agency IT infrastructure
        - secure access environments, such as the ABS DataLab, AIHW secure environments, or the Secure Unified Research Environment.

**For unit record data sharing, strong controls or safeguards need to be in place for the Project, People, Setting and Data Principles.**

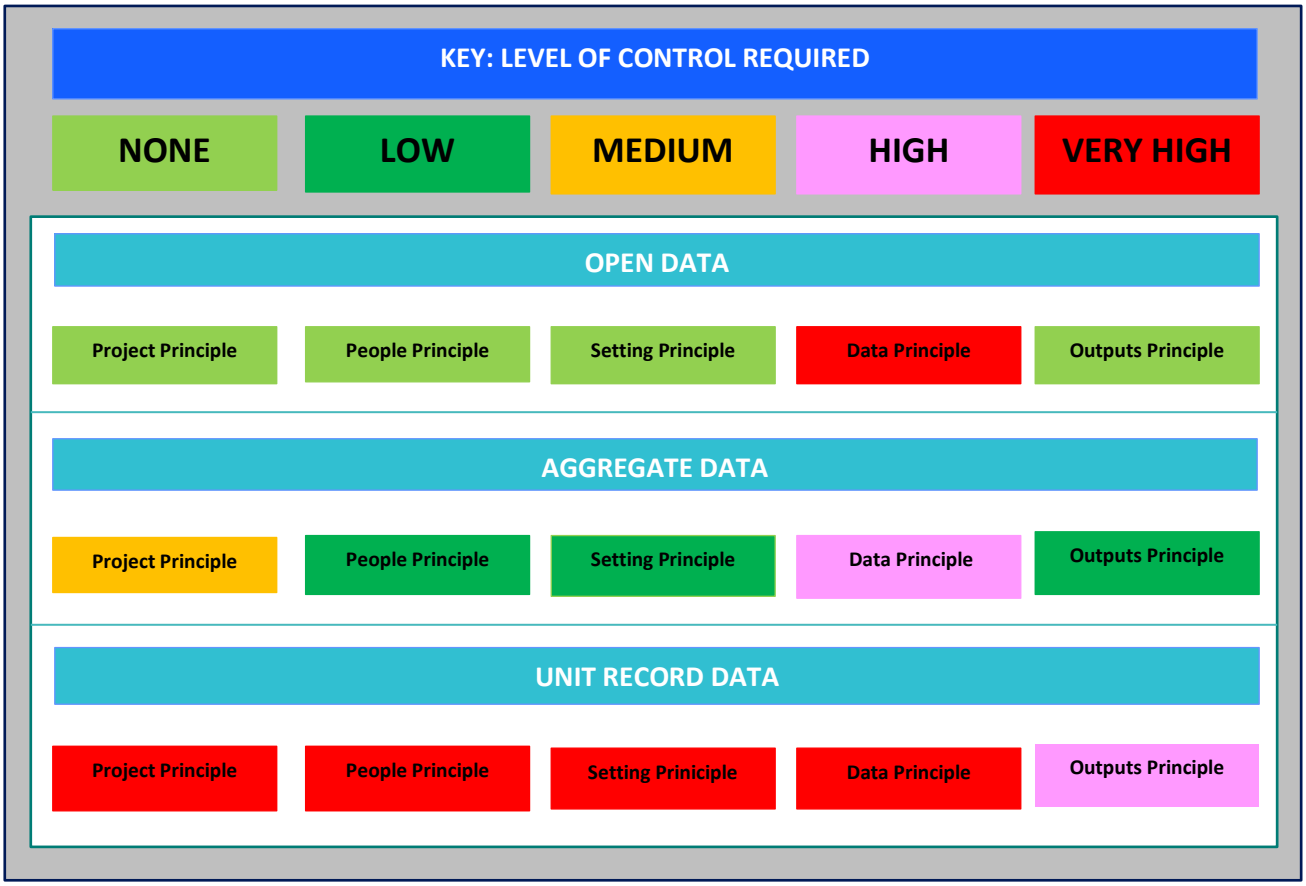


**Figure 1**: Data Sharing Principles for assessment, depending on the nature of the data to be disclosed, and the level of control or safeguards that need to be applied. Adapted from the *Best practice guide to applying data sharing principles. 2019.*

# Transferring data to the data requestor

Once all agreements have been finalised and approved by the data custodian and recorded in the enterprise records management system (Objective), the data should be transferred to the intended recipient using a secure file transfer mechanism as described in the *Transferring Confidential Information Policy and Procedure.*

# Roles and Responsibilities

| Position | Responsibility |
|---|---|
| Data custodians | Accountable for data governance decisions for assigned data holdings and for authorising and facilitating safe data access, use and sharing.<br>Accountable for the completion of Data Sharing Agreements and Five Safes disclosure risk assessments. |
| Data stewards | Responsible for metadata management; maintaining data dictionaries; ensuring data quality; and the utilisation of data standards. |
| Chief Health Data Officer | Accountable for safe and competent data practices within ACTHD. |
| All staff | Implementing disclosure risk assessments and completion of data sharing agreements for all internal and external data disclosures. |
| | Application of appropriate data management techniques as described in the *Statistical Disclosure Policy and Procedure,* prior to disclosure. |
| | Sending personal information (including personal health information) or confidential information to internal or external recipients using the mechanisms outlined in the *Transferring Confidential Information Policy and Procedure.* |
| | Awareness of the *Data Quality Policy and Procedure* and its recommendation not to disclose data where data quality issues are not known or cannot be communication to the data requestor. |

# Evaluation

| Outcome Measures | Method | Responsibility |
|---|---|---|
| No reported data breaches will originate from failure to identify and mitigate disclosure risks | Review of nature of data breaches recorded on the Data Breach Registry | All business areas<br>Director, Data Strategy and Governance |

# Glossary

| Term | Definition |
|---|---|
| Consumer – as defined in the *Health Records (Privacy and Access) Act 1997 (ACT)* | An individual who uses, or has used, a health service. |
| Personal health information – as defined in the *Health Records (Privacy and Access) Act 1997 (ACT)* | 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. |
| Personal information – as defined in the *Information Privacy Act 2014 (ACT)* | 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 *Information Privacy Act 2014 (ACT)* | 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. |

# Version Control

| Version | Date | Comments |
|---|---|---|
| V0.1 | January 2023 | Data Strategy and Governance, DAB |
| V0.2 | February 2023 | Population Health Division, Health Policy and Strategy Branch, Epi team, DAB, Mental Health and Suicide Prevention Division |
| V0.3 | March 2023 | ACTGS review |
| V0.4 | April 2023 | DSG addition DDM IGA. Consultation inclusions. |
| V 1.0 | June 2023 | Final draft |
| V 1.0 | September 2023 | Aboriginal and Torres Strait Islander Health Partnership |

# Appendix A

## Disclosures of personal health information

The *Health Records (Privacy and Access) Act 1997* (ACT) defines personal health information as '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.'

A consumer means an individual who uses, or has used, a health service, or in relation to whom a health record has been created.

The treating team in relation to a consumer, means the health service providers involved in diagnosis, care or treatment for the purpose of improving or maintaining the consumer's health for a particular episode of care, and includes—

a) if the consumer named another health service provider as the consumer's current treating practitioner—that other health service provider; and

b) if another health service provider referred the consumer to the treating team for that episode of care—that other health service provider.

The *Health Records (Privacy and Access) Act* 1997 (ACT) allows for personal health information to be used and disclosed only in certain circumstances.

Health Privacy Principle 9 requires that except where personal health information is being shared between members of a treating team to the extent necessary to improve or maintain the consumer's health or to manage a disability of the consumer, a **record keeper must not use personal health information** that was obtained for a particular purpose for any other purpose unless:

a) the consumer has consented to use of the information for that other purpose; or

b) the record keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a significant risk to the life or physical, mental or emotional health of the consumer or another person; or

c) use of the information for that other purpose is required or authorised by—
    i. a law of the Territory; or
    ii. a law of the Commonwealth; or
    iii. an order of a court of competent jurisdiction;

d) the purpose for which the information is used is directly related to the purpose for which the information was obtained; or

e) the use of the information is related to the management, funding or quality of the health service received by the consumer.

Health Privacy Principle 10 requires that a **record keeper to must not disclose personal health information** about a consumer from the record to an entity other than the consumer, unless:

a) the information is being shared between members of a treating team for the consumer only to the extent necessary to improve or maintain the consumer's health or manage a disability of the consumer; or

b) the consumer is reasonably likely to have been aware, or to have been made aware under principle 2, that information of the kind disclosed is usually disclosed to the entity; or

c) the consumer has consented to the disclosure; or

d) the record keeper believes, on reasonable grounds, that the disclosure is necessary to prevent or lessen a serious and imminent risk to the life or physical, mental or emotional health of the consumer or someone else; or

e) the disclosure is required or allowed under—
   i. a law of the Territory (including this Act); or
   ii. a law of the Commonwealth; or
   iii. an order of a court; or

f) the disclosure of the information is necessary for the management, funding or quality of the health service received, or being received, by the consumer.