Environmental Scan of Data Custodian Resources

Scalable Governance, Control & Management of FAIR Sensitive Research Data Project - Data Custodian Community of Practice

Version: 1.0

Current: 7 November 2022

Table of contents

Purpose

The Data Custodian Community of Practice was established through the Scalable Governance, Control & Management of FAIR Sensitive Research Data Project, funded by the Australian Research Data Commons (ARDC).

This national collaborative project is set to deliver:

- a secure, trusted and scalable environment for data governance
- control and management services for data custodians
- secure remote data analysis environments for researchers.

The Data Custodian Community of Practice (CoP) was launched to elicit and clarify the needs of data custodians such that secure data platform operators could build in controls that meet the needs of custodians.

Data custodians require a robust, accredited, regulated and functional environment to satisfy governance requirements and controls for sensitive data. This is critical to enable data cleaning and deidentification, linkage, extraction, sharing with access controls and analysis.

Secure data platforms that, by-design, meet the needs of data custodians will enable researchers to overcome significant barriers to making sensitive data findable, accessible, interoperable, reusable (FAIR).

This document provides an environmental scan of publicly available requirements of data custodians and will be used in conjunction with targeted interviews with key stakeholders, to generate a set of known data custodian requirements of secure data access systems.

The Environmental Scan was completed collectively by the Data Custodian Community of Practice Committee.

Scope of the Environmental Scan

The Environmental Scan was conducted to collect and review publicly available requirements of data custodians. The scan will be used to identify best practice guidelines for operators of secure data access environments.

Note: The Environmental Scan represents the best efforts of the Data Custodian Community of Practice and is intended only as a guide to the regulatory environment governing the use of sensitive data in research. It is not definitive, and readers must satisfy themselves of the particulars of any information presented here.

In scope

The following document types are in-scope for the Environmental Scan, where they have an impact on the sharing of data and the requirements for secure, remote-access data platforms:

- Australian Government and state and territory government legislative instruments
- Regulations made under legislative instruments
- Guidelines (such as NHMRC, published ethical guidelines, government policy documents)
- Security questionnaires (included only where publicly available)
- Significant international instruments with implications for Australian use of data.

Out of scope

- A number of legislative instruments are relevant to data custodians. These have been noted, but not reviewed in the Environmental Scan unless they are also relevant to operators of secure data access platforms.
- Members of the Data Custodian CoP are aware than some data custodians have their own assessments and criteria. The majority of these are not publicly available, and therefore could not been included in this review.
- It is noted that the Scalable Governance, Control & Management of FAIR Sensitive Research Data Project also facilitates Research User, and Research Infrastructure Communities of Practice. As such, this review of resources is limited to the available guidelines and resources specifically developed for data custodians and which impact on the operation of secure data access platforms.

Next steps

- In parallel to this scan, researchers at Curtin University have compiled interviews with key data custodians, on their perspectives on data sharing. This qualitative analysis will uncover what data custodians see as their role, any barriers they encounter, and opportunities for improving data custodianship.

- The Data Custodian CoP will continue to note any data custodian requirement documents to build on repository of guidelines and resources (with publicly available information and with links where possible).
- It may be decided to extend this work to include operational-level requirements in the future.
- The CoP will facilitate two workshops on topics of interest to data custodians, guided by the interviews, to corroborate requirements with a wider group of stakeholders; one in late 2022, and another one in May 2023.A Report on Data Custodian Requirements for System Operators will be developed through the CoP, to be completed by June 2023.

Environmental Scan template

The template below was used to complete the Environmental Scan. The template and the documents to be reviewed were agreed on by the Data Custodian CoP Committee in July 2022.

Item	*Full name of document*
Description of item	*Plain English description of the document*
General	
Document Owner	*Organisation/Individual that produced the instrument*
Document Type	*Legislative Act, Regulation (made under an act), guideline, checklist, policy, template, security questionnaire*
Document source (link)	*Include link to retrieved document here*
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	*Accreditation, penetration testing, data storage and backup, Business Continuity/Disaster Recovery Plans*
Users and access	*Multifactor authentication controls, user computing environments, physical locations*
Structure and projects	*Overall platform structure, research project separation, ingress/egress controls, file and user logging, governance process for projects, reporting*
Computing resources	*Virtual machine setup, CPU/RAM/Disk space available, standard software applications, paid and additional software options*
Project completion	*Data retention/return, data archiving options, data destruction and reporting/certification of destruction*
Other technical requirements	*List any other technical requirements here.*

Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	*Requirements for training of data users, any required accreditation of users including criminal record or working with children checks*
Service levels	*Any documented service level expectations, service desk availability, response times*
Data breach response	*Data breach response/notification time expectations if stated*
Other data governance requirements	*List any other data governance requirements here*
Relevance and implications	
Key benefits and implications for Data Custodians	
Key datasets governed by the instrument	
Relevance to Australian secure data access platform operators	
Issues	
Key issues or omissions relevant to operators of secure data access platforms	

Instruments reviewed

Instruments are listed alphabetically by authoring organisation.

Australian Bureau of Statistics - National Statistical Service: A Guide for Data Integration Projects Involving Commonwealth Data for Statistical and Research Purposes

Item	National Statistical Service: A Guide for Data Integration Projects Involving Commonwealth Data for Statistical and Research Purposes.
Description of item	This guide provides advice to implement the governance and institutional arrangements for statistical data integration involving Commonwealth data as agreed by heads of Australian Government agencies in 2010. It gives effect to the High Level Principles for Data Integration involving Commonwealth Data for Statistical and Research Purposes (the High Level Principles) and applies to all in scope statistical and research projects involving Commonwealth data. The purpose of this guide is to provide conceptual and practical advice to assist data custodians, integrating authorities and data users (such as researchers) in understanding and implementing the framework for data integration projects that use Commonwealth data for statistical and research purposes. It provides guidance on the planning, management and approval processes for Commonwealth statistical data integration projects, as well as advice on practical aspects of managing and conducting projects such as data management and security and appointing an integrating authority with responsibility for the whole project. In many cases, it will be possible to use or adapt existing practices for undertaking data integration projects to align with the Commonwealth arrangements. The guide takes into account the commitments of data custodians under the Privacy Act 1988 and other legislation relating to the disclosure, use or dissemination of the source data. It builds upon already available guidelines including the National Statement on Ethical Conduct in Human Research and related guidelines of the Office of the Australian Information Commissioner, as well as agency specific guidelines and resources.
General	
Document Owner	Australian Bureau of Statistics
Document Type	Guidelines
Document source (link)	https://statisticaldataintegration.abs.gov.au/roles-and-responsibilities/data-custodians

Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	• Secure storage of sensitive and classified material, and high value assets, for example through clear desk and clear screen policies (required to comply with the protective security framework). When unattended, sensitive information or high value assets should be stored in locked cabinets, containers or rooms and computers should be locked by activating the screen saver or logging off. • Assignment of unique personal identification code and a secure means of authentication for system access. • User accounts, access rights and security authorisations managed through an accountable system or records management process. • Protocols that ensure access rights are not shared with or provided to others. • Audit trails that include date and user identification to track and monitor access to systems and data and how they are used. • Control mechanisms to prevent unauthorised access, deletion, modification, duplication, printing or transmission of files. • Systems maintenance plans that provide adequate ongoing resources for security upgrades. • A secure internet gateway. For high-risk projects this gateway must be reviewed annually by Australian Signals Directorate, or equivalent. • Encryption of all electronic data transfer to restrict access to information to authorised users and prevent deciphering of intercepted information. ---Electronic data transfer should only occur where there is a secure internet gateway. • Use of a courier, if there are technical, security or other reasons that restrict the transfer of data electronically. At media level, it is expected that all information contained on the disc or other medium will be encrypted. • Protocols and control mechanisms to prevent storage of sensitive or confidential information on portable devices such as laptops or thumb drives unless they are both encrypted and password protected. This requirement is consistent with the Protective Security Framework. • Storage of datasets associated with an integration project on a password protected stand-alone computer in a secure room or on a password protected server on a computer network with a secure firewall. • To preserve privacy and confidentiality in accordance with High Level Principle 6, identifying information (such as name, address and date of birth) should be used only for the purpose of creating linkage keys and not stored on the integrated dataset, unless specifically required and approved for the project purpose and enabled by legislation.

	• Project-specific linkage keys should not enable links to be established with other datasets or projects. The code (algorithm) used to create linkage keys should also be kept confidential to prevent anyone re-identifying records through their knowledge of the key. • For projects assessed as posing a high risk, the integrating authority must be accredited, that is, they must be approved by the Cross Portfolio Data Integration Oversight Board (the Oversight Board) as having the capacity to deal with high-risk data integration projects.
Users and access	• Access to unit record information is decided on a strict need-to-know basis through a formal approval process. Individuals must only have access to information that is required for them to perform specific functions or tasks for a specific data integration project. The 'need-to-know' principle is a fundamental rule of personnel security according to the Protective Security Framework and is mandatory for all data integration projects. • A senior officer is responsible for managing and monitoring access control, including reviewing who can access particular datasets when personnel move positions and their work no longer requires access. • Appropriate personnel security arrangements are in place to ensure only those who are eligible and suitable to have access to the information are authorised to have access. For example, staff undergo security checks, sign an undertaking to acknowledge their confidentiality responsibilities, and are subject to sanctions or penalties for breaches of confidentiality. In the case of high-risk projects penalties for disclosure should include jail terms and/or fines. • The policies, protocols and obligations regarding security, the protection of personal information and breaches of security or confidentiality are communicated to all staff on an on-going basis through training, policy and procedural documentation and other corporate awareness raising activities. • Induction and training strategies are in place for staff to place a strong emphasis on the appropriate use of the technology environment, e.g. not having passwords written down where they can be discovered by third parties, not storing confidential information on laptops or thumb drives without protection such as encryption and passwords. • Control of access to all buildings or areas where confidential data is accessed or stored. This is required for all security classified information according to the Protective Security Framework and should apply in the case of all high-risk data integration projects. • Sign in registers for all visitors to the building.

	• Reception personnel and/or contract guards. • Wearing of photographic security passes. • Procedures to escort and supervise contractors, consultants and other persons on site when in secure or non-public areas. • Security surveillance and alarm systems (closed circuit TV cameras, CCTV etc. to detect unauthorised access. • Building access control barriers.

Structure and projects	Structure The following list provides an overview of the general stages of a project once all of the agreements have been signed and approved 1. Extract and transfer data - the data custodians provide data to the integrating authority, as was specified in the project agreements. 2. Prepare data for linking - prior to linking, the data needs to be cleaned and standardised. This may be conducted by the data custodians and/or integrating authority. 3. Linking and merging of data - the source data is combined to create a new integrated dataset. This stage is managed by the integrating authority, however, some components may be outsourced or conducted in partnership. 4. Access to integrated data - the integrating authority is responsible for providing the data users with secure access to the integrated dataset, de-identified and confidentialised according to the requirements of data custodians. 5. Analysis of integrated dataset - data users conduct analysis of the integrated dataset and release outputs. 6. Evaluation and project completion - the integrating authority conducts the evaluation and completion of the project, this includes managing the storage or destruction of the integrated dataset **Governance** Data custodians, under the Commonwealth arrangements concern the access and use of Commonwealth datasets in statistical data integration projects, as well as the design and management of administrative data holdings to support wider statistical and research use. Data custodians are responsible for: • In Principal approval • Final approval • Project delivery. Data custodians have the following roles in managing their datasets for data integration: • Role 1 • Maximise the value of data holdings • Role 2 • Assess project risk • Role 3 • Comply with policy and legislation • Role 4 • Ensure safe storage of unit record data • Role 5 • Safely transmit unit record data • Role 6 • Enter project agreements. **Reporting** Data users need to: • give data custodians the opportunity to review the research results prior to publication, if required

	- provide documented feedback to the integrating authority (e.g. procedural or data quality issues).
Computing resources	Not stated.
Project completion	A project is considered complete once the approved purpose of the project is met, the related datasets destroyed, or if retained, the reasons for and necessity of retention documented and a review process set up, for example, if the project is ongoing, or the integrated dataset is required to support a family of projects. Data integration projects using the same source datasets, for similar purposes, with the same integrating authority, are referred to as a family of projects. If such retention was not part of the initial approval process, re-approval of the decision to retain should be obtained from all data custodians. Archiving of statistically integrated data sets should be restricted to confidentialised datasets. Once the approved purpose of the project is met, the integrated dataset and project linkage keys should be destroyed in a way that complies with secure disposal requirements, unless retention of the dataset is required for long-term studies or has otherwise been agreed by data custodians. Linkage keys that have been created to facilitate future studies involving data linkage, should always be stored separately from the integrated dataset and the source dataset, with appropriate security and authorisation controls. If integrated datasets are being retained, the reasons for retention as well as storage and disposal arrangements should be well documented in the project agreements, and a review of storage and access process set up. If such retention was not part of the initial approval process, then the integrating authority must get approval of the decision to retain the dataset from the data custodian(s). This is essential to comply with High Level Principle 6 – Preserving Privacy and Confidentiality. Where identifiers need to be retained, for example for longitudinal studies, they will be kept separate from the integrated dataset and the separation principle observed. The integrating authority is responsible for the integrated dataset and must strictly control access for the life of the data.
Other technical requirements	Ideally, Commonwealth data custodians should provide metadata (information about the data) for each dataset. Providing this information will help integrating authorities and data users to understand the available data and its limitations. The metadata should be made available to prospective data users and to the integrating authority so that they are able to make informed decisions about whether the data will meet the research need or can be successfully linked with other source data.

	The data custodian is responsible for providing source datasets which are of an agreed upon quality, ensuring that data users and the integrating authority are aware of any issues with the quality of the data or limitation of its use. It is important that data custodians are transparent about the quality of their data.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Induction and training strategies are in place for staff to place a strong emphasis on the appropriate use of the technology environment, e.g. not having passwords written down where they can be discovered by third parties, not storing confidential information on laptops or thumb drives without protection such as encryption and passwords.
Service levels	Not stated.
Data breach response	• Contain the breach and do a preliminary assessment. This includes recovering lost records, shutting down the breached system or revoking access privileges. The organisation should then appoint someone to assess the situation. • Evaluate the risks associated with the breach. Organisations should look at the type of information contained in the data breach, and the nature of the breach, to determine what harm it may cause. • Notify those affected by a data breach. The OAIC recommend that this be direct notification by phone, letter, email or in person (unless the costs of direct notification are prohibitive). • Prevent future breaches. Agencies and organisation need to investigate the cause of the data breach and consider if a review of the existing prevention plan is required.
Other data governance requirements	Prior to giving in principle approval for a project, it is the responsibility of data custodians to assess the risk of a project to determine whether a project should proceed and whether an accredited Integrating Authority is required to manage the project. This risk assessment may be undertaken by a ‘lead data custodian’ appointed with the mutual agreement of all data custodians, jointly by all of the data custodians, or individually by each data custodian. Input or clarification may be sought from integrating authorities with expertise in data integration and from data users.

ACT - Health Records (Privacy and Access) Act 1997

Item	Health Records (Privacy and Access) Act 1997
Description of item	The Act provides privacy rights in relation to ACT Government Health Information and for the integrity of Health Information.
General	
Document Owner	ACT Government
Document Type	Legislative Act
Document source (link)	https://www.legislation.act.gov.au/a/1997-125/
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	Privacy Principle 4.1 requires the health records are protected against loss, unauthorised us or disclosure or other misuse. There is no further detail about how this must be achieved.
Users and access	Not stated.
Structure and projects	Privacy Principle 9.1 provides for the use of health records without consent where the use of the information is related to the management, funding or quality of the health service provided to the consumer, providing an avenue for the use of health records in research. Principle 10.3 further clarifies that disclosure for research is permitted where the records are suitably de-identified.
Computing resources	Not stated.
Project completion	Data destruction is addressed under Principle 4.3 but there are no specific instructions on the mode of destruction.
Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	Not stated.
Other data governance requirements	Not stated.

Relevance and implications
The Act provides authority to share health information with researchers in a deidentified form for the purpose of management, funding or quality of the health service provided to the consumer.
ACT Government and health service provider information.
Platform operators as holders of ACT Health Information would be subject to the ACT and should review it and satisfy themselves that they comply with it.
Issues
Not stated.

ACT – Information Privacy Act

Item	Information privacy Act 2014
Description of item	The Act provides for the protection of privacy and personal information by ACT agencies and contractors with Territory Privacy Principles (TPPs).
General	
Document Owner	ACT Government
Document Type	Australian Capital Territory Government Legislative Act
Document source (link)	https://www.legislation.act.gov.au/a/2014-24/
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	Not stated.
Users and access	Not stated.
Structure and projects	Not stated.
Computing resources	Not stated.
Project completion	Not stated.
Other technical requirements	Not stated.

Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	Not stated.
Other data governance requirements	Not stated.
Relevance and implications	
Data custodians dealing with the sharing of ACT Government data need to be aware of the Territory Privacy Principals and ensure they comply with them when releasing data to researchers.	
Platform operators dealing with ACT Government information should familiarise themselves with the Territory Privacy Principals (which are largely aligned with the Australian Privacy Principles).	
Issues	
Not stated.	

Australian Commission on Safety and Quality in Health Care - Data Governance Framework 2016

Item	Australian Commission on Safety and Quality in Health Care: Data Governance Framework 2016.
Description of item	A data governance framework provides a structure for the development and implementation of data management policies. The Australian Commission on Safety and Quality in Health Care's (the Commission) Data Governance Framework provides an overview of its data governance arrangements comprising: • Key data governance concepts including collection, handling and reporting of data in compliance with legislative, regulatory and policy requirements • The Commission structures and roles to support good data management practices • Key data management principles • An overview of policy, guideline and procedures including integrated data management. The framework contains key information for all Commission staff. It is also a source of information for external agencies and funded data collections that may or may not share data with the Commission. The data governance arrangements apply to all data requested, collected or funded by the Commission.
General	
Document Owner	Australian Commission on Safety and Quality in Health Care
Document Type	Framework
Document source (link)	https://www.safetyandquality.gov.au/sites/default/files/2021-06/acsqhc_-_data_governance_framework_-_dec_2016.pdf

Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	**Privacy** The Commission is subject to privacy obligations under the National Health Reform Act, the Privacy Act 1988 and the Privacy Amendment (Enhancing Privacy Protections) Act 2012. The Privacy Act 1988 sets out 13 Australian Privacy Principles (APPs) which apply to the collection, use, disclosure and other aspects of handing of personal information. These principles apply to and must be complied with by the Commission. **Security** Systems and processes used for collection, analysis and storage of data and information have been designed to ensure that the confidentiality, integrity and availability of data and information is protected. Data and information must be maintained in a secure environment and in accordance with the Australian Government Protective Security Policy Framework and the Australian Government Information Security Manual. 1. Data will only be collected, stored, used, published and archived with appropriate authority. 2. Data will be collected, stored, used, and archived according to defined procedures. 3. Data will be defined and documented in a consistent form (metadata), including quality indicators. 4. International and national standards and conventions for data and data management will be formally recognised and adopted where appropriate. Best-practice solutions (e.g. METeOR for metadata) will be adopted for specific aspects of the Commissions business. 5. Wherever possible, data will be collected once, from one source and stored for a defined purpose. 6. Data will be protected with appropriate security systems and procedures. 7. Data will be made easily accessible to users to promote and support re-use, in accordance with authorisation principles and agreements. 8. The input of stakeholders and experts (e.g. in the form of advisory groups) will be used to continually monitor and improve data management practices, particularly in the development of new data sources, safety and quality indicators, collection methodologies, and METeOR specifications. 9. Data management activities will be subject to routine audits to monitor the effectiveness of the implementation of policies and procedures. This process will be facilitated by the Data in Safety and Quality Improvement Working Group.

	Data storage Data can be stored in a variety of methods including: • Structured formats, such as databases, geospatial data and maps • Semi-structured formats, such as spreadsheets • Published formats, including content on websites • Non-structured formats, such as emails, documents, computers, disks, hard drives and USB sticks.
Users and access	Staff will be supported in their data management responsibilities and activities through appropriate and well-resourced systems, procedures, induction materials, education, training and support. By being provided with access to data, data users are assuming responsibilities for its correct use, analysis, interpretation and reporting and they must be supported in this role through effective IT systems, education, training and support.
Structure and projects	The data governance framework for the Commission requires the collaboration and shared responsibilities between: 1. Governance – which provides the Commission's objectives, required outcomes and boundaries for our work, as well as defining and promoting data management activities, standards and skills, and providing the resources to support these activities. 2. People – responsible for acquiring, storing, managing and disseminating data according to data management policies. These people include data stewards, data custodians and data users. 3. Systems – in the form of policies, procedures, security software and hardware to support data management. **Governance** Commission Board - The Commission's board governs the organisation and is responsible for the proper and efficient performance of its functions. Chief Executive Officer - The Chief Executive Officer manages the Commission's day-to-day administration and is supported by an executive management team, internal management committees and staff members. Data in Safety and Quality Improvement Working Group - As part of its role to develop and oversee the implementation of this framework the Data in Safety and Quality Improvement Working Group will assume responsibility for: • Developing, implementing and maintaining the Commission data management policies and • procedures manual.

	• Developing and delivering appropriate education, training and support activities for data • stewards, data custodians and data users. • Establishing and reviewing an overall program of standards, monitoring and compliance, which • encompasses: • Ensuring data holdings are allocated to Data Stewards and data custodians; • Setting, implementing and monitoring standards for: o The storage and use of data holdings (including reference and master data sets) o Security of data holdings o Data quality o Metadata requirements and solutions; and o Other data management compliance measures as required. • Resolving issues raised by data stewards and data custodians. • Initiating and participating in the development of IT solutions for data management activities. • Provide guidance and approval to any metadata standards (including The Metadata Online Registry (METeOR). **People** Data steward - Collectively they are responsible for ensuring that data custodians and data users have an awareness and understanding of the Commission’s data management policies and procedures, and access to appropriate education and training in order to implement those policies and procedures. For each of the data holdings under their care, Data Stewards also have a responsibility to ensure that their users have access to the information (mostly in the form of metadata) and skills they require to correctly access and use that data. A data steward will provide clear delegation and instructions to data custodians so that access and security privileges to their data holdings are maintained and monitored. Data custodian - Data users are those staff within the Commission who need access to the data for analysis but who are not custodians or stewards of the data. Data users normally have varying levels of data literacy and data management skills. Data Users - Data users are those staff within the Commission who need access to the data for analysis but who are not custodians or stewards of the data.
Computing resources	Not stated.

Project completion	Not stated.
Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Data users must be supported in this role through effective IT systems, education, training and support.
Service levels	Not stated.
Data breach response	Not stated.
Other data governance requirements	Over time the Commission will develop and measure compliance with data management policies and procedures, based on the assessment of risks. As an organisation the Commission will need to determine the highest risk data management activities and ensure that there are checks and safeguards in place. In addition to systems support for compliance, the Commission will implement reviews and audits of specific aspects of data management to assess levels of compliance, and any issues which may be limiting the Commission's ability to comply. The Data in Safety and Quality Working Group has responsibility for implementing data management compliance systems and support, as well as for initiating reviews and audits.
Relevance and implications	
This instrument defines systems and processes used for collection, analysis and storage of data and information in compliance with legislative, regulatory and policy requirements, key data management principles and provides and overview of policy, guidelines and procedures including integrated data management.	
Health Information and sensitive information. Health information includes: • Information collected in connection with the provision of a health service • Information or opinion about the health or disability of an individual • An individual's expressed wishes about the provision of health services • Any information about health services provided to an individual.	
The information provided in this instrument could help inform secure data access platform operators regarding security controls, data storage and data management principles.	

Issues
The use of the data governance framework will ensure that data conforms to appropriate standards of data management and quality prior to use, and data are used in accordance with appropriate approvals. This document does not contain information about data disclosure and reporting, staff education, support and training, user and access controls, and data deletion. Other policy documents developed by the Commission need to be referenced to find out this information.

Australian Government - Healthcare Identifiers Act 2010

Item	Healthcare Identifiers Act 2010
Description of item	*"This Act facilitates the use of the healthcare identifier for the purposes of communicating and managing health information about a healthcare recipient (including through the My Health Record system)."*
General	
Document Owner	National Health and Medical Research Council (NHMRC)
Document Type	Australian Government Legislative Act
Document source (link)	https://www.legislation.gov.au/Details/C2017C00239
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	Healthcare identifiers such as a Medicare number, their use and disclosure are strictly regulated by the Act.
Users and access	Not stated.
Structure and projects	Health identifiers may only be assigned by authorised services providers and their use. Use for research approved by a NHMRC-registered HREC is permitted under the act but would likely not be approved unless there was a compelling reason to do so.
Computing resources	Not stated.
Project completion	Not stated.
Other technical requirements	Not stated.

Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	Not stated.
Other data governance requirements	Not stated.
Relevance and implications	
Not stated.	
Medicare Benefits Schedule, Pharmaceutical Benefits Scheme, My Health Record (though not in the de-identified form normally used for research).	
Secure data access platform operators should be aware that healthcare identifiers are a special class of information under this act and ensure they comply with the act if a project is planned that includes them.	
Issues	
Not stated.	

Australian Government - My Health Records Act 2012

Item	My Health Records Act 2012
Description of item	*“Health information may be collected, used and disclosed from a healthcare recipient’s My Health Record for the purpose of providing healthcare to the recipient, subject to any access controls set by the recipient (or if none are set, default access controls). There are other limited circumstances in which health information may be collected, used or disclosed from a My Health Record.”*
General	
Document Owner	Australian Government
Document Type	Australian Government Legislative Act
Document source (link)	https://www.legislation.gov.au/Details/C2017C00313

Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	The Act establishes My Health Record Rules which may include the System Operator proving My Health Record Information for research.
Users and access	Not stated.
Structure and projects	Not stated.
Computing resources	Not stated.
Project completion	Not stated.
Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	Not stated.
Other data governance requirements	Not stated.
Relevance and implications	
Authorised data custodians may compile My Health Record data for the purposes of research.	
Research data derived from My Health Record will require platform operators to review the Act and comply with it, though if de-identified data is used for research, then standard privacy and information security controls should already be aligned with the requirements of the Act.	
Issues	
Not stated.	

Australian Government – Privacy Act 1988

Item	Privacy Act 1988 and (Privacy Notifiable Data Breaches) Act 2017
Description of item	The Privacy Act 1988 (Cth) and the Privacy (Notifiable Data Breaches) Act 2017 (Cth).
General	
Document Owner	Australian Government.
Document Type	Legislative Act and amendments.
Document source (link)	https://www.legislation.gov.au/Details/C2014C00076.
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	The Act establishes 13 Australian Privacy Principles (APPs) which bind Australian entities, including data custodians and secure platform operators. The Act also gives the Information Commissioner the responsibility to receive and investigate complaints and to make determinations in relation to complaints. The Act applies both to personal information and health information about an individual. There are some exceptions in dealing with personal information. The Act also gives the CEO of the NHMRC the power to issue guideline to protect privacy in medical research or the provision of health services. Notifiable data breaches – See below.
Users and access	Not stated.
Structure and projects	Research projects which are completed outside Australia using Australian Data may be subject to the Act under Section 5B.
Computing resources	Not stated.
Project completion	Compliance with the APPs extends to all parts of the project and the secure destruction of potentially re-identifiable data is an important part of ensuring a project does not infringe on privacy. Data custodians will often require evidence of data destruction and platform operators should be cognisant of the effect this requirement on the design of platform backup and archiving solutions.
Other technical requirements	Not stated.

Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	A mechanism for defining and reporting notifiable data breaches was established in the Privacy (Notifiable Data Breaches) Act 2017. The implications of this is that secure data access platforms need to have a data breach mechanism that includes notification of data breaches to data custodians and/or the Information Commissioner within an agreed timeframe to allow compliance with the Act.
Other data governance requirements	Not stated.
Relevance and implications	
Data custodians share data with researchers in a way that is compliant with the Act and NHMRC guidelines. Custodians are likely to require data breach response plans and privacy plans be provided for review before authorising a platform operator to hold their data.	
The Privacy Act applies to all personal and health information held by government or other Australian entities.	
Platform operators should have well-developed plans to address the privacy principals and potential reportable breaches and these plans should be periodically reviewed for compliance with the Act.	
Issues	
Not stated.	

Australian Government - Rights Responsibilities and Roles of Data Custodians 2013

Item	Rights, responsibilities and roles of data custodians.
Description of item	This paper identifies the rights, responsibilities and roles of data custodians relative to those of the other key participants in data integration projects involving Commonwealth data for statistical and research purposes, namely integrating authorities and users of integrated datasets.
General	
Document Owner	Australian Commonwealth Government
Document Type	Guidelines
Document source (link)	https://toolkit.data.gov.au/Data_Integration_-_Roles_and_responsibilities_of_data_custodians.html
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	Before data custodians release data to an integrating authority they need to consider: • Existing legislation which enables the release of, and access to, data by integrating authorities (i.e., legislation which applies to data custodians and integrating authorities). • Privacy impacts relating to the use and disclosure of personal information or business data. This may include an assessment against the Commonwealth Privacy Act and equivalent state/territory or other legislation. Agency-specific legislation will also need to be considered. It is the responsibility of data custodians to ensure they are authorised by legislation or consent to release identifiable data to an integrating authority. The data custodians must also be satisfied that the integrating authority has the necessary legislative protections in place prohibiting disclosure of identifiable data, before the commencement of a data integration project. A Privacy Impact Assessment should be considered for ‘high risk’ projects. This will help data custodians identify and address any potential privacy risks around the collection, use and release of data.
Users and access	It is the responsibility of data custodians to ensure good data management practices, (including clear documentation, the use of standard definitions and classifications, the maintenance of appropriate metadata, and quality assurance) are undertaken before data is provided to an integrating authority. It is the right of data custodians to have data linkage, merging and access services provided on their behalf by an integrating authority.

Structure and projects	**Governance** Data custodian - Data custodians are agencies responsible for managing the use, disclosure and protection of source data used in a statistical data integration project. Data custodians collect and hold information on behalf of a data provider (defined as an individual, household, business or other organisation which supplies data either for statistical or administrative purposes). The role of data custodians may also extend to producing source data, in addition to their role as a holder of datasets. **Platform Structure** Data custodians have six key roles in the Commonwealth data integration arrangements. These roles reflect the need for data custodians to strike a balance between maximising the inherent value of data assets and minimising privacy concerns associated with the use of this data. The roles are: • Safe storage of unit record level information; • Assessing the level of risk for each data integration project; • Ensuring compliance with relevant legislation, including privacy, for data release; • Entering into agreements with integrating authorities; • Safe transmission of data; and • Maximising the value of data holdings.
Computing resources	Not stated.
Project completion	Data users may be required to seek clearance from data custodians on the use and interpretation of data before publishing research outputs.
Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	Integrating Authorities undertaking high risk data integration projects must be bound by the Commonwealth Privacy Act (or a state/territory equivalent) and be subject to criminal penalties for a breach of legislation with regard to an unauthorised disclosure of information. For low and medium risk projects, at a minimum, integrating authorities must have an appropriate policy framework in place to ensure that no identifiable data is disclosed, other than where allowed by legislation.

Other data governance requirements	A key role of data custodians is to determine the level of risk for a data integration project, using the risk assessment framework developed for Commonwealth data integration projects. The level of risk is an important part of determining if a project should proceed and whether an accredited Integrating Authority is required to manage the integration project (i.e. if the project is assessed as high risk). Each data custodian must enter into an agreement with a nominated integrating authority. This agreement may take the form of a contract, Memorandum of Understanding or other arrangement as appropriate for the parties concerned. When the data custodian and integrating authority is the same agency, appropriate internal governance arrangements, rather than an agreement, will need to be in place. The purpose of a project agreement is to help ensure that datasets are managed and used in accordance with data custodian requirements throughout the life of the project.
Relevance and implications	
This document helps define the responsibilities and rights and roles of the data custodian in relation to release of, and access to, source datasets for data integration projects. It also forms the basis for how data custodians will work collaboratively with other participants involved in the data integration projects. The core elements for the terms of a project agreement are provided in this document.	
Commonwealth data for statistical and research purposes.	
The information provided in this instrument could help inform secure data access platform operators regarding the key factors to be considered before releasing data to an integrating authority and the rights and responsibility of data custodians in relation to integrating authorities and to data users. The roles of data custodians involving maximising the inherent value of data assets and minimising privacy concerns associated the use of the data are clearly defined here.	
Issues	
These guidelines identify issues data custodians need to consider before releasing data to an integrating authority including: existing legislation, privacy impact relating to the use and disclosure of personal information or business data, the existence of any data protocols governing access to and the use of data sets and that the data integration project takes into account the public benefit which can be derived from the use of integrated datasets.	

Australian Government - Best Practice Guide to Applying Data Sharing Principles 2019

Item	Best Practice Guide to Applying Data Sharing Principles 2019
Description of item	This Guide has been written to assist agencies holding Australian Government data (data custodians) to safely and effectively share the data they are responsible for by using five Data Sharing Principles (the Principles). This Guide has been structured to assist data custodians to consider the appropriate safeguards to apply before sharing Government data, and to promote more flexible, principle-driven data access arrangements. Part 1 contains information and questions for data custodians to consider prior to sharing data, such as the data sharing maturity of an organisation and their approach to managing risk. Part 2 explains each of the Principles in a practical order, beginning with the project assessment. It provides examples of how each principle operates and poses questions to help data custodians apply them. Part 3 includes further guidance on how to manage data sharing agreements once they are in place.
General	
Document Owner	Australian Commonwealth Government (Department of the Prime Minister and Cabinet)
Document Type	Guidelines
Document source (link)	https://www.pmc.gov.au/sites/default/files/publications/data-sharing-principles-best-practice-guide-15-mar-2019.pdf
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	**Data Security** • Data to be held in a subsystem within the data custodian's IT system. • Protecting work areas from oversight of unauthorised people. • Maintaining a 'clear screen' (i.e. securing workstations appropriately when away). • Not on-sharing information to unauthorised people. • Requiring outputs that are intended for wider sharing to be approved by the data custodian. • Reporting any security incidents to the data custodian as soon as practicable. • Not removing any of the information from the approved setting without authorisation. • Not sharing login details.

	• Keeping physical copies (for example, CD, USB stick or printed) of data locked away and secured during transfer to a user. Data can be provided in the form of a downloaded file on a secure drive rather than transferring it to portable media. It is recommended that removal of direct identifiers is applied in most cases of data sharing. Identifiers should only be retained if they are absolutely critical for the project being considered and even then encryption of identifiers is a preferable option.
Users and access	• Working in an agreed location (for example, in a personal office, an access controlled room or at home). • Direct and active supervision. • Access during certain restricted times. • Making users aware of surroundings and taking care in open plan offices to avoid data being viewed on screen by unauthorised people. Protecting work areas from oversight of unauthorised people. • Maintaining a 'clear screen' (i.e. securing work stations appropriately when away). Closed IT environment with no external email or internet access. • Role-based access. • Two-factor authentication. • Recording of access sessions, with auditing/review conducted in a transparent manner. There are also closed IT systems with password-protected, role-based access available (such as the ABS DataLab, the Secure Unified Research Environment (SURE), the Secure eResearch Platform (SeRP) or the E-Research Institutional Cloud Architecture (ERICA)) through which many government agencies undertake their work.
Structure and projects	**Governance** Acknowledging the value of public sector data, and the need use it efficiently and with appropriate safeguards, the Australian Government established the Office of the National Data Commissioner (ONDC) in July 2018. The ONDC is responsible for implementing a data sharing framework that improves access to and re-use of public sector data, while maintaining data privacy and security. **Data Sharing Framework** The ONDC, together with the Australian Bureau of Statistics (ABS), has developed the Principles to support agencies' 'responsibility to share' by providing an approach for effectively managing the risks associated with

	data sharing. The Data Sharing Principles are based on the Five Safes Framework. 1. Projects: Data is shared for an appropriate purpose that delivers a public benefit. 2. People: The user has the appropriate authority to access the data. 3. Settings: The environment in which the data is shared minimises the risk of unauthorised use or disclosure. 4. Data: Appropriate and proportionate protections are applied to the data. 5. Output: The output from the data sharing arrangement is appropriately safeguarded before any further sharing or release.
Computing resources	Government agencies may undertake their work using closed IT systems with password-protected, role-based access available such as the ABS DataLab, the Secure Unified Research Environment (SURE) or the E-Research Institutional Cloud Architecture (ERICA).
Project completion	Retention of data on a secure server or specific computer/drive with appropriate password and access protections. Requirements to provide evidence of data destruction at the end of project or project approval period.
Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Training can provide benefits to all parties, ensuring everyone understands their obligations and responsibilities in a data sharing community. The training should emphasise the positive behaviours and attitudes necessary to use the data in a manner consistent with the requirements of the data sharing agreements. The legal consequences of data misuse need to be raised in training, but it is also important that users understand other non-legal penalties can apply, such as withdrawal of access to data, which may detrimentally affect all data users within a community. Training should also be simple, user-centred, positive and interactive (for example, data misuse scenarios can be used to highlight, and facilitate discussion about, legal, moral and procedural issues around data sharing). The data custodian, or a training provider engaged by the data custodian, may deliver tailored training. It can be used to clearly convey that an organisation must meet its obligations, and that individual users must understand how to appropriately access, use and destroy data, consistent with the data sharing agreement.

	An alternative to training may be to provide users with a “do and don’t” document. This approach should be used cautiously as it has been found to be less effective than face-to-face training, although it may be acceptable if controls in the other Principles are enhanced. Users are less likely to read a long document and it may not be able to effectively articulate all nuances of appropriate and inappropriate data use. As a complement to the training, the data custodian may choose to periodically test users to ensure they understand their responsibilities and can demonstrate appropriate attitudes and behaviours regarding safe data use. For example, providing a scenario relating to an observed procedural breach and requesting the user describe how they would respond to the event, rather than simply asking whether they should report an observed breach. It is recommended that at a minimum, testing be conducted at the same time, or as soon as possible after, the training. Combining tools may also be appropriate in that a test could be used to train people by asking for their views on do’s and don’ts. The user may be required to undergo an authorisation process to assess the user’s knowledge, skills and motivations to determine whether they can use (and in some cases store) any shared data appropriately.
Service levels	Not stated.
Data breach response	Any breaches of terms and conditions (such as unauthorised accesses or privacy breaches) need to be reported and appropriate actions taken.
Other data governance requirements	Not stated.
Relevance and implications	
This Guide has been structured to assist data custodians to consider the appropriate safeguards to apply before sharing Government data. It provides information and questions for data custodians to consider prior to sharing data, such as the data sharing maturity of an organisation and their approach to managing risk. It includes five principals for data sharing which provide a disclosure risk management framework which balances risks against public benefit. It provides guidance on what needs to be considered after the Principles have been applied including whether the controls appropriately safeguard the data to be shared.	
Public sector data that the government collects from individuals and businesses or generated through administrative functions of government agencies.*t*	
The information provided in this instrument could help inform secure data access platform operators regarding security controls, data storage and access, training and an approach for effectively managing the risks associated with data sharing.	

Issues
Barriers to sharing data easily can be mitigated with appropriate risk management. The Data Sharing Principles detailed in this instrument provide an approach for effectively managing the risks associated with data sharing and enabling safe and effective sharing of data held by the public sector in a way that delivers public benefit, protects privacy and maintains confidentiality.

New South Wales Government - Government Information Public Access Act 2009

Item	Government Information (Public Access) Act 2009
Description of item	An Act to facilitate public access to government information.
General	
Document Owner	New South Wales Government
Document Type	Legislative Act
Document source (link)	https://legislation.nsw.gov.au/view/html/inforce/current/act-2009-052
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	Not stated.
Users and access	Part 4 stated the access applications to government information.
Structure and projects	Not stated.
Computing resources	Not stated.
Project completion	Not stated.
Other technical requirements	Not stated.

Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	Part 6 stated the protections and offences related to government information.
Other data governance requirements	Not stated.
Relevance and implications	
Key benefits and implications for data custodians	Relevant if include government information.
Key datasets governed by the instrument	Government information.
Relevance to Australian secure data access platform operators	Applicable if facilitate government information data sharing.
Issues	
Key issues or omissions relevant to operators of secure data access platforms	Not stated.

New South Wales Government - Health Records and Information Privacy Act 2002

Item	Health Records and Information Privacy Act 2002
Description of item	An Act to make provision for the protection of health records and information; and for other purposes.
General	
Document Owner	New South Wales Government
Document Type	Legislative Act
Document source (link)	https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2002-071

Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	**Schedule 1 Health Privacy Principles** 5 Retention and security (1) An organisation that holds health information must ensure that— (a) the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and (b) the information is disposed of securely and in accordance with any requirements for the retention and disposal of health information, and (c) the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and (d) if it is necessary for the information to be given to a person in connection with the provision of a service to the organisation, everything reasonably within the power of the organisation is done to prevent unauthorised use or disclosure of the information. Note— Division 2 (Retention of health information) of Part 4 contains provisions applicable to private sector persons in connection with the matters dealt with in this clause. (2) An organisation is not required to comply with a requirement of this clause if— (a) the organisation is lawfully authorised or required not to comply with it, or (b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the State Records Act 1998). (3) An investigative agency is not required to comply with subclause (1)(a).
Users and access	Part 4 Division 3 Access to health information, contains specific provisions for private sector persons that are additional to, and assist the operation of, the general principles in HPP 7 (Access to health information).
Structure and projects	Not stated.
Computing resources	Not stated.

Project completion	Not stated.
Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	Proceedings for an offence against this Act are to be dealt with summarily before the Local Court.
Other data governance requirements	Part 2 General operation of Act 11 How this Act applies to organisations (1) This Act applies to every organisation that is a health service provider or that collects, holds or uses health information. Note— The term organisation means a public sector agency or a private sector person. (2) An organisation to whom or to which this Act applies is required to comply with the Health Privacy Principles and with any health privacy code of practice or provision of Part 4 that is applicable to the organisation. (3) An organisation must not do any thing, or engage in any practice, that contravenes a Health Privacy Principle or a health privacy code of practice or a provision of Part 4 in respect of which the organisation is required to comply. Note— The application of Health Privacy Principles and the provisions of Part 4 may be modified by health privacy codes of practice. See section 39.
Relevance and implications	
Key benefits and implications for data custodians	Relevant if include NSW Health Records and Information.
Key datasets governed by the instrument	It applies to every organisation that is a health service provider or collects, holds or uses health information.
Relevance to Australian secure data access platform operators	Applicable if facilitate NSW health information data sharing.

Issues	
Key issues or omissions relevant to operators of secure data access platforms	Not stated.

New South Wales Government - Privacy and Personal Information Protection Act 1998

Item	Privacy and Personal Information Protection Act 1998
Description of item	An Act to provide for the protection of personal information, and for the protection of the privacy of individuals generally; to provide for the appointment of a Privacy Commissioner; to repeal the Privacy Committee Act 1975; and for other purposes.
General	
Document Owner	New South Wales Government
Document Type	Legislative Act
Document source (link)	https://legislation.nsw.gov.au/view/html/inforce/current/act-1998-133
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	**Part 1 Preliminary - Division 1 Principles** 12 Retention and security of personal information A public sector agency that holds personal information must ensure— (a) that the information is kept for no longer than is necessary for the purposes for which the information may lawfully be used, and (b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, and (c) that the information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse, and (d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.
Users and access	Not stated.

Structure and projects	Not stated.
Computing resources	Not stated.
Project completion	Not stated.
Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	**Part 8 Miscellaneous** 62 Corrupt disclosure and use of personal information by public sector officials (1) A public sector official must not, otherwise than in connection with the lawful exercise of his or her official functions, intentionally disclose or use any personal information about another person to which the official has or had access in the exercise of his or her official functions. Maximum penalty—100 penalty units or imprisonment for 2 years, or both. (2) A person must not induce or attempt to induce a public sector official (by way of a bribe or other similar corrupt conduct) to disclose any personal information about another person to which the official has or had access in the exercise of his or her official functions. Maximum penalty—100 penalty units or imprisonment for 2 years, or both. (3) Subsection (1) does not prohibit a public sector official from disclosing any personal information about another person if the disclosure is made in accordance with the Public Interest Disclosures Act 1994. (4) In this section, a reference to a public sector official includes a reference to a person who was formerly a public sector official. 70 Proceedings for offences Proceedings for an offence against this Act are to be dealt with summarily before the Local Court.
Other data governance requirements	Not stated.

Relevance and implications	
Key benefits and implications for data custodians	Clarification of personal information and provide the protection of personal information.
Key datasets governed by the instrument	Not stated.
Relevance to Australian secure data access platform operators	1. Regulation to refer if include Personal information on the platform 2. The definition of personal information
Issues	
Key issues or omissions relevant to operators of secure data access platforms	Not stated.

New South Wales Government - Statutory Guidelines on Research (HRIPA 2002)

Item	Statutory Guidelines on Research (Health Records and Information Privacy Act 2002)
Description of item	An Act to facilitate public access to government information.
General	
Document Owner	New South Wales Government
Document Type	Guidelines under Act
Document source (link)	https://www.ipc.nsw.gov.au/sites/default/files/file_manager/privacy_statutory_guidelines_research.pdf
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	The health information should be retained in a form that is at least as secure as it was in the sources from which the health information was obtained unless more stringent legislative or contractual provisions apply. Researchers must be responsible for ensuring the appropriate security for any confidential material, including that held in computing systems.
Users and access	The procedures formulated by institutions must include guidelines on the establishment and ownership of and access to databases containing confidential information, and any limits on this. Access to health information is restricted to appropriate personnel involved in conducting the proposed study.

Structure and projects	Not stated.
Computing resources	Not stated.
Project completion	Not stated.
Other technical requirements	Where computing systems are accessible through networks, particular attention to security of confidential data is required. Security and confidentiality must be assured in a way that copes with multiple researchers and the departure of individual researchers.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	Failure to comply with statutory guidelines constitutes a breach of the HRIPA 2002.
Other data governance requirements	When the data are obtained from limited access databases, or via a contractual arrangement, written indication of the location of the original data, or key information regarding the database from which it was collected, must be retained by the researcher or research unit.
Relevance and implications	
Key benefits and implications for data custodians	Relevant if study includes NSW Health Records and Information.
Key datasets governed by the instrument	It applies to every organisation that is a health service provider or collects, holds or uses health information.
Relevance to Australian secure data access platform operators	Applicable if facilitate NSW health information data sharing.
Issues	
Key issues or omissions relevant to operators of secure data access platforms	Not stated.

National Health and Medical Research Council - Australian Code for the Responsible Conduct of Research (2018)

Item	Australian Code for the Responsible Conduct of Research, 2018 (the 2018 Code)
Description of item	The 2018 Code provides a framework for "high-quality research, credibility and community trust in the research endeavour".
General	
Document Owner	National Health and Medical Research Council (NHMRC)
Document Type	Guideline
Document source (link)	https://www.nhmrc.gov.au/about-us/publications/australian-code-responsible-conduct-research-2018
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	The 2018 Code makes it a responsibility of institutions to provide facilities for the safe and secure storage of materials and the training and education of researchers in responsible research conduct.
Users and access	Not stated.
Structure and projects	Compliance with the 2018 code is a requirement of NHMRC and Australian Research Council Funding.
Computing resources	Not stated.
Project completion	Not stated.
Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	The 2018 Code requires institutions to provide appropriate training and education of researchers in responsible research conduct.
Service levels	Not stated.
Data breach response	Not stated.
Other data governance requirements	Not stated.

Relevance and implications
No specific relevance to data custodians or platform operators except that research institutions are responsible for ensuring data is held and used securely.

National Health and Medical Research Council - Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and communities: Guidelines for researchers and stakeholders 2018

Item	Ethical conduct in research with Aboriginal and Torres Strait Islander Peoples and communities: Guidelines for researchers and stakeholders 2018 (the Guidelines)
Description of item	The Guidelines are for use by researchers and ethical bodies to ensure research is safe, respectful, responsible, high quality and of benefit to Aboriginal and Torres Strait Islander people.
General	
Document Owner	National Health and Medical Research Council (NHMRC)
Document Type	Guidelines
Document source (link)	https://www.nhmrc.gov.au/about-us/resources/ethical-conduct-research-aboriginal-and-torres-strait-islander-peoples-and-communities
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	Projects with Aboriginal and Torres Strait Islander people need to recognise the right to assert and retain ownership of the cultural and intellectual property related to the information that is provided to a research project.
Users and access	Not stated.
Structure and projects	Platform operators should be aware of the need for approval from an Aboriginal Health Research Ethics Committee in research with Aboriginal and Torres Strait Islander Peoples and of intellectual property rights, including data sovereignty arrangements in research agreements: *“Research agreements should cover the management of Aboriginal and Torres Strait Islander cultural and intellectual property rights. It is important to note that Western law may establish different forms of intellectual and cultural property or protect it in different ways to how Aboriginal and Torres Strait Islander Peoples conceive and recognise their cultural and intellectual property.”* *“This means anything that is written, spoken or created by Aboriginal and Torres Strait Islander Peoples, whether it is a story, a painting, a*

	sculpture, an object, a dance, a song, or music (cultural practices) and any knowledge of their land, culture or kinship that is used to express their cultural identity, should be considered the cultural and intellectual property of the contributor (and, potentially, their community) and should be respected as such. It is acknowledged that Aboriginal and Torres Strait Islander Peoples' intellectual property continues to expand via inclusion of contemporary creative and original works that have originated from Aboriginal and Torres Strait Islander cultural heritage."
Computing resources	Not stated.
Project completion	While the Guidelines do not specify data retention and destruction requirements, issues of IP and data sovereignty should be discussed with researchers to ensure expectations relating to the research data are met by the platform operator.
Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Platform operators should ensure staff are aware of the Guidelines and Principles and are ready to address project-specific requirements.
Service levels	Not stated.
Data breach response	Not stated.
Other data governance requirements	Not stated.
Relevance and implications	
Data custodians have guidance on the fundamental principles of research with Aboriginal and Torres Strait Islander Peoples.	
Platform operators should be aware of the potential need for data governance practices to include provision for handing the data of Aboriginal and Torres Strait Islander Peoples in a way consistent with the principles in the Guidelines.	
Issues	
No specific requirements are set out in the guidelines for platform operators.	

National Health and Medical Research Council - National Statement on Ethical Conduct in Human Research 2007 (updated 2018)

Item	National Statement on Ethical Conduct in Human Research2007 (Updated 2018)
Description of item	The National Statement provides guidance on the ethical conduct of research for: NHMRC-registered HRECs, researchers, research participants.
General	
Document Owner	National Health and Medical Research Council (NHMRC)
Document Type	Guideline
Document source (link)	https://www.nhmrc.gov.au/about-us/publications/national-statement-ethical-conduct-human-research-2007-updated-2018
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	The National Statement gives HRECs a framework for assessing risk of disclosure of information and guidance to balance the risks associated with human research against the expected benefits of research projects. The Statement includes a section on the “Collection, Use and Management of Data and Information” including guidance on data minimisation and separation and the use of secured computing environments.
Users and access	The National Statement makes no specific recommendations on the requirements for platforms except that they must be secure.
Structure and projects	The National Statement is a document dealing entirely in research governance and requires the development of Data Management Plans for human research. It also has specific sections on biospecimens and genomics research and outlines requirements for research with Aboriginal and Torres Strait Islander people.
Computing resources	Not stated.
Project completion	The National Statement requires that Data Management Plans consider secure data retention and eventual disposal at project completion but does not specify standards.
Other technical requirements	Not stated.

<table>
<tr><th colspan="2">Custodian Requirements of Secure Data Access Platforms (Data Governance)</th></tr>
<tr><td>User training or accreditation</td><td>The National Statement requires that HRECs or other ethical review bodies consider whether researchers are appropriately qualified to conduct research.</td></tr>
<tr><td>Service levels</td><td>Not stated.</td></tr>
<tr><td>Data breach response</td><td>The National Statement provides guidance on the suspension of research and possible withdrawal of ethical approvals due to adverse events that may affect participants but does not touch on data breach protocols or</td></tr>
<tr><td>Other data governance requirements</td><td>Not stated.</td></tr>
<tr><th colspan="2">Relevance and implications</th></tr>
<tr><td colspan="2">The National Statement provides a well-developed and trusted guide to understanding the risks of various types of ethical research and the processes to control and minimise risk.</td></tr>
<tr><td colspan="2">The guidance set out in the National Statement is used by HRECs and other ethical review bodies to assess the benefits and risks of research projects, including risks to privacy of participants.</td></tr>
<tr><th colspan="2">Issues</th></tr>
<tr><td colspan="2">HRECs and other ethical review bodies are required to assess the adequacy of data protection and security for each research project though does not specify detailed standards.</td></tr>
</table>

Northern Territory Government - Data Custodianship Guidelines

Item	NT Government Data Custodianship Guidelines
Description of item	*Plain English description of the document*
General	
Document Owner	*National Health and Medical Research Council (NHMRC)*
Document Type	Policy/Guidelines
Document source (link)	https://dipl.nt.gov.au/lands-and-planning/building/northern-territory-land-information-systems-ntlis/ntlis-policies-and-standards/data-custodianship-guidelines?curr=252115&print=yes&SQ_PAINT_LAYOUT_Not stated.ME=multi
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	Not stated.
Users and access	Not stated.
Structure and projects	Custodians are responsible for providing metadata consistent with ANZLIC metadata guidelines and for the coverage, completeness, quality, currency and accuracy of data. The guidelines also encourage users of NT data to advise custodians of errors or omissions in datasets.
Computing resources	Not stated.
Project completion	Not stated.
Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	Not stated.

Other data governance requirements	Not stated.
Relevance and implications	
NT Government data custodians are provided with guidance on the sharing of data, including for the purpose of research.	
The Guidelines as they do not provide any specific requirements to be met by operators.	
Issues	
Not stated.	

Queensland Government - Environmental Protection Water Policy 2009: Data Handling (Ver: Feb 2018): Custodianship and management

Item	Data Handling (Ver: Feb 2018): Custodianship and management
Description of item	This is a three-page document. Which forms part of the Environmental Protection Water Policy 2009 – Monitoring and Sampling Manual. Defining custodianship and outlining data management procedures, including quality assurance and control.
General	
Document Owner	*Environmental Protection (Water) Policy 2009: Department of Environment and Science*
Document Type	*Internal policy document*
Document source (link)	*https://environment.des.qld.gov.au/__data/assets/pdf_file/0023/90374/data-handling-custodianship-and-management.pdf*
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	N/A – the policy chapter doesn’t address security or privacy needs. Where security is mentioned “a structured data management system that provides reliable and secure consistent storage, access and reporting”. This is about the need for secure measures
Users and access	N/A – the policy chapter focuses on data capture (via instruments in environment) and the need for data custodians to be responsible for “for ensuring data are collected, maintained and made available according to standards, policies or other licences, agreements or

	specifications”. Other than the role of data custodians elements around use/access to ensure this best-practice is undertaken is not discussed.
Structure and projects	N/A – data transfer, storage etc is not discussed – however the principals of good data management (in general) are noted: Clear and available documentation, standard definitions and classifications, complete metadata, and storage capability (not further clarified)
Computing resources	Not stated.
Project completion	Not stated.
Other technical requirements	While not a tech requirement the policy document notes that data provided by third parties (in the environmental protection field) stored via the Queensland Government does not make the government responsible for what is stored. “The provision of correct and accurate data is the sole responsibility of the data custodian, and the Queensland Government will not be held responsible for incorrect data submitted by other organisations or agencies.”
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	N/A – the focus is not on people using the data stored but third parties capturing and storing the data on the Queensland Government Platform. Details on how are not provided.
Service levels	Not stated.
Data breach response	Not stated.
Other data governance requirements	Detail around minimum data captured and provided is covered but at a overarching level – not detailed.
Relevance and implications	
This policy document – is an information guide that informs data custodians (focusing on third party data collectors) about (superficially) data management, data collection and custodianship.	
Water and environmental protection data collection – what appears to be captured by third party or non-Government entities.	
No relevance. The policy document provides some value around defining roles and minimum data standards – but it doesn’t address issues of secure data platforms	
Issues	
Generic and of limited value to platform operators.	

Queensland Government - Queensland Government Enterprise Architecture: Data Governance Guideline 2019

Item	Data governance guideline: October 2019 | v1.0.1 | OFFICIAL – Public
Description of item	Providing information to Queensland Government Agencies – around the need for better planning, monitoring and controlling of their data. A 20-page document
General	
Document Owner	Queensland Government Enterprise Architecture
Document Type	Guidelines
Document source (link)	https://www.qgcio.qld.gov.au/documents/data-governance-guideline
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	Data security is discussed as a need – the "how to" is not provided. Data security is – assessing the confidentiality, availability and integrity of data and ensuring that it is appropriately accessed and used." – for guidance around data security and privacy practice a URL is provided: https://www.qgcio.qld.gov.au/documents/information-security-policy (this policy statement provides details about minimum needs ISO27001 and risk management processes etc.).
Users and access	Access is discussed as a requirement (no barriers) – "data should be accessible" but only "to the right people who have access to the right data at the right time" – who, what, when and how with respects to access data is not detailed.
Structure and projects	Elements of structure and project systems are noted – issues around data architecture, storage, security – are offered – but these are definitional or descriptors. Controls for data flow, user access, action logs are not highlighted.
Computing resources	Not stated.
Project completion	Not stated.
Other technical requirements	The policy notes the value of data steering committees and delegation roles, governance roles, around data access. This is outside of the data custodian role but worthy to note.

Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	The guidelines highlight the value and necessity of training but do not proffer what this training should entail or associated accreditation.
Service levels	Not stated.
Data breach response	As part of the data lifecycle management the guidelines highlight the need to minimise or manage data breaches – but this is without detail of identification, reporting, reacting.
Other data governance requirements	Not stated.
Relevance and implications	
The guidelines provides a functional diagram offering an overview of the process of implementing data governance outlined in this guideline. It is a valuable document re: data governance; to be used to form a response structure – but there is a need for process/actions regarding 'how to'. There are a number of hyperlinks in the document that may be useful in providing solutions to 'how-to'. These were not explored in this scan.	
The document is designed to cover all datasets considered assets of the Queensland Government	
Highly relevant to secure data access operators – but noting a guideline so possibly more higher-level.	
Issues	
Not stated.	

South Australian Government – Health Care Act 2008

Item	SA Health Care Act 2008
Description of item	This act provides for the governance, management and administration of the South Australian public health system.
General	
Document Owner	State Government of South Australia
Document Type	Legislative Act
Document source (link)	https://www.legislation.sa.gov.au/lz?path=%2FC%2FA%2FHealth%20Care%20Act%202008
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	Not stated.,
Users and access	Not stated.
Structure and projects	Not stated.
Computing resources	Not stated.
Project completion	Not stated.
Other technical requirements	Not stated..
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	Not stated.
Other data governance requirements	Not stated.

Relevance and implications
Key datasets governed by the instrument: South Australian public health datasets.
Relevance to Australian secure data access platform operators is limited. The Act provides the overarching basis for empowering the SA Health Minister to approve secondary uses of the data ("authorised activities"). In provides no further conditions on this use. It is only relevant for South Australian health datasets.
Issues
Key issues or omissions relevant to operators of secure data access platforms.

Tasmanian Government - Personal Information and Protection Act 2004

Item	Personal Information and Protection Act 2004
Description of item	The Acts purpose is to protect the privacy of individuals by controlling the ways in which the government can collect, keep, use, and release records containing sensitive personal information that clearly identifies an individual. The Act also enables individuals to access that information. This information can appear in many different kinds of records, including case files and patient records kept by the Departments of Health and Human Services and Justice, as well as their predecessors.
General	
Document Owner	Tasmanian Government - Attorney General
Document Type	Legislative Act
Document source (link)	https://www.legislation.tas.gov.au/view/whole/html/inforce/current/act-2004-046
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	Not stated.
Users and access	Not stated.
Structure and projects	Not stated.
Computing resources	Not stated.
Project completion	Not stated.

Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	Not stated.
Other data governance requirements	**Collection and Disclosure** Use and disclosure *(1) A personal information custodian must not use or disclose personal information about an individual for a purpose other than the purpose for which it was collected unless –* *(c) if the use or disclosure is necessary for research or the compilation or analysis of statistics in the public interest, other than for publication in a form that identifies any particular individual –* *(i) it is impracticable for the personal information custodian to seek the individual's consent before the use or disclosure; or* *(ii) the personal information custodian reasonably believes that the recipient of the information is not likely to disclose the information;* **Sensitive information** *(2) A personal information custodian may collect sensitive information about an individual if –* *(a) either of the following applies:* *(i) the collection is necessary for research or the compilation or analysis of statistics in the public interest and any resulting publication does not identify the individual;* *(4) A personal information custodian may collect sensitive information that is health information about an individual if –* *(a) the collection is necessary for any of the following purposes:* *(i) research relevant to public health or public safety;*
Relevance and implications	
The Act grants data custodians the right to disclose data for the purpose of research.	

Sensitive information is defined as: *(a) personal information or an opinion relating to personal information about an 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 preferences or practices; or* *(ix) criminal record; and* *(b) health information about an individual;* The format of data is not specified nor restricted
Issues
Not stated

Victorian Government – Centre for Victorian Data Linkage Guidelines

Item	The Centre for Victorian Data Linkage (CVDL) Guidelines
Description of item	The Centre for Victorian Data Linkage (CVDL) was established in 2009 with the aim of developing data linkage capacity and infrastructure in Victoria in line with best practice. In 2018, the CVDL was accredited as by the Commonwealth Government an integrating authority, able to link sensitive Commonwealth data. This document provides an overview of the CVDL, the data linkage assessment and approval process, datasets available in the CVDL's Integrated Data Resource and the Virtual Machine access model.
General	
Document Owner	Victorian Government
Document Type	Guidelines
Document source (link)	https://www.health.vic.gov.au/reporting-planning-data/data-custodians
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	Data Requestors from Department of Health (DH) or other government departments are required to complete a privacy threshold assessment and if required a full Privacy Impact Assessment on their project. The CVDL will undertake a privacy impact threshold assessment and if required a full Privacy Impact Assessment (PIA) for external research projects. All external Data Requestors must complete the DH Deed of Acknowledgment and Confidentiality which outlines the terms and conditions of access to the data (with signatures from all recipients of the data and from the organisation legally responsible for the project). The use of personal and health information in Victoria is governed by the Privacy and Data Protection Act 2014 and the Health Records Act 2001. The use of personal and health information in data linkage must accord with the Information Privacy Principles and Health Privacy Principles described in these Acts. The CVDL is currently implementing a secure cloud-based environment Victorian data Access Linkage Trust (VALT), for release of linked data for approved requests. This will involve researchers

	accessing linked data for specific projects in a secure Virtual Machine. The Microsoft Azure platform is used by CVDL. The Azure cloud environment has been certified up to “Protected” by the Information Security Registered Assessors Program (IRAP) of the Commonwealth. Researchers require authorisation from the CVDL for removal of research results and outputs from the Virtual Machine to ensure a sufficient level of aggregation has been undertaken to meet privacy and confidentiality requirements. The CVDL employs data separation to help protect an individual's privacy during the linkage and integration process. This separation means that an individual’s identifying information is kept separate from the corresponding content information and access by the CVDL staff is restricted to either one type of data or the other.
Users and access	**Accessing linked data** • A project-specific virtual machine is created in the DH Microsoft Azure data analysis environment which contains the approved linked, unit-record level, de-identified data for the project. • Creation and maintenance of the project-specific virtual machine will incur a cost which will be charged to the Data Requestor on a cost recovery basis. • Approved Data Requestors’ login to the project-specific virtual machine and analyse the data using a range of data analysis tools. Using the project Linkage ID, the researcher can determine which records from different datasets belong to the same individual, without having access to personal identifiable information. • Unit-record level data cannot be downloaded or copied from the virtual machine. Aggregated outputs are vetted by the CVDL before they can be removed from the environment. • On completion of the project and/or after a timeframe approved by the CVDL, access to the virtual machine is removed.
Structure and projects	Governance Data custodians are responsible for good data management practices, including how the information is securely collected, managed and disclosed while in their care. The Centre for Victorian Data Linkage (CVDL) works closely with data custodians to ensure they understand their responsibilities and accountability for authorising the release of their data for an

approved research project. The use of each dataset involved in a data linkage project must be approved by the relevant data custodian.

CVDL's objective is to ensure the terms and conditions of any agreement fully reflect the data custodian's interests and requirements, and that adequate controls are observed by all parties.

Data Linkage team

The CVDL Linkage team uses the Victorian Linkage Map (VLM) to find records that belong to the individuals that are the subject of the project in the approved datasets, and assign an anonymous Linkage ID that represents an individual.

Data Integration team

The CVDL Integration/Content team uses the Linkage ID to extract the approved content data items from the relevant datasets and creates new project specific person IDs.

Data de-identification processes are undertaken (i.e. aggregation and removal of personal identifiable data) to minimise the risk of re-identification of the data.

Quality assurance is undertaken ensuring technical and administrative processes are aligned with the research request.

A technical specification is produced and provided to the Data Requestor to finalise, and formalised what the disclosed linked output will entail (this is the final step before the Content team undertakes the content extraction, it is imperative that you ensure your requirement have been met.

Client Services team

The Client Services role is to initially assess the linkage technical feasibility of the research project, and assist with the administration and coordination of the project from the application stage through to the delivery of the linked data.

<ins>Structure</ins>

The Data Requestor completes and submits the CVDL’s data linkage application - The application process requires the requestor to document their research or policy questions in detail and to identify which data items will assist in addressing these questions.

The data linkage application undergoes a technical feasibility assessment - which involves checking:

	(i) the application against the Information Privacy and Health Privacy principles from respective Acts ensuring the individual's privacy is maximise, and assessing the potential risk of re identification (ii) the availability of requested data items, operational considerations, data access requirements, and alignment with the department's objectives. A member of the Client services team contacts the Data Requestor to arrange access to a secure folder within the CVDL's SharePoint site. Reporting/Presentation of data As part of the department's terms and conditions to access linked data, all analysis reports and/or presentation of linked data provided by DH must be provided to DH (via the CVDL Client services team) for review before submission for publication.
Computing resources	Separate virtual machines (data environments) will be set up for each approved project, and registered users provided with access to their project specific data via their project virtual machine. While multiple researchers can be registered to use a specific virtual machine, however, there can only be two concurrent users on each virtual machine. Researchers can analyse the data on the virtual machine, using available software such as R, Python and SQL. Researchers will also have access to Microsoft Office suite of products. Researchers may request to install preferred software such as Stata on a virtual machine on a BYO licence arrangement. Approved researchers will be provided with a log-on to access the virtual machine.
Project completion	On completion of the project and/or after a timeframe approved by the CVDL, access to the virtual machine is removed.

Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Once the data custodian has approved a data linkage project, a member of the CVDL Client Services team will work with the data custodian to: • Ensure all supporting documents are in place, including at the administrative, technical and operational levels • Determine and document the agreed information needed for the linkage project • Prepare a data extraction plan prior to the extraction process commencing • Establish data transfer protocols to ensure security obligations are met. The Client services team can provide input/or feedback on the Human Research Ethics Committee (HREC) applications relating to accessing the linked data. Client services team will assist in providing an indication on a completion timeframe for each project depending on the complexity of the request and provision of all relevant approvals.
Data breach response	Not stated.
Other data governance requirements	An ethical review and approval of all research projects is a statutory requirement under the Health and Information Privacy Principles. Data Requestor external to the Victorian Government must obtain Human Research Ethics Committee (HREC) approval from an accredited Victorian HREC or, for cross-jurisdictional studies, from a HREC accredited under the National Mutual Acceptance scheme. Data Requestors Internal to Victorian Government require Victorian HREC approval if the request is of a sensitive nature meets the criteria under Health Privacy Principle 2.2G or Information Privacy Principle 2.1C or is published externally.

Relevance and implications

This instrument defines the responsibilities of data custodians in terms of the project assessment and approval process for each dataset involved in a data linkage project held by the Victorian Government and external to the Victorian Government. This instrument outlines the range of processes to ensure compliance with the requirements of the Privacy and Data Protection Act and Health Records Act, as well as best practice data linkage techniques.

- These datasets are most commonly used in data linkage projects, however the CVDL also links additional datasets on a project-by-project basis where authorisation is provided by the data custodian.

- Victorian Admitted Episodes Dataset
- Victorian Emergency Minimum Dataset
- Victorian Cost Data Collection
- Public mental health services
- Alcohol and Drug Information System
- Victorian Integrated Non-Admitted Heath Dataset
- Elective Surgery Information System
- Victorian Cancer Registry
- Victorian Radiotherapy Minimum Dataset
- Mental Health Community Support Services
- Family Services
- Family Violence Services
- Sexual Assault Services
- Disability Services
- Homelessness Services
- Victorian Death Index
- Community Health
- Child Protection
- Public Housing Tenancies
- Perinatal data collection
- Australian Early Childhood Development Census
- Intensive Care Registry
- Trauma Registry
- Cardiac Thoracic Registry
- Home and Community Care
- Early childhood intervention
- Births Registry
- Public housing applications
- Public Health Event Surveillance

The information provided in this instrument could help inform secure data access platform operators regarding security and privacy controls, data management principles, governance requirements and computing resources required including virtual machine access.

Issues
The use of The Centre for Victorian Data Linkage (CVDL) Guidelines will ensure that data linkage capacity and infrastructure in Victoria is in line with best practice with the aim to safely manage health information and cross jurisdictional research projects. This instrument does not include any information on training or data breaches.

Victorian Government – Victorian Health Records Act 2001

Item	Victorian Health Records Act 2001
Description of item	The purpose of this Act is to promote fair and responsible handling of health information. The Act provides a framework to protect the privacy of individuals' health information. This document contains information on the application of this Act for private and public sector organisations and exemptions. It contains information on access to health information and making a complaint. The Act establishes the 11 Health Privacy Principles (HPPs) that will apply to health information collected and handled in Victoria by the Victorian public sector and the private sector.
General	
Document Owner	Victorian Government
Document Type	Legislative Act
Document source (link)	https://content.legislation.vic.gov.au/sites/default/files/2022-08/01-2aa.047%20authorised.pdf
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	The Act contains a schedule of 11 privacy principles - The Health Privacy Principles (HPPs) The access regime and the HPPs are designed to protect privacy and promote patient autonomy, whilst also ensuring safe and effective service delivery, and the continued improvement of health services. The HPPs generally apply to: • All personal information collected in providing a health, mental health, disability, aged care or palliative care service • All health information held by other organisations.

	A number of the Health Privacy Principles, and the access and correction regime created by the Act, involve obtaining the consent of the individual whose health information is held. The HPPs can be summarised as: HPP 1 - COLLECTION Health information may only be collected if it is necessary for the organisation’s functions and if the individual has given consent. Some exceptions to consent exist. Health information must be collected lawfully, fairly, reasonably and preferably, directly from the individual. HPP 2 - USE AND DISCLOSURE OF HEALTH INFORMATION The organisation may only use or disclose health information about an individual for the primary purpose for which the information was collected or for a directly related and reasonably expected secondary purpose. Some exceptions exist. HPP 3 - DATA QUALITY The organisation must take reasonable steps to ensure the health information held is accurate, complete, up-to-date and relevant to the organisation’s functions or activities. HPP 4 - DATA SECURITY AND DATA RETENTION The organisation must protect health information from unauthorised access, modification, or disclosure. Health service providers must retain health information for the period set out in HPP 4.2. All other holders of health information must destroy or permanently de-identify health information if it is no longer needed. HPP 5 - OPENNESS The organisation must ensure the privacy procedure is easily accessible so people know what information is held about them, why it's being held and how their information is collected, stored, used and disclosed. HPP 6 - ACCESS AND CORRECTION Individuals have a right to access and correct any health information held about them. The organisation may, in some circumstances, refuse to provide access to health information or to correct it.

	HPP 7 - UNIQUE IDENTIFIERS The organisation may only assign identifiers, such as patient identification numbers, to individuals if this step is reasonably necessary for the organisation to function efficiently. HPP 8 - ANONYMITY As far as it is lawful and practical, individuals should have the opportunity to maintain their anonymity. HPP 9 - TRANSBORDER DATA FLOWS When health information travels outside Victoria, the organisation has a responsibility to ensure that the privacy of the information is safeguarded. HPP 10 - TRANSFER OR CLOSURE OF THE PRACTICE OF A HEALTH SERVICE PROVIDER If a health service provider is sold, transferred or closed down, and the provider is no longer there, it must notify its current or former clients via a public notice. A notice in the practice and letters to current clients are also required. Statutory regulations apply. HPP 11 - MAKING INFORMATION AVAILABLE TO ANOTHER HEALTH SERVICE PROVIDER Upon request from an individual, a health service provider must make information about that individual available to another health service provider.
Users and access	**Access to health information** Individuals have an enforceable right of access to their health information under the Victorian Health Records Act 2001 (the Act), if the request for access is made to a private sector organisation on or after 1 July 2002. Access requests to Victorian public sector organisations will continue to be subject to the Freedom of Information Act 1982.
Structure and projects	This Act is administered by the Health Services Commissioner. Structure of the Act The Health Privacy Principles (HPPs) in the Act apply to health information that is handled in Victoria. The Act will apply in two main ways. 1. Does the organisation provide a health, disability or aged care service?

	When an organisation provides a health, disability or aged care service, the HPPs apply to all identifying personal information originally collected by the organisation in the course of providing that service. All such information is "health information". Such a provider is referred to in the Act as a "health service provider". This will include personal information collected to provide services by: 2. Personal information collected in other situations The HPPs will apply to the collection, use and handling of identifying personal information that is defined as "health information" under the Act. This will include: • information or opinion about the physical or mental health, or disability, of an individual • an individual's expressed preferences about the future provision of health, disability or aged care services to him or her • the nature of health, disability or aged care services that have been, or are to be, provided to an individual • information originally collected in the course of providing a health, disability or aged care service to an individual • personal information collected in connection with the donation of human tissue • genetic information that is or could be predictive of the health of an individual or their descendants. Any organisation that handles this kind of identifying health information is subject to the HPPs, unless an exemption under the Act applies. The exemptions under the Act are very limited. The Act applies regardless of the size of the business or organisation. There is no "small business" exemption.
Computing resources	Not stated.
Project completion	**Data retention** *A health service provider must not delete health information relating to an individual, even if it is later found or claimed to be inaccurate, unless:* *(a) the deletion is permitted, authorised or required by the regulations or any other law;* *or (b) the deletion is not contrary to the regulations or any other law and occurs*

	(i) in the case of health information collected while the individual was a child, after the individual attains the age of 25 years; *or (ii) in any case, more than 7 years after the last occasion on which a health service was provided to the individual by the provider— whichever is the later.* *An organisation other than a health service provider must take reasonable steps to destroy or permanently de-identify health information if it is no longer needed for the purpose for which it was collected or any other purpose authorised by this Act, the regulations made under this Act or any other law.*
Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	An organisation must not do an act, or engage in a practice, that breaches a Health Privacy Principle or the access regime created by the Act. A contravention of the Health Privacy Principles is an interference with the privacy of an individual.
Other data governance requirements	Not stated.
Relevance and implications	
This instrument defines a framework for the collection and handling of health information that protects the privacy of the individual's information by applying privacy principles in compliance with laws and regulations.	
Datasets covered include: health, disability and aged care information handled by a wide range of public and private sector organisations. This includes health service providers, and also other organisations that handle such information. For example: • Bodies such as companies, incorporated associations, unincorporated associations, Local Government, Victorian Government agencies and Departments, public hospitals and other public bodies (such as Victoria Police); and • Sole practitioners, partnerships, Members of Parliament, and trustees.	
The information provided in this instrument could help inform secure data access platform operators regarding privacy principles that can be applied to the collection and handling of health information.	

Issues
The Health Records Act 2001 (the Act) creates a framework to protect the privacy of individuals' health information. It regulates the collection and handling of health information. It establishes Health Privacy Principles (HPPs) that will apply to health information collected and handled in Victoria by the Victorian public sector and the private sector. This Act does not include information on best practice guidelines for operators of secure data access environments such as data backup and recovery, user controls, computing resources, training, data breaches and governance requirements etc.

Western Australian Government - Freedom of Information Act 1992

Item	Freedom Of Information Act 1992
Description of item	An Act to provide for public access to documents, and to enable the public to ensure that personal information in documents is accurate, complete, up to date and not misleading, and for related purposes. Creates a general right of access to documents held by all state and local government agencies
General	
Document Owner	Attorney General
Document Type	Legislative Act
Document source (link)	https://www.legislation.wa.gov.au/legislation/prod/filestore.nsf/FileURL/mrdoc_44917.pdf/$FILE/Freedom%20Of%20Information%20Act%201992%20-%20%5B07-e0-00%5D.pdf?OpenElement
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	Not stated.
Users and access	Not stated.
Structure and projects	Not stated.
Computing resources	Not stated.
Project completion	Not stated.
Other technical requirements	Not stated.

Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Not stated.
Service levels	Not stated.
Data breach response	Not stated.
Other data governance requirements	*Access to a document may be given to the applicant in one or more of the following ways:* *(g) in the case of electronically, mechanically or magnetically stored information — by giving a written expression of the information in the form in which it is commonly available in the agency, or if there is no such common form, then in a form no less comprehensible than could be made available to the persons in the agency.* *If the applicant has requested that access to a document be given in a particular way the agency has to comply with the request unless giving access in that way –* *(a) would interfere unreasonably with the agency's other operations; or* *(b) would damage or harm the document or would be inappropriate because of the physical nature of the document; or* *(c) would involve an infringement of copyright belonging to a person other than the State,* *in which case access may be given in some other way.* Section 32: Personal information about third party, when access to maybe given This section applies to a document that contains personal information about an individual (the third party) other than the applicant. Various restrictions BUT: This section does not apply if access is given to a copy of the document from which the personal information referred to in subsection (1) has been deleted under section 24.
Relevance and implications	
Freedom of Information gives the public a right to access government documents, subject to some limitations. In Western Australia, under the Freedom of Information Act 1992 (the FOI Act), the right applies to documents held by most State government agencies (such as departments, public hospitals, public universities and State government authorities), Ministers and local government. Together, these bodies are referred to as "agencies".	

Agencies are required to assist applicants to obtain access to documents at the lowest reasonable cost. Access to documents is to be given under Parts 2 and 4 despite any prohibitions or restrictions imposed by other enactments (whether enacted before or after the commencement of this Act) on the communication or divulging of information, and a person does not commit an offence against any such enactment merely by complying with this Act. Anyone can also apply to have personal information about themselves in government documents amended if that information is inaccurate, incomplete, out of date or misleading.
Documents accessible under the FOI Act include paper records, plans and drawings, photographs, tape recordings, films, videotapes or information stored in a computerised form.
Issues
Not stated.

Western Australian Government - Privacy and Responsible Information Sharing public consultations

Item	Privacy and Responsible Information Sharing Consultation Summary Report
Description of item	The WA Government recognises that privacy is very important to Western Australians and is committed to ensuring everyone has the opportunity to have their say on the best arrangements for WA. Some proposed arrangements were outlined in a discussion paper which was opened for discussion by the general public, the WA public sector and a number of organisations in research and business. This report is a summary of this consultation.
General	
Document Owner	Government of Western Australia
Document Type	Consultation Report
Document source (link)	https://www.wa.gov.au/government/publications/summary-report-privacy-and-responsible-information-sharing
Custodian Requirements of Secure Data Access Platforms (Technical)	
Data security and privacy	Nothing specific – only that personal information should be protected wherever it is. Sensitive personal information should have greater protections.
Users and access	Not stated.

Structure and projects	Not stated.
Computing resources	Not stated.
Project completion	Not stated.
Other technical requirements	Not stated.
Custodian Requirements of Secure Data Access Platforms (Data Governance)	
User training or accreditation	Recommendation only: Government staff should be trained to prevent, report and respond to data breach.
Service levels	Not stated.
Data breach response	Recommendation only: There should be a clearly defined process to deal with breaches of privacy and breaches should be reported publicly.
Other data governance requirements	Recommendation only: Agencies should be open about what they're doing with personal information Government and its contractors should be open about how they handle and use personal information, including who it is shared with.
Relevance and implications	
The consultation feedback highlighted many people's concerns over the handling of personal information. Individuals want to know that their personal information is protected. Individuals and organisations want agencies to be open about what they are doing, how they handle and use personal information, and who it is shared with.	
While the information in this document is not a requirement of data custodians, it reflects the broader communities view on how data is managed, particularly if personal information is stored. It is important that these recommendations are seriously considered.	
Issues	
Not stated.	