Defining 'trusted entities' for the purposes of national data sharing

Appendix 4: Use case - Victorian Department of Health and Department of Families, Fairness and Housing

Use case information

Identifying Characteristic	Details
Use case name	Integrated Data Resource (IDR)
Date	Ongoing
Data Requester	Victoria Department of Health (DH) Victoria Department of Families, Fairness and Housing (DFFH) Universities/External Researchers
Data Custodian	Victoria Department of Health (DH) Victoria Department of Families, Fairness and Housing (DFFH)
Data Characteristics	Personal Sensitive Information Health Records Unique Identifiers Health Services Data Social Services Data Education Data
Approved purpose	The IDR is used for research, policy development and service delivery.
Approved timeframe	Since 2017 with ongoing annual refreshes.
Legal basis for sharing	Relevant legislation that applies on a case-by-case basis includes: • *Children, Youth and Families Act 2005* (Vic) • *Disability Act 2006* (Vic) • *Drugs, Poisons and Controlled Substances Act 1981*(Vic) • *Health Services Act 1988* (Vic) • *Housing Act 1983* (Vic) • *Inquiries Act 2014* (Vic) • *Mental Health and Wellbeing Act 2022* (Vic) • *Public Health and Wellbeing Act 2008* (Vic) • *Royal Commissions Act 1902* (Cth)

Identifying Characteristic	Details
	• *Victorian Data Sharing Act 2017* (Vic).
Additional Notes	The IDR is a data asset/sharing system that follows the 'share-once, use-often' principle and delivers many to many sharing. The IDR is managed by the Centre for Victorian Data Linkage (CVDL) in DH/DFFH. The IDR may only be accessed within the Victorian Data Access Linkage Trust (VALT) which is a secure access environment. VALT is a certified Accredited Data Service Provider by the Office of the National Data Commissioner. The CVDL was established in 2009 as Victoria's specialist linkage unit and has extensive experience in undertaking data linkage and integration services for government and researchers over the past 15 years. The CVDL undertakes around 100 new linkage projects each year, and many ongoing projects with regular or periodic linkage. The CVDL has extensive experience in linking data sets across health, human services, justice, police and education. This includes linkage of some Commonwealth datasets, including MBS, PBS and the Australian Immunisation Register. The CVDL primarily undertakes linkage using identifiers, but also has experience with Privacy Preserving Record linkage, such as Bloom Filters. At any time, CVDL's total project workload averages around 170 projects, including new and ongoing projects, and a small number of project amendments. Researchers and Victorian departments can place an application to CVDL to access data in the IDR.

Alignment with attributes

The below table displays the alignment of the use case with the trusted entity attributes.

- **Strong alignment:** The data custodian required the data requester to provide significant evidence of the attribute to assess trustworthiness.
- **Partial alignment:** The data custodian required the data requester to provide some evidence of the attribute to assess trustworthiness.
- **Not assessed:** The data custodian did not assess the attribute, or it was not applicable.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Transparency	**Verifiable audit and assurance processes** Where appropriate, internal and external processes will be implemented to verify compliance with legal and ethical standards, including those related to data environments and systems.			✓	Not applicable as the data is accessed in a secure access environment managed by the CVDL.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Transparency	**Public transparency standards** The agency will have public-facing processes and/or standards for data release and publication.			✓	Not assessed as data custodians that provide data to the CVDL for linking are responsible for maintaining their own public transparency information.
Transparency	**Transparent and defined project methodology** Clear and transparent project methodologies, including integration approaches, output vetting and risk management procedures, will be documented and shared with the relevant data custodian.	✓			Data requesters must submit a linkage request application, which includes a detailed project specification that specifies research/policy objectives and the requested data. The CVDL reviews the project specification and determines whether the project is feasible from both a technical and governance perspective. The CVDL team and the researcher work together to discuss potential issues in achieving the research objectives. This process enables the CVDL team to develop familiarity with different research methods and current research topics, while the researchers are provided with a better understanding of issues or limitations with the data requested. Output vetting is conducted jointly by the CVDL and data custodians.
Accountability	**Legally supported sharing** Data sharing arrangements will be legally authorised and supported by clear documentation such as agreements and data sharing registers.	✓			Requesters are required to sign data sharing agreements and/or confidentiality agreements.
Accountability	**Ethical consideration** Projects will undergo ethics consideration and where required approval, consent and review processes to ensure alignment with ethical standards.		✓		Depending on the legislative enabler to access the IDR an ethics assessment may be required.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
Accountability	**Defined roles and responsibilities** Agencies will have clear data roles and responsibilities to ensure accountability.	✓			Requesters are asked to exhaustively list who will have access to the data and their roles and contact information.
Accountability	**Authorised and skilled personnel** Personnel will have the knowledge, skills, authorisation and training to use data appropriately, including training in data breach and risk management.			✓	While project applicants manage the authorisation and skill level of their personnel accessing the data, CVDL staff have strong alignment with this attribute. The CVDL and relevant data custodians review the project application and outputs from a technical and governance perspective to ensure data will be used appropriately.
Data Management and Governance	**Data quality processes** Data quality management plans will be implemented to ensure data integrity and compliance.			✓	Not applicable as the data quality of the IDR is managed by the CVDL.
Data Management and Governance	**Data governance authorisations** Agencies will have established data governance processes which have clear decision-making authorisations. This includes an understanding of the agencies data governance priorities, dispute resolution processes and accountable data custodianship roles.	✓			
Data Management and Governance	**Defined metadata management practices with accountable data custodianship roles** Agencies will have defined metadata management practices which are accurate, consistent and accessible across the agency. This includes data lineage information.			✓	Not applicable as the metadata of the IDR is managed by the CVDL.
Data Management and Governance	**Consistent and controlled data release protocols**			✓	Not applicable as the CVDL has identified a standard list of variables that require confidentiality in consultation with data custodians. The CVDL reviews

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	Agencies will have clear operating models for data release, including for review, verification, and approval for release.				the outputs from the VALT and only releases the outputs such as tables, PowerPoint slides and reports if they meet confidentiality requirements. Unit record data is not released from VALT.
Data Management and Governance	**Established escalation and risk management frameworks** Agencies will have established escalation pathways for managing risks and incidents. Projects will have comprehensive risk management plans which consider privacy by design and security risk assessments.		✓		As data is accessed in the VALT, many of the risks associated with data access and data breaches are mitigated or managed by the CVDL team. Requesters and their agencies are required to comply with any mandated privacy breach reporting procedures. Data requesters and users are required to implement safeguards to minimise confidentiality risks by assessing the project risk against the ABS's Five Safe principles.
Security	**Secure transfer mechanisms** Agencies have secure mechanisms for data transfer to prevent breaches.			✓	Not applicable as data is only accessible in VALT.
Security	**Secure access control mechanisms** Agencies will implement data safeguards, use secure access environments appropriate to the sensitivity of the data, and restrict data access to authorised users with appropriate security clearances.			✓	Not applicable as data is only accessible in VALT.
Security	**Certified secure environment** Data will be accessed within certified secure environments appropriate to the classification of the data, e.g. ONDC Accredited Data Service Provider, IRAP-certified or Essential 8.			✓	Not applicable as data is only accessible in VALT.
Security	**Consistent security labelling and classification**			✓	Not applicable as security labelling and classification is managed by CVDL.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.				
Security	**Established security clearance assessments** Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.	✓			Where appropriate security clearance assessments are required to access data in CVDL.
Security	**Incident monitoring and response mechanisms** Mechanisms for incident monitoring, identification, and response are in place.			✓	Not applicable as incident monitoring is managed by CVDL.
Privacy	**Data minimisation protocols** Agencies will implement the privacy by design principle, including minimising the collection and storage of personal data to what is necessary to achieve the project, and adhering to approved retention and disposal practices.	✓			The CVDL team will ask requesters to fill out a technical specifications document which includes the research question and the specific data items required from the IDR. This is reviewed and assessed by the CVDL team to ensure that only the data items necessary for the specific research questions are provided.
Privacy	**De-identification mechanisms** Agencies will have controls and safeguards to manage re-identification risks, including removing direct identifiers, limiting access to sensitive data, using secure transfer mechanisms or controlled environments, and adhering to the separation principle.	✓			Requesters must meet confidentiality requirements to receive outputs from the VALT project specific virtual machine such as tables, PowerPoint slides and reports.
Privacy	**Privacy incident reporting** Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.	✓			Requesters and their agencies are required to comply with any mandated privacy breach reporting procedures.