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

Appendix 7: Use case – Commonwealth Department of Health, Disability and Ageing

Use case information

Identifying Characteristic	Details
Use case name	Supplying health data for the Person-Level Integrated Data Asset (PLIDA)
Date	Ongoing
Data Requester	The Australian Bureau of Statistics (ABS)
Data Custodian	The Department of Health, Disability and Ageing (DHDA)
Data Characteristics	Health data included: • Australian Immunisation Register (AIR) • Medicare Benefits Schedule (MBS) • Pharmaceutical Benefits Scheme (PBS)
Approved purpose	Analysis, research and statistical purposes
Approved timeframe	Data supplied to the ABS for period specified in the Public Interest Certificate (PIC).
Legal basis for sharing	Data sharing is authorised under the *National Health Act 1953*, *Health Insurance Act 1973* and *Australian Immunisation Register Act 2015*. DHDA issues PICs under these Acts. Data provided to the ABS is also protected by the *Census and Statistics Act 1905*.
Additional Notes	DHDA has data sharing arrangements with trusted data brokers to supply health data for approved purposes. An example is provision of data for the Person-Level Integrated Data Asset (PLIDA), a linked data asset that is managed by the ABS. The ABS provides access to PLIDA data to approved users in the ABS DataLab environment (or other ABS secure environments). Requests to conduct projects using PLIDA undergo an assessment and approval process, managed by the ABS. For a project to be approved, the ABS and the Data Custodians (the agencies responsible for the source data, in this case DHDA) must agree to the proposed use of the data. The ABS provides project proposals requesting PLIDA data to DHDA via a secure 'myData' Portal. The DHDA reviews and determines if the project proposal meets DHDA requirements, and if so, approves the proposal. The ABS then provides the researchers with access to PLIDA.

	The ABS is an Accredited Data Service Provider (ADSP) which means the National Data Commissioner has deemed the ABS capable of handling public sector data and minimising risk of unauthorised access or use. The ABS is authorised to undertake complex data integration, de-identification, and provide secure data access services to support data sharing. The DHDA leverages the ABS' accreditation (which is subject to ongoing monitoring by the Office of the National Data Commissioner) to be assured that the ABS consistently implements and performs appropriate data handling processes.

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.		✓		DHDA knows the ABS is subject to multiple compliance and assurance processes to meet Australian Government requirements, such as adhering to the Protective Security Policy Framework, and Infosec Registered Assessors Program (IRAP) cyber-security reviews. This information is available on the ABS website. DHDA also relies on the ABS's ONDC accreditation to trust that appropriate audit and assurance processes are in place.
Transparency	**Public transparency standards** The agency will have public-facing processes and/or standards for data release and publication.	✓			The ABS publishes information on its website about how PLIDA data can be accessed for research. DHDA leverages the many documents ABS publishes to have assurance of processes and standards.
Transparency	**Transparent and defined project methodology** Clear and transparent project methodologies, including integration approaches, output vetting and risk management procedures, will be	✓			The ABS uses the Five Safes Framework to facilitate safe data access and release. The ABS, in their role as data broker, provides DHDA with comprehensive research documentation for potential projects. This allows DHDA to make informed decisions about the appropriate use of their data.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	documented and shared with the relevant data custodian.				
Accountability	**Legally supported sharing** Data sharing arrangements will be legally authorised and supported by clear documentation such as agreements and data sharing registers.	✓			Data is supplied to PLIDA through a PIC from DHDA. The ABS provides approved researchers with secure access to integrated data under the Census and Statistics Act. The ABS' clear legislative authority for making data available in ways that protect privacy and maintain confidentiality provides assurance to DHDA when utilising them as a data broker.
Accountability	**Ethical consideration** Projects will undergo ethics consideration and where required approval, consent and review processes to ensure alignment with ethical standards.	✓			At the discretion of DHDA, Human Research Ethics Committee approvals are required for PLIDA projects that involve DHDA data. The ABS also conducts regular Privacy Impact Assessments of PLIDA.
Accountability	**Defined roles and responsibilities** Agencies will have clear data roles and responsibilities to ensure accountability.	✓			DHDA knows the ABS has processes in place to ensure only appropriate people can access data, such as application of the separation principle. ABS staff are also bound by the secrecy provisions in the Census and Statistics Act. DHDA also relies on ABS's ONDC accreditation to provide assurance that the ABS has appropriately trained staff.
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.	✓			The ABS is an Accredited Data Service Provider (ADSP) which means they have proven they have appropriately trained and experienced staff to manage data. The ABS provides technical training for personnel working with PLIDA data, and researchers requesting access to PLIDA must complete PLIDA training to be onboarded onto the PLIDA environment. This aligns with DHDA requirements.
Data Management and Governance	**Data quality processes**	✓			The ABS applies data quality management plans which includes guidance and validation protocols for personnel accessing PLIDA.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	Data quality management plans will be implemented to ensure data integrity and compliance.				
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.	✓			Specific authorisation roles are defined in the PIC which authorises DHDA to share data with ABS.
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 DHDA data custodians are responsible for data assets in PLIDA including the preparation of metadata and source data.
Data Management and Governance	**Consistent and controlled data release protocols** Agencies will have clear operating models for data release, including for review, verification, and approval for release.	✓			DHDA knows the ABS applies automated and manual data release controls to PLIDA outputs. Information about these controls is provided to Data Custodians and users.
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.			✓	The ABS and DHDA as Commonwealth entities are bound by the *Privacy Act 1988* (Cth) and required to follow the same notifiable data breach reporting procedures as outlined by the Commonwealth Information Commissioner.
Security	**Secure transfer mechanisms**			✓	Not applicable as DHDA data is accessed in secure access environments by PLIDA researchers.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
	Agencies have secure mechanisms for data transfer to prevent breaches.				
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.	✓			The ABS manages access to PLIDA with access restricted to authorised users in secure environments (i.e. ABS DataLab). The ABS only permits access to the DataLab environment once requesters have completed the Responsible Officer and Individual Officer legal undertakings and appropriate training. The ABS review and update access controls with safeguards tailored to data sensitivity. This information is available on the ABS website.
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.	✓			PLIDA data is only accessed in certified ABS secure environments.
Security	**Consistent security labelling and classification** Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.			✓	The ABS and DHDA follow the same Commonwealth standards on security labelling and classification.
Security	**Established security clearance assessments** Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.	✓			The ABS has security clearance and vetting procedures in place, consistent with Australian Government Security Vetting Agency standards.
Security	**Incident monitoring and response mechanisms** Mechanisms for incident monitoring, identification, and response are in place.	✓			The ABS has incident monitoring and response procedures in place, including automated controls and breach response protocols. Real and simulated breaches are managed as part of ongoing risk management. The ABS and DHDA adhere to the same Commonwealth legislative requirements for data breach reporting.

Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Reasoning for alignment with attributes
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 ABS publicly publishes the PLIDA Privacy Statement on how personal information is treated in PLIDA. The ABS and DHDA work together with researchers to ensure data minimisation protocols are in place.
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.	✓			The ABS applies deidentification techniques and implements functional separation (or roles) in all data integration projects. The ABS and DHDA adhere to portfolio and privacy legislation and manage re-identification risks. The ABS publishes information on these controls on their website.
Privacy	**Privacy incident reporting** Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.			✓	The ABS and DHDA will manage and respond to data breaches in accordance with the Commonwealth notifiable data breach conditions from the Information Commissioner.