

Defining ‘trusted entities’ for the purposes of national data sharing

Appendix 6: Use case - New South Wales Department of Communities and Justice

Use case information

Identifying Characteristic	Details
Use case name	NSW Human Services Dataset
Date	09/2025
Data Requester	Multiple
Data Custodian	<p>NSW Department of Communities and Justice with the following data partners:</p> <ul style="list-style-type: none"> • NSW Bureau of Crime Statistics and Research and Youth Justice NSW • NSW Registry of Births Deaths and Marriages • Legal Aid NSW • NSW Police Force • NSW Ministry of Health • NSW Department of Education • NSW Education Standards Authority • Revenue NSW.
Data Characteristics	<p>The Human Services Dataset (HSDS) contains de-identified data collected through the administration of different NSW Government services and some Commonwealth Government supports (i.e. welfare and medical benefits). Data is de-identified and contains information from all NSW residents born on or after 1 January 1990 and their relatives.</p> <p>The current version of the asset is the 2023 HSDS which includes data up to and including 30 June 2023.</p> <p>The list of datasets available within the 2023 HSDS can be found on the HSDS website.</p>
Approved purpose	<p>Approved purposes are contained in the Public Interest Direction and Health Public Interest Direction (PIDs) made by the NSW Privacy Commissioner for the Human Services Dataset Project.</p> <p>Two threshold criteria inform considerations of whether a proposal meets the Approved Purposes:</p> <ol style="list-style-type: none"> 1. Conformance to two guiding principles:

Identifying Characteristic	Details
	<ul style="list-style-type: none"> a) the proposed activity must facilitate or enable the Project Objectives, which is to ensure that effort and funding across government is focussed on interventions that will improve long-term outcomes for Vulnerable Children or Young Persons and their families at the earliest opportunity b) the data will be used to design and deliver better government services for Vulnerable Children or Young Persons and their families. <p>2. Under the overarching rubric of these guiding principles, the data that is collected and used will:</p> <ul style="list-style-type: none"> a) provide specific identifications of trends and gaps in government service usage and delivery; b) facilitate services that are better tailored to the needs of Vulnerable Children or Young Persons and their families both now and in the future; c) deliver clear evidence on service, support and program effectiveness and a detailed view of resource allocation and gaps; d) provide valuable information for research and planning of government supports and services; and e) enable Participating Agencies and other government agencies to meet the Project Objectives by implementing new policy and program development directed to improving outcomes for Vulnerable Children or Young Persons and their families.
Approved timeframe	Ongoing request with annual refresh.
Legal basis for sharing	<p>The creation and use of the Human Services Data set (HSDS) is enabled by the PIDs made for the Human Services Dataset Project by the NSW Privacy Commissioner under s41(1) of the <i>Privacy and Personal Information Protection Act 1998</i> and s62(1) of the <i>Health Records and Information Privacy Act 2002</i> in New South Wales, Australia. This direction was made on 20 December 2024 and will expire on 13 January 2026.</p> <p>The PIDs govern the extent to which the NSW Department of Communities and Justice and participating agencies may depart from the Information Privacy Principles and Health Privacy Principles for the purposes of the Project. This allows government agencies to collect, use and disclose data in ways that would otherwise be precluded by privacy legislation. In the case of the HSDS, the PIDs permit the collection and linkage of administrative datasets across government agencies, so that the data can be re-used to design and deliver better government services for vulnerable children or young persons and their families.</p>
Additional Notes	<p>Access and use of the HSDS is governed by the Department of Communities and Justice according to the following guidelines:</p> <ul style="list-style-type: none"> • The Guidelines for access to and use of the Human Services Dataset (HSDS) • Application forms for accessing the Human Services Dataset (HSDS) • Human Services Dataset application process flow chart <p>The data linkage for this project is performed by the Centre for Health Record Linkage (CheReL) and the dataset is hosted by the NSW Data Analytics Centre within the NSW Department of Customer Service. To protect privacy of individuals, the HSDS can only be accessed by authorised personnel in secure environments for approved projects. The secure environments are available within the NSW Data Analytics Centre (DAC) and ABS DataLab (for data linked with Commonwealth assets).</p>



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	Use case alignment to 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.			✓	Data can only be accessed in the NSW DAC and ABS secure environments. These environments along with governance and privacy procedures are annually audited to ensure compliance with the PIDs made by the NSW Privacy Commissioner. The DAC secure environment is accredited by the ONDC.
Transparency	Public transparency standards The agency will have public-facing processes and/or standards for data release and publication.			✓	Approved Analysts are not required to publish processes. NSW DCJ provides publicly available resources on their website about data collection and use.
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.	✓			Analysts requesting access to data for analytics purposes are required to complete a project proposal which includes provide research methods.
Accountability	Legally supported sharing Data sharing arrangements will be legally authorised and supported by clear documentation such as agreements and data sharing registers.	✓			The project must comply with the PIDs from the NSW Information and Privacy Commissioner and the <i>Data Sharing (Government Sector) Act 2015</i> (NSW) and the public interest directions from the NSW Information and Privacy Commissioner. There are two public interest directions related to this project for the:



Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Use case alignment to attributes
					1) Privacy and Personal Information Protection Act 1998 2) Health Records and Information Privacy Act 2002 Approved Analysts are legally obliged to use the information only for Approved Purposes, adopt best privacy, security and de-identification practices, and keep the information confidential, secure and protected from loss, unauthorised use or disclosure. Approved Analysts are required to sign a legally binding data privacy and confidentiality agreement.
Accountability	Ethical consideration Projects will undergo ethics consideration and where required approval, consent and review processes to ensure alignment with ethical standards.	✓			Projects are required to obtain ethics approvals if undertaking these specific activities: <ul style="list-style-type: none"> Aboriginal Health and Medical Research Council for those disaggregating or using Aboriginal data in analysis (other than describing the sample) NSW Population Health Services Research Ethics Committee for projects accessing the NSW Health data or when they want to link additional datasets to the HSDS DCJ Artificial Intelligence (AI) Ethical Review Board if the project is using AI techniques
Accountability	Defined roles and responsibilities Agencies will have clear data roles and responsibilities to ensure accountability.		✓		The Human Services Data Partnership provides governance over the HSDS in accordance with legislative and the requirements of the PIDs.
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.	✓			To be eligible for approval to access the HSDS, an analyst must: <ul style="list-style-type: none"> demonstrate evidence of technical ability in data or statistical analysis sign a legally binding data privacy and confidentiality agreement confirm that they have read and understood DCJ's data breach policy have a current Working with Children Check



Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Use case alignment to attributes
					<ul style="list-style-type: none"> have a current National Police Check (Criminal Records Check) be willing and available to undertake training on appropriate use of data, and privacy, confidentiality and security obligations <p>Approved Analysts must undertake training before accessing data and undertake privacy verification checks.</p>
Data Management and Governance	<p>Data quality processes</p> <p>Data quality management plans will be implemented to ensure data integrity and compliance.</p>			✓	Data providers are required to check and validate their own data prior to supply. Data providers update their notes each year and are required to supply a data quality statement with each annual refresh of data.
Data Management and Governance	<p>Data governance authorisations</p> <p>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.</p>			✓	Family and Community Services Insights, Analysis and Research and its contracted entities are required to comply with NSW Government policies and frameworks.
Data Management and Governance	<p>Defined metadata management practices with accountable data custodianship roles</p> <p>Agencies will have defined metadata management practices which are accurate, consistent and accessible across the agency. This includes data lineage information.</p>			✓	Data providers maintain the metadata of their assets and the DAC manages metadata for the HSDS .
Data Management and Governance	<p>Consistent and controlled data release protocols</p>		✓		Output checking processes are a combination of data requester and data custodian actions. Analytic output checkpoints must be



Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Use case alignment to attributes
	Agencies will have clear operating models for data release, including for review, verification, and approval for release.				<p>passed prior to external release (including any release to the requesting agency or party) from the secure analytical platform:</p> <ul style="list-style-type: none"> a) All analytical outputs must be aggregated, and where necessary, confidentialised, before it can be taken out of the DAC's Advanced Secure Analytics Lab (ASAL) or ABS DataLab analytic environment. As part of this process, the Approved Analyst must check the outputs to ensure these do not contain any personal information and that individuals cannot be re-identified. b) Aggregated outputs are checked by the DAC and FACSIAR (as the governance lead) to ensure that these outputs do not contain personal information and individuals cannot be re-identified. c) Members of the Human Services Dataset Governance Advisory Committee and Authorised Reviewers from relevant agencies review the aggregated outputs for disclosure and publication risks. d) The Data Custodian's approval may be sought for release of aggregated outputs that relate to significant projects or sensitive topics.
Data Management and Governance	<p>Established escalation and risk management frameworks</p> <p>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.</p>			✓	<p>The NSW Department of Communities and Justice operates a principal department and collaborative shared Audit and Risk Committee in line with the TPP20-08- Internal Audit and Risk Management Policy for the General Government Sector.</p>
Security	<p>Secure transfer mechanisms</p> <p>Agencies have secure mechanisms for data transfer to prevent breaches.</p>			✓	<p>Data is only ever transferred between the Government data partners and CheReL for linkage using CheReL's secure file</p>



Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Use case alignment to attributes
					transfer and data handling processes. CheReL securely transfers this information to: <ul style="list-style-type: none"> the DAC's ASAL – for linked NSW datasets; and ABS DataLab – for data linked with the Commonwealth PLIDA data.
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 HSDS is accessed in a secure access environment, either in the DAC's ASAL or ABS DataLab.
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.			✓	The HSDS is accessed in a secure access environment, either in the DAC's ASAL or ABS DataLab. Both these secure access environments are accredited by the ONDC.
Security	Consistent security labelling and classification Agencies will assign appropriate security classifications for data assets and outputs to guide handling and sharing.			✓	The DAC ensures there is appropriate security labelling and classification of data.
Security	Established security clearance assessments Agencies will consistently use established security clearance/vetting process, e.g. Australian Government Security Vetting Agency.	✓			Approved analysts are required to have a current Working with Children Check and have a current National Police Check (Criminal Records Check).



Theme	Attribute	Strong alignment	Partial alignment	Not assessed	Use case alignment to attributes
Security	Incident monitoring and response mechanisms Mechanisms for incident monitoring, identification, and response are in place.	✓			Under the PIDs, the Chair is obliged to notify the NSW Privacy Commissioner “where any entity involved in the Project collects, uses or discloses Personal Information other than in accordance with this Direction”. DCJ is also required under the Mandatory Notification of Data Breach Scheme to notify the Privacy Commissioner and affected individuals of eligible data breaches (unless a relevant exemption applies).
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 HSDS governance model enforces strict de-identification, access controls, and output vetting. CHeReL links data for approved analysts.
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.	✓			Approved Analysts are required to adopt best practice privacy, security and de-identification practices to minimise disclosure risk, such as the Human Services De-Identification Decision Making Framework and the Five Safes Framework. Approved Analysts are required to apply privacy verification checks to the de-identified, linked unit-level data, including de-identification, aggregation and confidentialisation. Approved Analysts must conduct these checks prior to commencing data analytics, and before the external or public release of any statistical outputs.
Privacy	Privacy incident reporting Agencies will have established processes to report privacy incidents and data breaches and fulfil legislative responsibilities.	✓			HSDS has a data breach policy which contains a copy of the data breach reporting form to be filled out if required.