Privacy and Information Security Statement

For more SA NT DataLink **Security and Privacy Protection** information please refer to: https://www.santdatalink.org.au/security

Privacy Legislation

SA NT DataLink is specifically prescribed as an entity covered by the *Privacy Act 1988 (Cth),* for the purpose of linkage & integrating data.

SA NT DataLink is an authorised Commonwealth Data Integrating Authority, with processes and practices accredited by the Australian Government. The SA Department of Health and Wellbeing (SA Health) staffed Data Linkage Unit at SA NT Datalink, is regulated and complies with the obligations under the *Privacy Act 1988 (Cth)*.

In addition, for the Northern Territory, the use and transfer of government data through SA NT DataLink for linked data activities, is subject to the *Information Act 2003 (NT).*

SA NT DataLink operates as a trusted third party, maintaining individual and community member's privacy and confidentiality. The policies and practices at SA NT DataLink enable government and non-government personal data to be securely controlled in accordance with the Separation Principle, and in doing so, enables privacy protecting data linkage activities for ethically approved health and medical research, in accordance with the *Privacy Act 1988 (Cth).*

For data activities involving South Australian and Local Government, SA NT DataLink is authorised under the Information Privacy Principal exemption approvals granted by the Privacy Committee of South Australia, complying with the *SA Government Cabinet Administrative Instruction 1/89, also known as the Information Privacy Principles (IPPs) instruction, Premier and Cabinet Circular 12.*

SA NT DataLink also complies and operates under the *Public Sector (Data Sharing) Act 2016 (SA)*.

Authorisation of research and analysis

All research studies using SA NT DataLink services must have data custodian permission and be approved by at least one National Health and Medical Research Council (NHMRC) registered Human Research Ethics Committee (HREC). In South Australia projects needing access to SA Government datasets require approval through the SA Department for Health and Wellbeing (SA Health) HREC. All Research Analysts sign deeds of confidentiality and compliance.

NT ethical approval for research is provided through the Menzies School of Health Research (Top End) HREC.

To efficiently link records across multiple data sources, separate approvals are sought for the personally identifying demographic variables from each dataset to be linked and securely stored the Master Linkage File (MLF). The MLF is research data infrastructure, held under very tight security, enabling a persistent and enduring mapping file (similar to the White Pages listing) that promotes re-use and the efficient high-quality extraction of the linked anonymised records being approved for analytical and research use.

Please email question to: santdatalink@unisa.edu.au

Jan 2025

Secure File Transfer Method

Secure encrypted data transfer methods are used by SA NT DataLink. Data files being transferred are encrypted, password protected and manually transferred using the Australian Government approved 'Safe Hands' deliver method or via secure electronic file transfer.

Data Security Protocols

SA NT DataLink's security protocols are in accordance with:

- Australian Government 'Protective Security Policy Framework' (PSPF) and Information Security Manual,
- Population Health Research Network 'Information Governance Framework',
- NHMRC 'Code for Responsible Conduct of Research'.

The SA NT DataLink data security protocols have been developed in association with the Privacy Committee of South Australia and the Northern Territory Information Commissioner, and the Health Consumer Alliance of SA.

Physical Security Measures

An Australian Government 'Protected Level' security classification and information security controls have been applied to ensures the personal data held within the Data Linkage Unit remains secure.

The Data Linkage Unit meets the Australian Government's physical security requirements for an Intruder Resistant Area with separated area with heightened security, secure access controls, CCTV coverage, and strict visitor supervision.

Within the secure 'Protected Area', data linkage activities are performed on a stand-alone IT network. There is no internet access to this network; all USB ports are disabled; and no mobile phones or wireless enabled devices are permitted. The Data Linkage IT equipment is secured in an Australian Govt. Defence Signals Directorate specified 'C-Class Cabinet'.

Separation of Duties and Separation of Content Data

SA NT DataLink's Data Linkage Unit only receives demographic information required to link individuals across multiple datasets. The personally identifying data is completely separate from content or service records. The content data remains held and managed separately under the control of each Data Custodian. With approval, de-identified content data can be provided for the approved use, with Data Custodians replacing their identifying information with privacy protecting linkage keys.

Only Data Linkage Staff in the secure 'Protected Area' have access to the identifying data. All staff are SA Health employees and possess current Working with Children police clearances, undergo security awareness training, and are bound by confidentiality agreements. The staff are subject to the SA Public Sector Code of Ethics, and potentially subject to severe penalties if confidentiality is breached, including jail terms, loss of employment, and loss of employer funded superannuation contributions.