Aus-InSCI Community Survey Project

(Australian Arm of the International Spinal Cord Injury Community Survey Project)

Privacy Policy

De-identified study data were harmonized and centrally stored on a password protected server that adheres to the current standards of data protection and safety at the Swiss Paraplegic Research Centre in Nottwil, Switzerland. A password protected carbon copy of the Australian data were also securely stored on the University of Sydney server after completion of the study. Data stored on University managed research data storage infrastructure in accordance with the University of Sydney Data Management Policy and a Research Data Management.

The participant's privacy will be protected at all times. Paper copies of the retuned completed surveys with no identifying information were to be kept locked in a cabinet at the John Walsh Centre for Rehabilitation Research for 7 years. The survey is anonymous but does contain re-identifiable coded information. Data stored electronically will be entered into a secure database, stored on the central study server (SPR, Switzerland).

The national linkage keys were generated and were to be held by the Population Health Research Network Centre for Data Linkage (PHRN-CDL) for the duration of the project prior to being destroyed. The data can therefore only be re-identified by the PHRN-CDL in conjunction with the partner participating organisation. All data provided were treated confidentially and no identifiable individual information were released in a way that would enable a person to be identified. The method of disposal will comply with relevant policies and contemporary disposal options. The data custodians will be informed in writing when the disposal will commence and is complete.

The PHRN-CDL linkage unit operates within a tight information security framework. The CDL's database and linkage system are held on servers located in a secure, controlled environment at Curtin University, Bentley, Perth. A variety of security controls are implemented; these include access controls, role-based delegations, encryption, firewalls, and physical access restrictions. The security controls are consistent with the PHRN Information Governance Framework and an external security audit has validated the CDL production environment. No data are stored on desktop PCs. Access to servers is via secure VDI available only to staff located in the secure CDL office environment. CDL office environment is secured through swipe card access to authorised personnel only.