The Australian Stroke Clinical Registry (AuSCR) Compliance with the 2014 Australian Privacy Principles

Background to AuSCR

- The AuSCR is an ethically approved clinical quality registry containing patient data collected for the express purpose of contributing to improved patient treatments and outcomes
- The AuSCR is managed by a consortium of organisations that have a key interest in stroke as a public health issue
- The collection, use, disclosure and access to data are all conducted in accordance with legal, ethical and national best practice guidelines

Australian Privacy Principles Requirements	AuSCR compliance
1. Open and transparent management of personal information	• AuSCR approved documents and policies are available on the AuSCR website (www.auscr.com.au) e.g. Patient Information Sheet; Data Security Policy; Data Custodian Policy; Complaints Policy; Data Access Policy; Quality Assurance and Data Management Processes Policy. • The Patient Information Sheet: ○ Outlines what information will be collected and the purpose for which it is collected, held and used. ○ Provides the AuSCR Office and relevant HREC contact details in the event of questions, concerns and complaints about the AuSCR. ○ States that the AuSCR is not permitted to identify patients by law and that, to maintain absolute security and confidentiality, anyone wanting to use any data from the Registry will be required to obtain approval from a Human Research Ethics Committee. • The AuSCR Complaints Policy outlines the procedures for investigating complaints. • The AuSCR Data Custodian Policy addresses data management processes which are based on the appointment of a Data Custodian, who has ultimate responsibility for appropriately collecting and maintaining the AuSCR data, including ensuring privacy and confidentiality. • The Data Security Policy explains the security related to the collection, storage and accessibility of the information in the Registry. • All personal information is kept strictly confidential: all data will be anonymised and aggregated in any presentations or publications and no patients will be identified in reports.
2. **Anonymity and pseudonymity**	• Anonymity and pseudonymity is impracticable for the AuSCR as identification of individuals is required in order to: ○ Make the necessary changes to patients' records e.g. opting-out from the registry; editing erroneous data. ○ Following up patients at 3-6 months post-stroke. • However anonymity is preserved in the way that the data are used e.g. reports, presentations. • Patients can opt-out their personal data at any time, with just an ID code remaining in the system.

Australian Privacy Principles Requirements	AuSCR compliance
3. Collection of solicited personal information	• The AuSCR collects personal information which is directly related to its functions and activities. Patients are provided with a Patient Information Sheet at the time of their stroke. The Patient Information Sheet includes details of the registry and its operations; potential benefits and risks; and, opt-out processes. • The AuSCR has all the appropriate human research ethics and local governance approvals in place including approval of an opt-out process for participation, which is the gold standard for registries. This model presumes that patients will be willing to be included in the AuSCR. Patients are advised that they will be registered in the AuSCR but they are able to remove their personal information from the AuSCR at any time. • Data collection does not occur without prior approvals from Human Research Ethics Committees and hospital research governance. • The Patient Information Sheet is also provided again to those eligible registrants followed up by AuSCR Office three months post-stroke.
4. Dealing with unsolicited personal information	• Not applicable. • Hospital staff can enter only required information into the AuSCR web tool. • AuSCR staff only enter follow-up data provided by the patient or their proxy.
5. Notification of the collection of personal information	• Patients are provided with the Patient Information Sheet which advises them of their inclusion in the AuSCR and outlines the kind of personal information which will be collected. • State-based public hospitals are not subject to the Commonwealth Privacy Act 1988. However, the AuSCR opt-out process facilitates the collection of personal information in an appropriate manner which is consistent and compliant with the need to maintain the confidentiality and security of such information. • The AuSCR Office contact details are provided on the Patient Information Sheet provided by each hospital. • The Patient Information Sheet confirms that there are no consequences for the patient if they choose not to participate in the AuSCR, and that their treatment and long-term care will not be affected by a decision to participate, or not to participate, in the AuSCR. • The Patient Information Sheet is also provided again to those eligible registrants followed up by the AuSCR Office three months post-stroke.

Australian Privacy Principles Requirements	AuSCR compliance
6. Use or disclosure of personal information	• The AuSCR data are summarised to provide information that can inform clinical practice and policy in stroke care. All data reported are de-identified and aggregated. • The AuSCR team is guided by the AuSCR Data Access Policy which outlines how data may be used and supplied. • Any persons wishing to undertake research using AuSCR data need to submit a proposal for review by the AuSCR Research Task Group, as well as having appropriate ethical clearances – a form of peer review which is independent of the AuSCR Management Committee. Data are only supplied to researchers, in approved studies, in a non-identifiable format. • Identifiable data are only used for data linkage or data quality checking processes by authorised staff/entities according to appropriate approvals for data linkage and the AuSCR Quality Assurance and Data Management Processes Policy e.g. ethics approved linkage with the National Death Index by the Australian Institute of Health and Welfare. • The use of data is made explicit in the Patient Information Sheet. • All AuSCR personnel sign a Confidentiality Agreement.
7. Direct marketing	• The AuSCR does not use, or disclose, information for the purpose of direct marketing as requests for the AuSCR data must comply with the National Statement on Ethical Conduct in Human Research. • Further follow-up contact for the purpose of other relevant research projects is only made with the patient if they have consented to being contacted again for this purpose.
8. Cross-border disclosure of personal information	• The AuSCR Data Security Policy states that collection, storage and transfer of AuSCR data will be compliant with amendments (March 2014) to the Commonwealth Privacy Act 1988, including maintaining security of data in relation to cross-border disclosure of personal information. • The AuSCR server and backups are maintained in Australia. No data are held offshore.
9. Adoption, use or disclosure of government related identifiers	• Medicare numbers are collected but would only be used where approved and required.
10. Quality of personal information	• The AuSCR Quality Assurance and Data Management Processes Policy outlines the data verification processes employed by the AuSCR. • Training hospital staff in data entry and use of the AuSCR Data Dictionary takes place before any live data are entered. Site visits and data quality audits of randomly selected medical records are used to verify the accuracy of data collected by the AuSCR. • AuSCR staff conduct quarterly reviews of data completeness and discrepancies, as well as bi-annual requests for ICD-10 discharge diagnosis reports to determine case ascertainment. • Information is provided in annual data quality reports on the quality of the aggregated, de-identified data in the registry e.g. proportion of missing data per field, rates of case ascertainment. • Data quality assurance processes are consistent with the Australian Commission for Safety and Quality in Health Care Standards for Clinical Quality Registries.

Australian Privacy Principles Requirements	AuSCR compliance
11. Security of personal information	• The AuSCR Data Security Policy provides guidelines for all security-related aspects for the registry. ○ AuSCR data are collected via a web tool that requires password access with varying levels of authority. The database itself is protected by Secure Sockets Layer – the highest available level of security. ○ The server is maintained in Australia at the Florey Institute of Neuroscience and Mental Health (AuSCR Data Custodian). ○ Any hard copy data are stored in locked cabinets contained within a building with swipe card access. ○ All AuSCR staff, data analysts and Management Committee members sign a Covenant of Confidentiality whereby they undertake to maintain the confidentiality of any data that they access in the AuSCR. ○ Hospital Users can only access data for their own site. ○ The Patient Information Sheet states that information is stored in a specially designed password protected database which can only be accessed by approved AuSCR staff who sign a Covenant of Confidentiality. ○ Secure methods of data transfer are used between AuSCR office and hospitals.
12. Access to personal information	• The Patient Information Sheet provides details on the demographic and acute stroke information entered into the AuSCR. • Personal details are confirmed at the time of the three month follow-up. • There are cost-free options for registrants to contact us about their data e.g. a free 1800 telephone number which is listed on the Patient Information Sheet and the AuSCR website (www.auscr.com.au).
13. Correction of personal information	• To ensure that any missing or discrepant data are corrected, the AuSCR conducts quarterly data cleaning activities in consultation with the hospital staff. • A systematic data quality audit process is in place. • All inaccurate information is amended by the AuSCR office when it is notified or becomes aware that particular information is incorrect. • Registrants can amend their personal details at the time of the follow-up survey.