AUSTRALIAN STROKE CLINICAL REGISTRY

FACILITATING QUALITY

# AuSCR DATA SECURITY POLICY

Version 4

Approved 11 March 2026

# 1.0 Preamble

This policy document describes the data security measures for the Australian Stroke Clinical Registry (AuSCR) including the collection, use of and access to, data. All these processes are conducted in accordance with legal, ethical and national best practice guidelines. The AuSCR data collection is currently operating within the integrated data management system called the Australian Stroke Data Tool (AuSDaT).

*This document should be read in conjunction with the AuSCR Data Access Policy and the Data Use and Publication Policy, which provide further information on this topic.*

# 2.0 Overview of AuSCR

The AuSCR is a clinical quality registry that contains information, collected from participating hospitals in Australia, about the management of acute stroke or transient ischaemic attack (TIA, no longer collected since May 2023). The information collected in the AuSCR is used to inform efforts to: understand the quality of health care provided in Australia; plan services; and assist with improved treatment and prevention efforts as part of supporting quality improvement efforts. The aggregated data are also used as part of observational studies to describe stroke care and outcomes of patients in Australia.

In brief, a data set of variables including personal information, stroke characteristics and clinical processes of care is collected using a comprehensive, secure data management system called the Australian Stroke Data Tool (AuSDaT). Data entry may be performed manually through the web-based portal or imported automatically from participating hospitals' health administrative systems via a secure Application Programming Interface (API), where this capability is supported. The details of the variables collected in AuSCR are outlined in the National Stroke Data Dictionary (NSDD). The NSDD provides nationally consistent standardised definitions, coding and recording guidance for all data items collected for the AuSCR through the AuSDaT system since implemented on 1st July 2016. The NSDD is available at: https://australianstrokecoalition.org.au/wp-content/uploads/2024/02/AuSDaT-National-Stroke-Data-Dictionary-April-2023.pdf

The initial data collection occurs during the hospital stay, and eligible patients are contacted to complete a patient-reported outcomes survey between 90-180 days post stroke admission. All people on the registry known to be alive are contacted mail and/or SMS.

# 2.0 Security Operating Principles

## 2.1 Secure Data Housing

AuSCR data are stored, managed and are the responsibility of the approved AuSCR Data Custodian. The Data Custodian must adhere to this Data Security Policy and the Data Custodian Policy within the constraints imposed by using common integrated data management system (i.e. AuSDaT), whereby decisions made by the AuSDaT Data Custodian or AuSDaT Coordinating Committee may impact on the AuSCR Data Custodian's capacity to comply until the complementary AuSDaT/AuSCR policies are aligned.

This policy should be read in conjunction with the AuSCR Data Custodian Policy.

Security of data is ensured in the following ways:

Data are housed in an ISO compliant environment which provides at least the minimum level of security required for hosting data that includes personal identifiers. Current server provision is by Amazon Web Services (Australia) based in Sydney. Amazon Web Services is certified compliant with ISO/IEC 27018:2019 (certificate date November 18, 2022 ) and ISO/IEC 27001:2022 (certificate date November 18, 2022).

The server will have an effective firewall and security policies that are regularly reviewed and maintained to ensure adherence to all local and national privacy laws and principles.

Key aspects of secure data storage of the AuSCR data within the AuSDaT system include:

- Robust backup procedure
- Comprehensive disaster recovery protocols, including system redundancy and automated failover to ensure continuity
- Routine validation and penetration testing of data security protocols aligned with industry standards.

## 2.2 Use of the AuSCR by individuals and protection of data

The online integrated data management system in which AuSCR data are collected (AuSDaT) is comprised of secure access controls to ensure that only authorised people are able to retrieve information from the database. Access to the AuSCR data is password and Multi-Factor Authentication (MFA) protected at an individual level, ensuring that an audit trail exists and data can be restored should unauthorised tampering or data corruption occur.

There are six types of user access in the AuSDaT system which is fundamental to the security of the online tool. Four of those user types can be utilised within the AuSCR program, with the other types being associated with AuSDaT operations. Access to AuSDaT system functionalities is governed by user roles, with each user type granted different levels of authority and permissions. All users are provided with a unique username, password and Multi-Factor Authentication (MFA) to ensure secure access at their assigned permission level. User access is provided to Hospital Coordinators by the AuSCR Office by a Program Coordinator. Hospital Coordinators can create local Hospital Data Collectors. This process ensures the ability to audit all users of the online tool. The matrix below, in Table 1, shows the level of user access to the functional elements of the AuSCR online tool.

### Table 1: AuSDaT roles and functionality

| | | AuSDaT Roles | | | | | |
|---|---|---|---|---|---|---|---|
| | | Hospital Data Collector | Hospital Coordinator | Program Coordinator | Follow-up Collector | National Data Manager | National Systems Administrator |
| **Functionality** | Health Service program profile | | ✓ | ✓ | | ✓ | ✓ |
| | Data entry | ✓ | ✓ | ✓ | | ✓ | |
| | Patient data import | | ✓ | ✓ | | ✓ | |
| | Data search | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Live summary results report downloading | ✓ | ✓ | ✓ | | ✓ | ✓ |
| | Data export | | ✓ | ✓ | | ✓ | ✓ |
| | Follow-up data entry | | | ✓ | ✓ | ✓ | |

## 2.3 Secure Transfer and Messaging

All identifiable data not entered directly into the secure web tool, but shared with AuSCR in the form of case ascertainment information, data for linkage projects or data for importing into the AuSDaT system for a program such as AuSCR, are transferred using the secure cloud service provided and maintained by The Florey Information Technology Department. Where this is not possible, all email communications utilising shared identifiable compressed data file should be password protected, with a separate email used to deliver the password details.

When extracted from the AuSDaT, identifiable data (e.g. personal information such as name, addresses) must be stored only on a secure networked, password protected hard drive within an organisation with authority to hold these data and cannot be downloaded onto portable devices such as a USB or personal computer drives.

## 2.4 Security Patches/Fixes

It is the responsibility of the AuSCR Data Custodian to ensure that the AuSCR data management platform operates such that it is protected against any threats which could adversely affect the security of the system, or the data held therein. Amazon Web Services is the current host of the server for the AuSDaT and it is compliant with relevant industry standards.

## 2.5 Ethics and Privacy

It is a requirement of the AuSCR project that appropriate approvals for the collection of data are provided for each hospital prior to participation. This may be granted by a Human Research Ethics Committee (HREC) with local research governance approvals at a site level, by a HREC exemption, or via local quality improvement approval pathways. Approvals must include approval for data to be collected using an opt-out process. An opt-out process presumes that an individual will be willing to be included on the AuSCR unless they expressly withdraw i.e. opt-out.

Contributing hospitals include private sector organisations (e.g. private hospitals) that are regulated by the Commonwealth Privacy Act 1998 and public sector organisations (e.g. public hospitals) that are regulated by state or territory privacy laws regarding the handling of public hospital information.

In addition, collection, storage and transfer of AuSCR data will be compliant with amendments (March 2014) to the Commonwealth Privacy Act 1988 which, amongst other purposes, is aimed at maintaining security of data in relation to cross-border disclosure of personal information i.e. data being sent, or accessible, to overseas parties. Documentation regarding AuSCR's compliance with the 2014 Privacy Principles can be found at: http://www.auscr.com.au/health-professionals/ethics/.

All AuSCR personnel are familiar with, and abide by, the requirements set out in Australian privacy legislation, the National Statement on Ethical Conduct in Human Research and the Australian Code for the Responsible Conduct of Research.

All personnel involved in the AuSCR (employed, volunteer or in-kind) who see, or have access to, identified data from AuSCR records, must sign the Covenant of Confidentiality to ensure their commitment to upholding the confidentiality and privacy of all participants.

## 2.6 Access to Information

All information held in the AuSCR database is confidential and access is restricted by role. The procedures for making a request for aggregated data in a standardised, anonymised report format are outlined in the AuSCR Data Access Policy and the AuSCR Data Use and Publication Policy.

## 2.7 Data Disposal

The AuSCR data collected through AuSDaT will be stored securely and will not be deleted at any point in time. The data management system does allow for individual records to be deleted, in a particular program, and archived according to policies and procedures, but the Statistical Linkage Key (SLK) and data relevant to other programs are retained. Deleted data are not accessible to users with the exception of the AuSDaT National Systems Administrator.

Archived AuSCR data will be secured and maintained separately by the AuSCR Data Manager on a secure server. A copy of de-identified data may be stored on an external secure e-research platform to facilitate access for reuse of data.

In the event that the data custodianship is transferred to another entity/organisation, the data remains the responsibility of the AuSCR Consortium through the data custodial organisation.

The destruction of data stored on digital media must be carried out in such a way as to ensure complete destruction and irreversible of the data. This outcome is achieved by electronically wiping, physically destruction or degaussing, the storage media. Electronic wiping is secure overwriting of data, referred to as disk wiping, which is more reliable than standard deletion or reformatting. Deleting files or reformatting drives does not guarantee removal, as most operating systems simply delete the pointers to data rather than the data itself.

Data stored on magnetic media (e.g. backup tapes) can be securely erased by exposing the media to a strong magnetic field or degaussing. Storage media such as hard drives, USB thumb drive, optical discs (e.g. CDs/DVDs) should be physically destroyed when electronic wiping is not feasible.

The person responsible for data disposal must assess and apply the most effective method based on the type of media and data sensitivity.

Where appropriate, certified third-party contractor may be engaged to carry out secure destruction of the data. All destruction procedures should be compliant with AS/NZS ISO 9001: 2000.

# 3.0 Technical Security Standards

The AuSCR data security standards and principles are outlined in Table 2.

### Table 2: AuSCR Security Standards and Principles

| Security Standard/Principle | |
|---|---|
| Adherence to legislation and national clinical standards for disease registries | Commonwealth of Australia Privacy Act 1988, incorporating the Privacy Amendment (Private Sector) Act 2000: sets out National Privacy Principles applicable to handling of personal information by private sector organisations.<br>Guidelines approved under Section 95A of the Privacy Act 1988 (National Health and Medical Research Council, December 2001) – includes guidelines for research or compilation or analysis of statistics relevant to public health or public safety, for management, funding or monitoring of a health service, and on the role of human research ethics committees.<br>Health Records and Information Privacy Act 2002 (NSW). The Act's provisions are generally consistent with those of the Commonwealth Privacy Act 1988 and apply to organisations operating in New South Wales.<br>National Statement on Ethical Conduct in Human Research (National Health and Medical Research Council, 2023) - guidance on how to fulfil |

| Security Standard/Principle | |
|---|---|
| | broader ethical obligations in the conduct of research, statistical and health service management activities.<br>Operating Principles and Technical Standards for Australian Clinical Quality Registries (Australian Commission for Safety and Quality in Health Care (ACSQHC), 2008, NHMRC Centre for Research Excellence in Patient Safety at Monash University and the National E-Health Transition Authority (NEHTA) - guidelines on establishing and operating a clinical quality registry.<br>Minimum Guidelines for Health Registers for Statistical and Research Purposes (National Health Information Management Group, 2001) – sets out good practice for health registers.<br>Australian Standard: Personal privacy protection in health care information systems (Standards Australia AS 4400 – 1995) |
| Industry Standards | AS/NZS ISO 9001:2015 Quality management systems – Requirements<br>AS/NZS ISO/IEC 27001:2006 Information technology – Security techniques – Information security management systems<br>ISO/IEC 11404 Information technology – General-Purpose Datatypes |
| Passwords | Passwords for user accounts are encrypted using bcrypt which is a key derivation function which derives one or more secret keys from a password, or a passphrase, using a pseudo-random function. Users are required to change their passwords every 4 months. |
| Multi-Factor Authentication (MFA) | The user is required to set up Multi-Factor Authentication (MFA) on their smartphone using an authenticator application, such as Okta, Microsoft Authenticator, or Google Authenticator. |
| Transfer of Data | Encrypted via Transport Layer Security (TLS). |
| Server Solution | Current server provision is by Amazon Web Services (Australia) based in Sydney. Amazon Web Services is certified compliant with ISO/IEC 27018:2019 (certificate date November 18, 2022) and ISO/IEC 27001:2022 (certificate date November 18, 2022). |
| Operating System | A Linux operating system managed entirely by Amazon AWS Cloud services. |
| Disaster recovery and back-up | Provided by Amazon Web Services. See:<br>Disaster Recovery Strategies on AWS |

# Covenant of Confidentiality

All personnel (employed, volunteer or in-kind) who see identified data (e.g. personal information such as name, addresses) from the Australian Stroke Clinical Registry (AuSCR) must sign this declaration.

I declare that it is necessary for me to access identified data held in AuSCR. I will preserve the confidentiality of the information released into my care and will adhere to the AuSCR Data Security Policy, the Commonwealth Privacy Act 1998, and all National Health and Medical Research Council guidelines on research as stated in the National Statement on Ethical Conduct in Human Research 2007 (updated 2023). I will adhere to the AuSCR Publication Policy and understand that I cannot publish or release data during or after my engagement with AuSCR, including release to the media, without written permission from the AuSCR Operational and Quality Improvement Committee.

**Declarant**

| | |
|---|---|
| **Name:** | |
| **Position:** | |
| **Signature:** | **Date:** |

**Witness**

| | |
|---|---|
| **Name:** | |
| **Position:** | |
| **Signature:** | **Date:** |