AuSCR

Australian Stroke Clinical Registry

AuSCR DATA SECURITY POLICY

Version 3

Approved 17th July 2016

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 now 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 and Publication Policies which provide further information on this topic.

1.1 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 and transient ischaemic attack (TIA). 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). This data entry may occur manually, with data entered through the web-based portal, or data may be imported from separate health administrative systems at participating hospitals that have this capability. 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 from the 1st July 2016. The NSDD is available at: http://www.auscr.com.au/

The initial data collection occurs during the hospital stay and eligible patients are followed-up between 90-180 days post-stroke onset. All people on the Registry known to be alive are contacted and asked to complete a follow-up questionnaire which is distributed by mail with subsequent telephone follow-up in the absence of a response to two mail outs.

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 an 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 27018:2014 (certificate date 1 October, 2015) and ISO/IEC 27001:2013 (certificate date November 4, 2014)
- 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
- Aspects of secure data housing fundamental to the storage of the AuSCR data within the AuSDaT system include:
    - Appropriate backup procedure
    - Disaster recovery procedures, including failover and redundancy
    - Regular and adequate testing of all data security procedures in accordance 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 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. Each user type has different levels of authority to access particular system functionality. All users are issued with a unique username and password enabling them the appropriate level of access to the system. User access is provided to Hospital Coordinators by the AuSCR Office by a Program Coordinator. Hospital Coordinators can, and should, manage the further creation of 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 data 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 approval for the collection of data at every hospital is given by a Human Research Ethics Committee (HREC) with local research governance as appropriate. Ethics approval 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 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. Identifiers will be removed once a program has finished with their standard reporting and approved analyses for publications, and archived data can be made available for secondary analysis.

Archived AuSCR data will be secured and maintained separately by the AuSCR Data Manager on a secure server.

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

Destruction of data stored on digital media must be done in such a way as to ensure complete destruction of the data. This outcome is achieved by electronically wiping clean, or physically destroying, the storage media. Deleting electronic data does not always mean that it has been completely destroyed. Most operating systems do not delete the actual data itself, but simply remove pointers to the data. Computer hard disks should be re-formatted. Even more secure is the process of disk wiping. Data stored on magnetic media (such as tapes) can also be erased by subjecting the media to a strong magnetic field or degaussing. Data stored on optical media (such as DVDs) should be physically destroyed. At the time, the person responsible for destroying confidential data needs to ensure that the most effective method is used. Alternatively, an external contractor can be used to securely destroy the data. Destruction 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. *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. *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. *National Statement on Ethical Conduct in Human Research* (National Health and Medical Research Council, 2007) - guidance on how to fulfil broader ethical obligations in the conduct of research, statistical and health service management activities. *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 *Minimum Guidelines for Health Registers for Statistical and Research Purposes* (National Health Information Management Group, 2001) – sets out good practice for health registers. *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* AS/NZS ISO/IEC 27001:2006 *Information technology- Security techniques - Information security management systems* 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,

Security Standard/Principle	
	using a pseudo-random function. Users are required to change their passwords every 4 months.
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 27018:2014 (certificate date 1 October, 2015) and ISO/IEC 27001:2013 (certificate date November 4, 2014)
Operating System	A Linux operating system managed entirely by Amazon AWS Cloud services.
Disaster recovery and back-up	Provided by Amazon Web Services. See: http://d36cz9buwru1tt.cloudfront.net/AWS_Disaster_Recovery.pdf

AuSCR

Australian Stroke Clinical Registry

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 May 2015).* 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 Management Committee.

	DECLARANT	**WITNESS**
NAME		
POSITION		
SIGNATURE		
DATE		
NAME		
POSITION		
SIGNATURE		
DATE		
NAME		
POSITION		
SIGNATURE		
DATE		
NAME		
POSITION		
SIGNATURE		
DATE		
NAME		
POSITION		
SIGNATURE		
DATE		