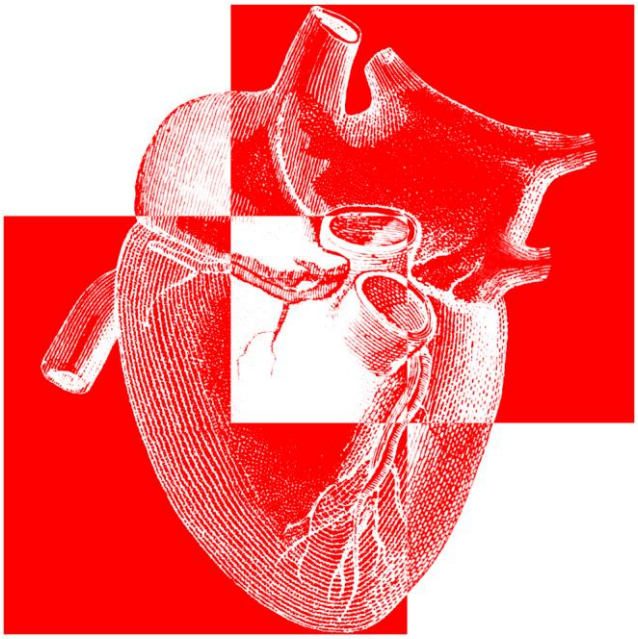
ANZSCTS National Cardiac Surgery Database Program



ANZSCTS National Cardiac Surgery Database Program Privacy Policy

Version 2.0

04 January 2016

Contents

1. Preface

The following policy defines how the Australian and New Zealand Society of Cardiac and Thoracic Surgeons, National Cardiac Surgery Database Program (hereinafter referred to as the ANZSCTS NCSDP) implements and adheres to privacy policies while undertaking registry activities. Monash University is bound by practices and policies which ensure that sensitive information is treated in an open and transparent way and that privacy principles are upheld at all times. The University Privacy Compliance Framework is available at: http://www.privacy.monash.edu.au.

The ANZSCTS NCSDP supports Monash University's commitment to information privacy by ensuring the security, confidentiality and privacy of all information housed within the registry as well as stakeholder information which is external to the registry.
All patient and stakeholder information will be handled in accordance with the Commonwealth Privacy Act (1988) including the Privacy Amendment (Enhancing Privacy Protection) Act 2012 and other state and territory laws and regulations relating to the collection, storage and dissemination of such information. An outline of the privacy act can be found at http://www.oaic.gov.au/privacy/privacy-act/the-privacy-act.

All registry activities have been approved by a Human Research Ethics Committee (HREC) which is recognized by the National Health and Medical Research Council (NHMRC).

2. Project Information

2.1. Purpose of the ANZSCTS NCSDP

The purpose of the ANZSCTS NCSDP is to improve cardiac surgery performance across Australia. Through systematic data collection from participating sites, the ANZSCTS NCSDP aims to provide health services with information that can facilitate quality improvement. The registry will collect key clinical data from individual healthcare encounters that will allow for risk adjustment of outcomes, and enable performance comparisons between surgeons as well as participating sites. Using a nationwide clinical quality registry, a proven method for data analysis, reporting and benchmarking, health services will receive annual reports as well as interim quarterly reports.

2.2. Project Overview

The ANZSCTS NCSDP is managed by the School of Public Health and Preventive Medicine, Monash University. The Program receives funding from The Victorian Department of Health, Queensland Health, the Clinical Excellence Commission (NSW) and individual funding from participating units. The Program has developed and will maintain a secure, online data collection tool and data storage mechanism for analysis and reporting. The ANZSCTS NCSDP will measure the outcomes of cardiac surgeries undertaken at participating sites, while concurrently collecting data on patient demographics, symptoms,

clinical presentation and diagnosis and treatment according to a standard set of data definitions (http://www.ccretherapeutics.org.au/assets/images/ascts-datadefinitionsmanual-v3-aug2009.pdf).

Data will be collected from patients at admission to hospital and again at 30 days post procedure. Sites will submit data to the ANZSCTS NCSDP via one of two methods: (1) direct entry into the ANZSCTS Database via a secure web portal, or (2) data export using a pre-approved template provided by the ANZSCTS NCSDP Management Team. Sites utilising the export method must have a system that has been accredited by the Management Team and utilise the secure file transfer protocol (SFTP) when exporting data. It is recommended that data submission is an ongoing process.

Data will be stored securely within Monash University's servers and retained indefinitely. All data activity will be in accordance with Monash University's Information Technology Services Security Framework Policy, which can be viewed online at: http://www.policy.monash.edu.policy-bank/management/its/it-security-policy.html.

In conjunction with Monash University, the Australian Commission on Safety and Quality in Health Care (ACSQHC) drafted a set of National Operating Principles for Australian Clinical Quality Registries in 2007. The ANZSCTS NCSDP meets these principles at all times when conducting research activities. The operating principles are available at http://www.safetyandquality.gov.au/our-work/information-strategy/clinical-quality-registries/strategic-operating-principles-for-clinical-quality-registries/.

The Australasian Cardiac Surgery Research Institution Limited (ACSRI) governs the ANZSCTS NCSDP, while the database itself is owned by the Australian and New Zealand Society of Cardiac and Thoracic Surgeons. Activities pertaining to the registry are managed by the Centre of Cardiovascular Research and Education in Therapeutics (CCRE-T), within the School of Public Health and Preventive Medicine, Monash University. The direction of the ANZSCTS NCSDP is governed by the ANZSCTS NCSDP Steering Committee who meet at least four times annually to conduct peer review of unit performance and to discuss program activities.

CCRET is responsible for developing and maintaining the data entry system, performing data quality controls, liaising with data managers where appropriate, amending patient data when the data manager does not have the authority to do so and providing feedback to sites regarding their performance.

All hospital data remains the property of that institution. All collective registry data and data management systems will be under the custodianship of Professor Christopher Reid, Monash University.

3. Information and Privacy

3.1. What is personal information?

Personal information can be defined as information or an opinion where an individual's identity is obvious or can be reasonably ascertained, whether true or otherwise.

Sensitive information is a subset of personal information and is subject to a higher level of protection than personal information. It includes information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political organisation, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual preferences or practices, criminal information, health information and genetic information.

Additional information regarding personal and sensitive information is available at: http://www.alrc.gov.au/sites/default/files/pdfs/108_vol1.pdf

3.2. What information is collected in the ANZSCTS NCSDP?

Sensitive and personal information will only be collected if required for essential registry functions. The ANZSCTS NCSDP collects information about patients and their health status before, during and after cardiac surgery. For example:

- Hospital identification number
- Name
- Date of birth
- Contact details (phone number and address)
- Medicare or Department of Veterans Affairs Number
- Surgical risk factors
- Details of the procedure undertaken
- Complications (if any)
- Discharge information
- Mortality data

For the ANZSCTS NCSDP to meet its objectives, it may need to collect personal data from stakeholders, other researchers, hospitals and health services and service providers.

3.3. How is information collected?

Every patient that undergoes a relevant procedure at a participating health service will have their data entered into ANZSCTS Database by a hospital staff member.

A case report form (CRF) is completed for each cardiac procedure and this data is in turn entered directly into either the ANZSCTS Database or the hospital's internal database.

Patients will be followed up by the hospital at 30 days post procedure and if required additional information may be requested from their local doctor.

All patients eligible for recruitment to the ANZSCTS NCSDP receive a Patient Information Sheet (PIS) before they are discharged from hospital. The PIS informs patients about the type of data collected and the purpose for collection. Depending on the urgency of the surgery being performed, patients will receive this form either before or after surgery. As the ANZSCTS NCSDP adopts an opt-off consent model, the PIS also explains the process by which a patient is able to remove their personal information from the database should they wish to do so. In a situation where the patient is unable to make an informed decision regarding the collection of their information (e.g. patients who have an impaired intellectual function) the information will be provided to the next of kin using the ANZSCTS NCSDP Next-of Kin Information Sheet (NOKIS).

When a patient, or their next of kin, decides against participating in the registry, the ANZSCTS NCSDP team will require personal information to be disclosed to ensure that they remove the correct information from the database.

3.3.1. Why collect identifiable, personal information?

It is important that personal information is collected from cardiac patients. This allows hospital staff to link back to patient medical records and follow up on health status post procedure. Furthermore, it enables follow up of patients that have been transferred to another health service and permits linkage activities. For example, the ANZSCTS NCSDP will link with the Australian Institute of Health and Welfare's (AIHW) National Death Index (NDI) to assess long term patient mortality.

It must also be acknowledged that information from the database may be used for research purposes to further improve cardiac surgery performance. Under no circumstances will patient, surgeon or unit identifiers be provided to third parties unless approved by the ANZSCTS NCSDP Steering Committee, however linkage to government databases are an exception. Aggregate data requests are to be submitted using the approved application form and provided to the ANZSCTS NCSDP Research Committee through the ANZSCTS NCSDP Manager. Applications will be considered by the Research Committee at each quarterly meeting and all applications approved by the Research Committee will be ratified by the ANZSCTS NCSDP Steering Committee. The ANZSCTS NCSDP Management Team will supervise all research activities and ensure that researchers undertake regular reporting. Requests for summary data need to be submitted to the ANZSCTS NCSDP Research Committee; however they do not need to be ratified by the Steering Committee.

No research or data linkage activity will occur without approval from an NHMRC approved HREC. Any research undertaken with ANZSCTS data will be bound by the same guidelines and legislation. Please refer to section 3.4.1. below for more information on how patients' privacy will be protected.

3.4. Security of personal information

3.4.1. How will the privacy of patients be protected?

Hospital staff have access to patient records and are primarily responsible for entering patient data online. Following data entry, forms are required to be kept secure in locked storage facilities for a period specified by the residing HREC, after which they are shredded according to the Australian Therapeutic Goods Administration Guidelines.

At CCRET, all tables, queries, forms, reports and macros related to the minimum dataset are locked and password protected, so that only authorised users can view or enter data. The CCRET will give the password to the Data Manager. It is the responsibility of the Data Manager to protect the password and the data on site.

The web interface is housed on an IIS Web Server by the faculty's IT team at Monash University's Clayton site. Data storage will be limited to the Microsoft SQL Server 2008 database which is located in the 'Red Zone' server room in Clayton. Nightly data back-up to an off-site data storage facility ensures that data is retained in the event of a disc failure or fire. The backup facility is encrypted using 2048-bit encryption.

To ensure confidentiality, the web based systems conform to industry best practice by adopting the following measures:

- Restricted user access to ANZSCTS NCSDP members, and an SPHPM programmer only
- Protected data exchange using 2048-bit SSL encryption
- Measures to prevent unauthorised access – maximum attempts, timeout after inactivity, enforced password formats, encrypted passwords
- Validation upon data entry to ensure data quality and prevent unauthorised access
- Audit logging to ensure all data changes are traceable

All information collected is treated as confidential and is protected by privacy legislation. Information disclosure is compliant with the law and only occurs with patient permission. Information is safeguarded by State and Commonwealth privacy laws. No personal information about patients will ever be disclosed in any publication or report.

ANZSCTS NCSDP utilises the SFTP when disseminating patient and surgeon identifiable data to hospital staff. Staff are informed of their responsibility to adhere to hospital policies if they chose to distribute the data. Furthermore, derived variables are not routinely disclosed. Utilising the SFTP ensures that patient privacy and confidentiality is not breached as the system is able to provide file access, transfer and management functionalities over a secure data stream. All SFTP transferred files are available for a limited amount of time and are archived automatically. When sending out correspondence which includes hospital and/or surgeon identifiable information, files are encrypted with a password and the password is provided in a subsequent email.

Access to ANZSCTS data is strictly limited and NCSDP staff must authenticate a user before they are given database access rights. All user accounts are password protected,

have expiration dates and are limited to individuals who have been authorised by relevant delegates (e.g. Principal Investigators or Data Managers). Access to the registry is site specific meaning that users cannot add/view/manage/delete data unless they have specific permissions to do so. If a patient has data across two separate hospitals, each hospital can only see data relevant to its site.

3.4.2. How will ANZSCTS NCSDP information be shared?

The ANZSCTS NCSDP will use aggregate data to produce general reports on cardiac outcomes for public, government, clinical and academic audiences. It is anticipated that these publications will help to inform the community about common trends and/or gaps that may exist in service provision. No publication or report will ever contain any identifying information about patients nor will patients ever be referred to directly.

Researchers who come into the data centre to conduct their analyses can be given access to the complete de-identified dataset. Alternatively, if they choose to conduct their research off site, they can send syntaxes to the ANZSCTS NCSDP Team and be provided with raw output. Researchers who conduct their analyses at the data centre are unable to remove data from the laptop which they are assigned, with ANZSCTS NCSDP staff restricting computer functions.

Sharing of personal information between the ANZSCTS NCSDP and participating hospitals must occur via the SFTP, which is outlined further in section 3.4.1.

The ANZSCTS NCSDP does not share patient identifiable information via email and has procedures in place to ensure that personal information is never transferred onto USBs, portable disks or disk drives. Furthermore, given the confidential nature of the information being collected and stored, appropriate access and data lock of procedures will be established with local IT networks.

4. Access to information

4.1. Accessing information in the ANZSCTS NCSDP

If patients would like access to their medical data, they are advised to obtain this information from the hospital in which they had their procedure.

Patients can notify ANZSCTS NCSDP staff if they believe that their data is inaccurate or incomplete (refer to section 6 for ANZSCTS NCSDP contact details). The Program Manager will take reasonable steps to either correct the information, or discuss alternative action with the patient. The ANZSCTS NCSDP Team will also advise the patient to contact their treating health service to update their records.

5. Addressing concerns

5.1. General concerns

If patients or other stakeholders have any concerns about the ANZSCTS NCSDP they can contact the ANZSCTS NCSDP Manager (refer to section 6 for the Program Manager's contact details).

5.2. Ethical concerns

If patients or other stakeholders have any ethical concerns about this project, participant rights, or would like to make a complaint about the research being conducted, they should contact the approving HREC at the relevant health service.

5.3. Complaints handling

A complaint can be made to any stakeholder, partner organisation, community or individual with whom the ANZSCTS NCSDP has an established relationship, in addition to any member of the public, whether an individual, organisation or entity. The ANZSCTS NCSDP takes privacy and data management responsibilities very seriously and welcomes any feedback on how to protect the rights of participants and improve the quality of its work. Complaints will be handled in a sensitive and timely manner and will protect the rights of those involved.

6. Contacting ANZSCTS NCSDP Team

Patients and other external stakeholders can contact the registry to update their details and/or opt out of participation by contacting the ANZSCTS NCSDP Manager on the details below.

Mail to: Lavinia Tran
Program Manager
ANZSCTS National Cardiac Surgery Database Program
CCRET, School of Public Health and Preventive Medicine
Level 6, The Alfred Centre
99 Commercial Road, Melbourne, VIC 3004

Email: anzscts.sphpm@monash.edu

Patient Hotline: 1800 285 382

Office Telephone: (03) 9903 0518

7. Changes to the ANZSCTS NCSDP Privacy Policy

This policy was approved and ratified by the ANZSCTS NCSDP Steering Committee on Monday 12th January, 2015. ANZSCTS NCSDP reserves the rights to update this policy at any time, as long as it complies with the Privacy Act and other relevant Commonwealth legislation.

Appendix A: Addressing the Australian Privacy Principles

The Privacy Amendment Act 2012 made many significant changes to the Commonwealth Privacy Act 1988 in March, 2014. This includes a set of 13 Australian Privacy Principles (APPs). The APPs are a set of principles that apply to both agencies and organisations, which are in turn classified as APP entities.

These entities replace the Information Privacy Principles (IPP) and the National Privacy Principles (NPP) and are responsible for regulating the handing of personal information by Australian Government agencies as well as private sector organisations.

These principles impose new regulations on organisations and agencies. The key differences between the NPPs and the APPs are detailed via the following link: http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/australian-privacy-principles-and-national-privacy-principles-comparison-guide.

The APPS outline how personal information should be collected, used, disclosed and corrected if incorrect. How the ANZSCTS NCSDP addresses these privacy principles is outlined below.

Permitted Health Situations

Some organisations are exempt from complying with some of the APPs if the situation is considered a 'permitted health situation'. There are five permitted health situations:

- The collection of health information to provide a health service
- The collection of health information for certain research and other purposes
- The use or disclosure of health information for certain research and other purposes
- The use or disclosure of genetic information
- The disclosure of health information for a secondary purpose to a responsible person for an individual

'Health information' is considered a type of sensitive information. The following situations allow the collection, use and/or disclosure of health information and thus are considered permitted health situations:

- Research is relevant to public health and safety
- The compilation or analysis of statistics is relevant to public health or public safety
- The purpose cannot be served by the collection of de-identified data
- It is impractical for the organisation to obtain individual's consent to the collection

Illustrative examples of health situations that are 'relevant to public health and safety' include research or the compilation or analysis of statistics relating to communicable diseases, cancer, heart disease, mental health, injury control and prevention, diabetes and the prevention of childhood disease.

The ANZSCTS NCSDP can be classified as a permitted health situation as the primary purpose of the registry is to improve clinical practice. Furthermore, providing quality healthcare to those with cardiovascular conditions is relevant to public health and safety. The registry requires the collection of identifiable health information to function. It is not practical to obtain consent from every individual undergoing cardiac surgery due to the large number of cases included in the registry (>10,000 annually). To ensure that ethical requirements are fulfilled, the ANZSCTS NCSDP has adopted a HREC approved 'opt-off' approach. This process helps to minimise recruitment bias and ensures that all groups are well represented in analyses, while allowing participants the right to withdraw their data from the registry should they wish.

More information regarding 'permitted health situations' is available via the following link: http://www.oaic.gov.au/images/documents/privacy/applying-privacy-law/app-guidelines/chapter-d-app-guidelines-v1.pdf

APP 1 – Open and transparent management of personal information

The privacy and confidentiality practices of the ANZSCTS NCSDP are outlined in the Monash University Privacy Policy. A copy of the policy can be obtained free of charge from the University's website (http://www.privacy.monash.edu.au)

The ANZSCTS NCSDP is committed to maintaining patient privacy and confidentiality at all times and therefore all patient information will be de-identified in disseminated reports. Patients will be provided with a PIS outlining the purpose of the database, the type of data collected as well as participant rights, including those pertaining to withdrawal of consent.

APP 2 – Anonymity and pseudonymity

The ANZSCTS NCSDP is unable to offer patients anonymity and/or the option of a pseudonym as it would impact on its ability to carry out key functions. According to the ACSQHC, "clinical quality registries need to be able to collect individually identifiable or re-identifiable information in order to:

1. Enable removal of cases upon request by patients who withdraw their consent by opting-off.
2. To allow for important outcome information to be collected at follow-up. This may in some instances require direct contact with the patient and/or linkage with the Commonwealth, State and/or local hospital information systems to determine mortality, rehospitalisation, etc.

3. To assist with data auditing processes (comparing registry data with information held in hospital records) and ensuring that ALL cases have been captured in the registry (to ensure that sites are not 'cherry picking' cases with positive outcomes'.
4. To allow for linkage with administrative datasets and other databases."

APP 3 – Collection of solicited personal information

The ANZSCTS NCSDP is a 'permitted health situation' and as such is exempt from APP 3.

The ANZSCTS NCSDP is classified as a 'permitted health situation' as its primary function is to improve public health through the monitoring and improvement of cardiac surgery in Australia. In addition, it would be unable to carry out key functions (as described above) without collecting identifiable health information.

APP 4 – Dealing with unsolicited personal information

If unsolicited information is received by the ANZSCTS NCSDP, the following will occur:

- ANZSCTS NCSDP staff will determine if the received information is in relation to a routinely collected variable (as per the ANZSCTS NCSDP Data Definitions Manual).
- If yes, the data will be retained and APPs 5 to 13 will apply.
- If no, the information will be deleted, and the sender notified.

APP 5 – Notification of the collection of personal information

All patients eligible for recruitment to the ANZSCTS NCSDP receive a PIS before they are discharged from hospital (following cardiac surgery). The PIS informs patients about the type of data collected and the purpose for collection. As the ANZSCTS NCSDP adopts an opt-off consent model (as qualified by the National Statement on Ethical Conduct in Human Research (2003) Chapter 2.3 — available at: (http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/e72.pdf) the PIS also explains the process by which a patient is able to remove their personal information from the database. The patient is informed that their personal information may be used for linkage to government databases and the contact details of the Program Manager are available so that patients are able to direct their queries and voice concerns.

In a situation where the patient is unable to make an informed decision regarding the collection of their information (e.g. patients who have an impaired intellectual function) the information will be provided to the next of kin using the ANZSCTS NCSDP Next-of Kin Information Sheet (NOKIS).

APP 6 – Use or disclosure of personal information

The ANZSCTS NCSDP will never disclose personal information about an individual for purposes unrelated to the key functions of the database.

APP 7 – Direct marketing

The ANZSCTS NCSDP will never use or disclose personal information about an individual for direct marketing.

APP 8 – Cross-border disclosure of personal information

Data received by the ANZSCTS NCSDP is stored on a secure Monash University server located at the University's Clayton campus. The ANZSCTS NCSDP does not send or store data outside Australia; however this is subject to change, as New Zealand health services may join the registry in the upcoming years.

APP 9 – Adoption, use or disclosure of government related identifiers

The ANZSCTS NCSDP uses its own derived field (Operation ID) as a unique identifier. Operation ID is automated by the ANZSCTS Database upon submission of the data. Therefore, whilst Government identifiers are collected (Medicare number, Department of Veteran Affairs number) they are not adopted by the database as a unique identifier.

The ANZSCTS NCSDP will not disclose government identifiers to third parties unless it is for the purposes of an approved linkage with databases such as the NDI operated through the AIHW.

APP 10 – Quality of a person's health information

The ANZSCTS NCSDP is able to ensure the accuracy and quality of its data by performing data audits. As recommended by the ACSQHC, all sites participating in the database are audited every three years (approximately). The auditing procedure determines adequate case ascertainment (all eligible cases must be entered to prevent sites from 'cherry picking' cases with favourable outcomes) and suitable data integrity. The results of the audit are reviewed by the Steering Committee and feedback is provided to the site to promote improved performance. Furthermore, individuals are encouraged to contact the ANZSCTS NCSDP is they believe that their health information is not recorded accurately.

APP 11 – Security of personal information

The CCRET at the School of Public Health and Preventive Medicine is one of the few medical research establishments in Australia with extensive experience in the management of large database and the storage of identifiable information.

The ANZSCTS NCSDP ensures that the use of identifiers is in accordance with the Therapeutic Goods Administration's guidelines for Good Clinical Practice and Privacy Principals in all relevant Privacy Legislation (http://www.tga.gov.au/sites/default/files/ich13595an.pdf).

The web interface itself is housed on an IIS Web Server by the faculty's IT team at the Monash Clayton site. Data storage will be limited to the Microsoft SQL Server 2008 database located in the Monash Clayton campus secure (Red Zone) server room and to access controlled Monash University drives. All traffic between the data collector's browser webserver and the database server are encrypted with 2048-bit encryption.

All systems access will be logged to an individual's user account and IT staff will have the capacity to monitor logs for inappropriate access.

In the case of fire or loss of data, the database server is mirrored each day to a backup facility (which is also encrypted as above).

Following data entry, case report forms will be housed in locked filing cabinets and filed according to Record Number. The Data Manager will hold the keys for the filing units.

APP 12 – Access to personal information

If patients would like access to their medical data, they are advised to obtain this information from the hospital in which they had their procedure.

APP 13 – Correction of personal information

The ANZSCTS NCSDP takes reasonable steps to ensure that the personal information which it holds is accurate, complete and up-to-date, relevant and not misleading having regard to the purpose for which it is held.
If a patient wishes to correct data held by the ANZSCTS NCSDP, they will be advised to contact the Program Manager. The Program Manager will take reasonable steps to either correct this information, or, if necessary discuss alternative action with the patient.