AUSTRALIAN AND NEW ZEALAND COLLABORATIVE PERFUSION REGISTRY
Privacy and Security Policy

1.1. Preface

The following policy defines how the Australian and New Zealand Collaborative Perfusion Registry (hereinafter referred to as the ANZCPR) implements and adheres to privacy and information security policies while undertaking registry activities. Flinders Medical Centre 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 Flinders Medical Centre is part of the Southern Adelaide Local Health Network (SALHN), and the Privacy and Security Compliance Framework is found in the SALHN Information Communication Technology (ICT) policy directives. These security policies are based on the South Australian Government Information Security Management Framework (ISMF) and the SA Government Protective Security Management Framework; which are available at: http://dpc.sa.gov.au/policies-standards-and-guidelines#Security.

The ANZCPR supports SALHN'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 https://www.oaic.gov.au/privacy-law/privacy-act/.

All registry activities have been approved by the Southern Adelaide Clinical Human Research Ethics Committee (SAC HREC) which is recognised by the National Health and Medical Research Council (NHMRC).

1.2. Project Information

1.2.1. Purpose of ANZCPR

The purpose of the ANZCPR is to collect and report data relevant to the practice of cardiopulmonary bypass. This is achieved through utilisation of the data to understand clinical practice, provide a foundation for research, and to facilitate quality improvement.

This is achieved through the maintenance of a prospective data set on cardiac surgical procedures performed in multiple sites throughout Australia and New Zealand and through the collaborative network of perfusion and interested researchers, who share the commitment to cooperation and collaboration in the pursuit of excellence in perfusion.

The ANZCPR aims to improve patient outcomes through its ability to provide research infrastructure and support to the Australian and New Zealand perfusion community, and by its ability to produce relevant and timely research publications.

1.2.2. Project Overview

The ANZCPR is managed by the Cardiac Surgery Research and Perfusion Department of Flinders Medical Centre. The Program has developed and will maintain a secure, online data collection tool and data storage mechanism for analysis and reporting. The ANZCPR will measure the outcomes of cardiac surgeries undertaken at participating sites, while concurrently collecting data on patient demographics, symptoms, clinical presentation, and diagnosis, procedure and perfusion information and treatment according to a standard set of data definitions (see ANZCPR Data Definitions).

Data is collected from patients at admission to hospital, throughout their hospital stay and again at 30 days post procedure. Sites will submit data to the ANZCPR via data export using a pre-approved template provided by the ANZCPR Project Manager. Sites utilising the export method must have a system that has been accredited by the ANZCPR Steering Committee and utilise the secure file transfer protocol (SFTP) when exporting data. It is recommended that data submission is an ongoing process.

Data is stored securely within Flinders Medical Centre's servers and retained indefinitely. All data activity is in accordance with SALHN Information Communication Technology Services Security Framework Policy.

The ANZCPR meets the Australian Commission on Safety and Quality in Health Care (ACSQHC) National Operating Principles for Australian Clinical Quality Registries at all times when conducting research activities.

The operating principles are available at: http://www.safetyandquality.gov.au/our-work/information-strategy/clinical-quality-%20%20registries/strategic-operating-principles-for-clinical-quality-registries/.

The ANZCPR Steering Committee governs the ANZCPR, while the database itself is owned by the ANZCPR Data Management Team. Activities pertaining to the registry are managed by the Flinders Medical Centre Cardiac Surgery Research and Perfusion Department, within the Cardiac and Thoracic Surgery Unit of Flinders Medical Centre. The direction of the ANZCPR is governed by the ANZCPR Steering Committee who meet at least annually to conduct peer review of unit performance and to discuss program activities.

The Cardiac Surgery Research and Perfusion Department, FMC 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 Associate Professor Robert Baker, Flinders Medical Centre.

1.3. Information and Privacy

1.3.1. 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

1.3.2. What information is collected in the ANZCPR?

Sensitive and personal information is de-identified prior to being transferred to the ANZCPR.

The ANZCPR collects information about patients and their health status before, during and after cardiac surgery. For example:

- Age
- Date of birth
- Ethnicity
- Height and Weight
- Surgical risk factors
- Details of the procedure undertaken
- Complications (if any)
- Discharge information
- Mortality data

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

1.3.3. How is information collected?

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

A case report form (CRF) is completed for each cardiac procedure and this data is in turn entered into a hospital internal database. Any identifying information is then removed, and the data is given a unique identifying number before being exported to the ANZCPR.

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 ANZCPR 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 ANZCPR adopts an opt-out 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 ANZCPR Next-of Kin Information Sheet (NOKIS).

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

1.3.4. Why collect identifiable, personal information?

It is important that personal information is collected from cardiac patients at each hospital. This allows hospital staff to link back to patient medical records and follow up on health status post procedure. However this personal information does not leave the hospital. All data exported to the ANZCPR has no personal identifiers attached, each record has been de-identified and a unique number has been given to the data prior to being exported.

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. Aggregate data requests are to be submitted using the ANZCPR Data Access Request Form and provided to the ANZCPR Steering Committee through the ANZCPR Project Manager and are subject to the ANZCPR data Access and Publication Policy. Applications will be considered by the Steering Committee at either the annual meeting, or on an ad hoc basis as required. The ANZCPR Steering Committee will supervise all research activities and ensure that researchers undertake regular reporting. Requests for summary data need to be submitted to the ANZCPR Steering Committee.

No research or data linkage activity will occur without approval from an NHMRC approved HREC. Any research undertaken with ANZCPR data will be bound by the same guidelines and legislation. Please refer to section 1.4.1., below, for more information on how patients' privacy will be protected.

1.4. **Security of personal information**

1.4.1. How will the privacy of patients be protected?

Hospital staff has access to patient records and are primarily responsible for entering patient data online.

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

The ANZCPR server is part of the Flinders Medical Centre (FMC) health network, and thus governed and secured by Southern Adelaide Local Health Network Information Communication Technology policies and procedures. These security policies are based on the South Australian Government Information Security Management Framework (ISMF) and the SA Government Protective Security Management Framework.

Data storage will be limited to the Microsoft SQL Server 2008 database which is located in Flinders Medical Centre with a back-up server in eHealth systems, SA and managed by its policies and procedures.

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.

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

- Restricted user access to ANZCPR members and a programmer only
- Measures to prevent unauthorised access such as enforced password formats
- 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.

ANZCPR utilises a secure website to transfer de-identified data.

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

1.4.2. How will ANZCPR information be shared?

The ANZCPR 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 request data to conduct their analyses can be given access to the complete de-identified dataset.

The ANZCPR does not have access to any patient identifiable information. Each patient receives an ID Number and all identifiers are removed.

1.5. Access to information

1.5.1. Accessing information in the ANZCPR

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.

1.6. Addressing concerns

1.6.1. General concerns

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

1.6.2. 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.

1.6.3. Complaints handling

A complaint can be made to any stakeholder, partner organisation, community or individual with whom the ANZCPR has an established relationship, in addition to any member of the public, whether an individual, organisation or entity. The ANZCPR 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.

2. Security

2.1. Security goals

The Australian and New Zealand Collaborative Perfusion Registry (ANZCPR) is committed to safeguard the confidentiality, integrity and availability of all electronic information of the registry to ensure that regulatory and operational requirements are fulfilled.

The overall goals for information security at ANZCPR are the following:

- To prevent unauthorised physical access, damage, and interference to the ANZCPR's premises and information.
- To prevent loss, damage, theft or compromise of assets and interruption to the ANZCPR's activities.
- To ensure the correct and secure operation of information processing facilities.
- To minimise the risk of systems failures.
- To maintain the integrity and availability of information and information processing facilities.
- Ensure compliance with current laws, regulations and guidelines.
- To ensure the protection of information in networks and the protection of the supporting infrastructure.
- To maintain the security of information and software exchanged within an institution and with any external entity.
- To detect unauthorised information processing activities.
- To ensure authorised user access and to prevent unauthorised access to ANZCPR information systems.
- To prevent unauthorised access to information held in application systems.
- To prevent errors, loss, unauthorised modification or misuse of information in applications.
- To protect the confidentiality, authenticity or integrity of information by cryptographic means.
- To ensure the security of system files.
- To maintain the security of the ANZCPR application system software and information and to reduce risks resulting from exploitation of published technical vulnerabilities.
- To maximise the effectiveness of and to minimise interference to, or from the information systems audit process.

2.2. Security strategy

ANZCPR's current strategy and framework for risk management are the guidelines for identifying, assessing, evaluating and controlling information related risks through establishing and maintaining the information security policy (this document).

ANZCPR shall ensure the availability of continuity plans, backup procedures, defence against damaging code and malicious activities, system and information access control, incident management and reporting.

The term information security is related to the following basic concepts:

- ***Confidentiality:*** Information is not made available or disclosed to unauthorised individuals, entities, or processes.
- ***Integrity:*** Safeguarding the accuracy and completeness of data collected.
- ***Availability:*** Being accessible and usable upon demand by an authorised entity.

Every user of ANZCPR's information systems shall comply with this information security policy. Violation of this policy and of relevant security requirements will therefore constitute a breach of trust between the user and the ANZCPR, and may have consequences for continuation in contributing to the ANZCPR.

2.3. **Scope**

Facilities include, and are not limited to the following, as well as the physical and environmental infrastructure such as:

- computer processors of all sizes, whether general or special purpose, and including personal computers
- special purpose devices connected to the SA Health data network, such as biomedical equipment, clinical equipment, paging systems and engineering control systems
- peripheral, workstation and terminal equipment
- laptop computers, personal digital assistants (PDAs) and other mobile computing equipment
- telecommunications and data communications rooms, closets, cabling and equipment
- local and wide area network equipment
- environmental control systems, including air-conditioning and other cooling equipment, alarms, fire suppression and other safety equipment
- required utility services, including electricity, emergency generators, un-interruptible power supplies, water supply
- buildings and building improvements accommodating information technology equipment

Information includes both raw and processed data such as:

- electronic data files, regardless of their storage media or format, and including hard copies and data otherwise in transit
- information derived from processed data, regardless of storage or presentation media.

Software includes any software administered, in-house developed programs and those acquired from external sources such as:

- operating system software and associated utility and support programs
- application enabling software, including data base management, telecommunications and networking software
- application software and the processing functions it provides.

Security Incidents include, and not limited to, the following:

- actual or attempted unauthorised access to, use of, or copying of data or information, regardless of its form (electronic, hard-copy, voice etc)
- actual or attempted unauthorised changes to, or destruction or erasure of information
- actual or attempted unauthorised access to premises or facilities
- fraudulent use or misuse of data, information or ICT assets for financial or other advantage, or causing detriment to another
- theft of hardware or software
- virus or worm intrusion (or similar)
- software malfunctions, including and not limited to, incorrect processing of data affecting its integrity, incorrect display of information affecting its confidentiality, incorrect application of access controls or ability to bypass access controls
- any other violation of SA Health security policies and supporting documentation

Threat Management includes, and not limited to, the following:

- software viruses, worms, trojans and other forms of malicious software
- operating systems and application software vulnerabilities that can be exploited by malicious software.

3. Security Domain Compliance Recommendations

3.1. Physical Security

The ANZCPR server and networking equipment is located in a lockable area and not accessible by unauthorised people. Any obsolete Information Communication Technology assets that have held ANZCPR data are disposed of securely.

The ANZCPR server is part of the Flinders Medical Centre (FMC) health network, and thus governed and secured by Southern Adelaide Local Health Network Information Communication Technology policies and procedures. These security policies are based on the South Australian Government Information Security Management Framework (ISMF) and the SA Government Protective Security Management Framework.

Offices, rooms and data entry/processing facilities are secured with physical entry controls. Public access points are isolated and controlled.

3.2. Communications and Operations Management

The ANZCPR server is secured as part of eHealth and is therefore governed by SALHN ICT Security Policies procedures.

Operational procedures are documented.

Formal change management procedures are documented as part of the ANZCPR Clinical Registry Data Access and Publication Policy and all stakeholders provide authorisation before a change is made.

ANZCPR Development, test and production networks environments are separated, password protected and only used by the ANZCPR Project Manager, and CTSU IT Database Programmer.

Capacity of the ANZCPR infrastructure (e.g. network bandwidth) and system components (disk space, memory) are monitored and upgraded as required.

Antivirus software is installed on all servers, PC's and mobile devices and updates are installed as soon as possible via institution networks and following institution policies and procedures.

Outbreaks of malicious software are dealt with through institution network policies and procedures.

All ANZCPR Data is backed up to a reliable media on a daily basis and stored at a location separate to the primary site.

The ANZCPR Project Manager has been designated as the network manager to oversee the FMC CTSU IT Database Programmer and has responsibility for controlling the ANZCPR network.

Data transfer agreements for the ANZCPR are documented in the ANZCPR Clinical Registry Data Access and Publication Policy and through the ANZCPR Data Transfer Guidelines. All external data transfers to the ANZCPR are currently de-identified.

The use of removable media is prohibited, and data access is documented in the ANZCPR Clinical Registry Data Access and Publication Policy.

Formal procedures have been developed and are being followed for information handling as outlined in the ANZCPR Clinical Registry Data Access and Publication Policy.

The process to publish information electronically is documented, well understood and requires specific controls including approval.

An audit log management process is documented and enforced.

Logs are secured and unable to be altered.

A common and automatic time source is used for systems.

3.3. Access Control

The Australian and New Zealand Collaborative Perfusion Registry (ANZCPR) user role and the information within the ANZCPR that can be accessed by each user is provided in the ANZCPR Users Guide.

ANZCPR users are registered through the Project Manager.

Administrators and internal Database users are identified at the point of registration.

If not known to the ANZCPR, any external administrators are required to show photo identification.

Site users can only view information that they enter into the ANZCPR, and not information from other parties.

Users Responsibilities can be found in the ANZCPR Users Guide which is enforced and compliance is checked annually.

All users have unique identifiers.

Passwords are enforced as a combination of letters and numbers.

3.4. Information Systems Development and Maintenance

Requirements for ANZCPR security controls are assessed for all new systems.

The ANZCPR data entry is validated by the application.

Application processing routinely validates specific information.

ANZCPR testing data is selected carefully and not identifiable.

Application source code access is controlled.

Any changes to ANZCPR system is managed through formal, documented change management procedures.

Any changes or updates to systems are tested before implementing into the live environment.

There is documentation for staff explaining how to identify and report suspected security events or weaknesses.

Formal security incident management procedures are developed, enforced and reviewed regularly.

3.5. Business Continuity Management

As the ANZCPR is part of the Flinders Medical Centre (FMC) health network, and thus governed and secured by Southern Adelaide Local Health Network, Information Communication Technology policies and procedures are in place to ensure business continuity. IT Disaster Recovery plans are in place to ensure prioritisation for recovery.

All plans and processes are tested and updated annually as per the South Australian Government Information Security Management Framework (ISMF) and the SA Government Protective Security Management Framework.

All other institutions are governed by local health network guidelines and policies.

4. Ownership

4.1. Owner of the security policy

The ANZCPR Steering Committee is the owner of the security policy (this document). Any policy changes must be approved and signed by the ANZCPR Steering Committee.

4.2. Registry owner

The ANZCPR Steering Committee is the owner of the ANZCPR. The ANZCPR Steering Committee, in consultation with the IT department, is responsible for the development and maintenance of information and related information systems. The ANZCPR Steering Committee has defined which users or user groups are allowed access to the information and what authorised use of this information consists of. The ANZCPR Steering Committee responsibilities are defined in the ANZCPR Steering Committee Guidelines.

4.3. System administrator

The ANZCPR Project Manager is the administrator for the ANZCPR information systems and the information entrusted to the ANZCPR by other parties. The ANZCPR Project Manager, along with the FMC CTSU IT Manager, is responsible for protecting the information, and has implemented systems for access control to safeguard

confidentiality and has ensured all backup procedures are performed so as to ensure that critical information is not lost. The ANZCPR Project Manager implements, runs and maintains the security system in accordance with this Privacy and Security policy.

4.4. Users

ANZCPR data managers are responsible for getting acquainted and complying with this security policy and local site IT regulations. Questions regarding the administration of various types of information are posed to the ANZCPR Steering Committee or the ANZCPR Project Manager.

5. Information security policy

The ANZCPR Steering Committee ensures that this ANZCPR Privacy and Security, as well as guidelines and standards, are utilised and acted upon.

The ANZCPR Steering Committee ensures that sufficient training and information material are made available for all users, in order to enable the users to protect ANZCPR's data and information systems.

This Privacy and Security policy is reviewed and updated annually or when necessary, in accordance with principles described in ISO/IEC 27001.

All important changes to ANZCPR's activities, and any other external changes related to the threat level, will result in a revision of this policy.

5.1. Access control/Authorisation

Access to ANZCPR is only authorised by the ANZCPR Steering Committee. This includes access rights, including accompanying privileges.

5.2. Security of system files

Any changes to the ANZCPR comply with existing routines.

The implementation of changes to the production environment is controlled by formal procedures for change management, in order to minimise the risk of damaged information or information systems.

5.3. Security in development and maintenance

System development must satisfy definite security requirements and be reviewed by the Steering Committee prior to changes taking place, including data verification and securing the code before being put in production.

All software is thoroughly tested and formally accepted by the ANZCPR Steering Committee and the FMC CTSU IT Administrator prior to being transferred to the production environment.

6. Contact Information

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

ANZCPR Project Manager: Mr Richard Newland

Cardiac Surgery Research and Perfusion
Level 6, Flinders Medical Centre
Flinders Drive
Bedford Park SA 5042

Email: Richard.Newland@sa.gov.au
Phone: 08 8204 5382

Changes to the ANZCPR Privacy and Security Policy

This policy was approved and ratified by the ANZCPR Steering Committee on …….. February 2016.

ANZCPR 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 ANZCPR 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 ANZCPR 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. To ensure that ethical requirements are fulfilled, the ANZCPR has adopted a HREC approved 'opt-out' 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: https://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 ANZCPR are outlined in this Privacy and Security Policy.

The ANZCPR 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 Patient Information Sheet (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 ANZCPR 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.

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'.

To allow for linkage with administrative datasets and other databases."

APP 3 – Collection of solicited personal information

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

The ANZCPR 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 ANZCPR, the following will occur:

- ANZCPR staff will determine if the received information is in relation to a routinely collected variable (as per the ANZCPR 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 ANZCPR receive a PIS before they are discharged from

hospital (prior to or following cardiac surgery). The PIS informs patients about the type of data collected and the purpose for collection. As the ANZCPR adopts an opt-out 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 ANZCPR Next-of Kin Information Sheet (NOKIS).

APP 6 – Use or disclosure of personal information

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

APP 7 – Direct marketing

The ANZCPR 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 ANZCPR is stored on a secure Flinders Medical Centre server located at the SALHN Institution. The ANZCPR does not send or store data outside Australia.

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

The ANZCPR uses its own derived field (Procedure ID) as a unique identifier. Procedure ID is automated by the ANZCPR upon submission of the data. Therefore, whilst Government identifiers are collected at site (i.e., Medicare number) they are never adopted by the database as a unique identifier – all identifiers are removed prior to sending the information from the contributing institution to the ANZCPR.

The ANZCPR cannot disclose government identifiers to third parties.

APP 10 – Quality of a person's health information

The ANZCPR 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 ANZCPR is they believe that their health information is not recorded accurately.

APP 11 – Security of personal information

The ANZCPR 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).

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.

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 ANZCPR 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 ANZCPR, 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.