ACOR Ltd
Cardiac Procedures Registry

Privacy and Confidentiality Policy

Policy Number: **005**
Policy Title: Privacy and Confidentiality
Policy Sponsor: ACOR
Developed by: Cardiac Procedures Registry Project Manager
Version Number: **2.0**
Version Date: **15 Oct 2015**
Effective Date: **01 Nov 2015**
Review Date: **01 Nov 2016**

Policy Version Control

Version	Date	Author	Change Description
1	01 Jun 2014	Erin Morton	Document created
1.1	20 Mar 2015	Lauren Bell	For finalisation
1.2	23 Jun 2015	Lauren Bell	Change of corporate logo
2.0	15 Oct 2015	Erin Morton	Update of Privacy Act references, incorporation of Steering Committee feedback

1. Rationale and Purpose

Australasian Cardiac Outcomes Registry Limited (ACOR) recognises the need to improve the standards of patient cardiac care in Australia and New Zealand. The Cardiac Procedures Registry (CPR) Policy provides the framework to develop and establish the Registry to collect and report on standardised information from all patients undergoing specific cardiac procedures and therapies within hospitals in Australia and New Zealand.

This policy defines the various measures and overall approach implemented to ensure the privacy and confidentiality of sensitive information associated with the Registry is both established and maintained.

2. Definitions

The following definitions shall apply for the purposes of this policy unless otherwise stated:

ACOR	Australasian Cardiac Outcomes Registry Limited and its designees
CSANZ	Cardiac Society of Australia and New Zealand
HREC	Human Research Ethics Committee
IT	Information Technology
Operator	entity providing the administration and operation of the Registry and all associated services detailed in the Specifications of the ACOR-Operator agreement.
Registry	Cardiac Procedures Registry (CPR)

3. Privacy and Confidentiality

The CPR requires collection of certain patient identifying information, and is composed of sensitive information; from individual patients, clinicians, and hospital sites. It is imperative that the privacy and confidentiality of its data is protected. The Operator is the custodian of the data and observes all laws in relation to privacy and confidentiality of the data.

3.1 Privacy and Confidentiality

3.1.1 The Operator and ACOR comply with the relevant Commonwealth, State and Territory legislation and regulations, specifically with the *Privacy Act (1988) (*'the Privacy Act'*),* the Privacy Amendment (Enhancing Privacy Protection) Act 2012, the Privacy Regulation 2013, including the 13 Australian Privacy Principles (APPs), as if the Operator were an agency under the Privacy Act.

3.1.2 ACOR and the Operator act in accordance with the Operating Principles and Technical Standards for Australian Clinical Quality Registries Guidelines, and are guided by Human Research Ethics Committee review. HREC is responsible for resolution of any potential privacy complaints by individuals.

3.1.3 All Registry personnel abide by ACOR Policies and Standard Operating Procedures, reasonable ACOR and Operator directives, and current and relevant privacy legislation and regulation including the "National Statement on Ethical Conduct in Human Research" and the "Australian Code for Responsible Conduct of Research" in addition to the above.

3.1.4 Confidential information is defined as information designated as confidential by the Discloser or which should by its nature reasonably be considered to be confidential information and may be provided in writing, electronically, verbally or otherwise. It does not include any information proven to be in the public domain or known by the Recipient at the time of disclosure, other than through a breach of contractual agreement.

3.1.5 All Registry personnel must take measures to keep confidential and not disclose to any person any Confidential Information regarding the Registry except as authorised or required by law, as per the terms of contractual agreement with ACOR.

3.1.6 Privacy and confidentiality measures affecting all types of Registry data handling including input, access, output, and also database linkage are taken. Education and training are provided to all staff as appropriate.

3.1.7 Any private and confidential information provided to or from the Registry, in uploaded or downloaded documentation, will be provided via a Secure Report Depot. Use of the Secure Report Depot will ensure all documents are encrypted in transfer and at storage. Valid log-

in credentials are required and user access can only be authorised by SAHMRI. Audit logs are tracked against each user and specific documents can be assigned as view only and locked to download.

3.2 Data Input

3.2.1 Data is entered and saved into the Registry by site staff at a level that includes patient identifying information and other confidential information.

3.2.2 Data collected is limited to that specified by Registry protocol and approved by HREC unless mandated through legislation, enabled through regulation or legislation, or within the scope of an institution's quality assurance activity.

3.2.3 If an Opt-Out Approach form has been completed by an individual, only information mandated through legislation, enabled through regulation or legislation, or within the scope of an institution's quality assurance activity may be collected.

3.2.4 All entries are inputted as accurately and completely as possible to enable potential cross-referencing between individuals (whether patients or clinicians) either at a database level or beyond.

3.2.5 All measures and responsibilities are taken by site staff and the Registry or subcontractors as appropriate to maintain the privacy and confidentiality of raw "source" data in addition to database entries. All confidential electronic documentation is provided through the Secure Report Depot.

3.3 Database Access

3.3.1 Access to retrieve Registry information from the database is restricted to authorised persons only.

3.3.2 Retrievable data for an individual is determined by the role of the person seeking access.

3.3.3 Data entry staff have full access to patient identifiers to enable additions to or editing of a patient's database file. Access for all other personnel is automatically restricted to de-identified data.

3.3.4 De-identified data can be accessed in identifiable or re-identifiable format upon approval of request justification by ACOR and relevant HREC as appropriate.

3.3.5 All measures and responsibilities are taken by recipient staff to maintain the privacy and confidentiality of retrieved data. All confidential electronic documentation is provided through the Secure Report Depot.

3.4 Data Output

3.4.1 Access to Registry report outputs is restricted to authorised persons only.

3.4.2 Each automated Registry report (eg. to sites and to ACOR) is set-up with a specified level of database detail dependent on the report client and as prescribed by the Operator and corroborated by ACOR.

3.4.3 Data collected for the Registry must not be used for any purpose other than that of the Registry.

3.4.4 The level of detail included in any customised reports as requested by individuals is limited by the role of the person requesting the report and as specified by the Operator and corroborated by ACOR.

3.4.5 De-identified data is provided in identifiable or re-identifiable format upon approval of request justification by ACOR and relevant HREC as appropriate.

3.4.6 All measures and responsibilities are taken by recipient staff to maintain the privacy and confidentiality of report data. All confidential electronic documentation is provided through the Secure Report Depot.

3.5 Data Linkage

3.5.1 Linkage of patient data within the Registry and with other databases including disease, procedure and outcome registries, enhance Registry value but the capacity requires usage of individually identifiable data. Where possible this is via use of national Individual Healthcare Identifiers (eg. Medicare number), and again all measures and responsibilities are taken by relevant staff to maintain the privacy and confidentiality of such data.

4. Scope

This policy applies to all aspects of the Registry and groups or individuals that will utilise it including the CPR Steering Committee, nominated working groups, Registry Operator Team, and all data users and report clients.

5. Responsibilities

Super-user

- All Operator or sub-contractor staff responsible for or working on IT security components including Registry operating system will ensure Registry information is restricted to authorised persons only.
- Persons authorised to release identifiable or re-identifiable data shall ensure the proper authorisations are gained and procedures followed.

Registry Operator Team

- Liaise between CPR Steering Committee/working committees, report clients, site Data Managers and super users.
- Recommend level of data retrieval for individual data user accounts and automated client reports.
- Review data audit trails to ensure data privacy and confidentiality is maintained.

CPR Steering Committee and working groups

- Advise and approve level of data access for individual data user retrieval, and also for automated and customised client reports.

HREC

- Review of whether the registry conforms to relevant privacy principles and guidelines.

All Registry Personnel

- Maintain access account details including passwords in strict secrecy.
- Participate in educational and training opportunities as required.
- Maintain awareness of privacy and registry policies and procedures that relate to their area.

- Take responsibility for and maintain the privacy and confidentiality of all Registry-related data.
- Request identifiable/re-identifiable data only as appropriate.
- Provide feedback on database privacy and confidentiality measures to ACOR Steering Committee, working groups and Registry Operator Team as required.

6. Authorities, Compliance and Risk

Access to the Registry is restricted to authorised personnel.

Compliance to this policy is mandatory for all data users, report clients, ACOR members, staff of the Registry Operator(s), and any third-party service providers.

Compliance applies to all information associated with the Registry including paper, data, software, and networks.

The risks of non-compliance with this policy are:

- Divulgence of private and confidential information to unauthorised personnel.
- Harm occurring to individuals as a result of unauthorised data access.

6.1 Exemptions

Exemptions to policy components can be requested of ACOR or their designated Exemption Authority where compelling justification exists. Those seeking exemption must submit a justification and risk assessment to ACOR or their designated Exemption Authority via the Registry. The assessment must also identify substitute measures to be taken to control and reduce non-compliance risk, and acknowledge acceptance of any residual non-compliance risk.

7. References

The following documents (current versions where applicable):

7.1 CPR Policies

POL	Title
CPR POL001	Governance and Intellectual Property
CPR POL002	Choice and Changes of Data Variables
CPR POL003	Education and Training
CPR POL004	Security Measures
CPR POL005	Privacy and Confidentiality
CPR POL006	Quality Control Procedures
CPR POL007	Communication
CPR POL008	Data Collection
CPR POL009	Output Information and Registry Reports
CPR POL010	Changes to Registry Conduct

7.2 Standards and Guidelines

Title	Organisation/Owner
Operating principles for Australian Clinical Quality Registries	Australian Commission on Safety and Quality in Healthcare
Guidelines for the establishment and management of clinical registries	Australian Commission on Safety and Quality in Healthcare, NHMRC
Architecture Overview: Clinical Registries.	National E-Health Transition Authority (NEHTA)
Privacy Act 1988, Privacy Amendment Act 2012, Privacy Regulation 2013, and Australian Privacy Principles	Australian Government
National Statement on Ethical Conduct in Human Research	National Health and Medical Research Council
Australian Code for Responsible Conduct of Research	National Health and Medical Research Council, the Australian Research Council and Universities Australia

7.3 Other

Title	Organisation/Owner
Client Registry Services Agreement	ACOR
Registry Services and Operating Agreement	ACOR
Testing and Validating Draft Operating Principles and Technical Standards for Australian Clinical Quality Registries	Monash University, Australian Society of Cardiothoracic Surgeons, CCRE Therapeutics.

8. APPROVALS

Prepared by _____
Cardiac Procedures Registry Project Manager

Approved by _____
Chair of CPR Steering Committee, on behalf of ACOR Limited