VICTORIAN CARDIAC OUTCOMES REGISTRY

VICTORIAN CARDIAC OUTCOMES REGISTRY

VCOR Privacy Policy

Version 2.0

1 December 2016

MONASH University

Table of Contents

Document Version Control 3

Document Version Control 3

1. Preface 4

2. Project Information 4

2.1 Purpose of VCOR 4

2.2 Project Overview 4

3. Information and Privacy 5

3.1 What is personal information? 5

3.2 What information is collected in VCOR? 5

3.3 How is information collected? 6

3.3.1 Why collect identifiable, personal information? 6

3.4 Security of personal information 7

3.4.1 How will the privacy of patients be protected? 7

3.4.2 How will VCOR information be shared? 8

4. ACCESS TO INFORMATION 8

4.1 Accessing information in VCOR 8

5. ADDRESSING CONCERNS 9

5.1 General concerns 9

5.2 Ethical concerns 9

5.3 Complaints handling 9

6. CONTACTING VCOR 10

7. CHANGES TO THE VCOR PRIVACY POLICY 10

APPENDIX A: The Australian Privacy Principals 11

Permitted health situations 11

APP1: Open and transparent management of personal information 11

APP 2: Anonymity and pseudonymity 12

APP3: Collection of solicited personal information 12

APP4: Dealing with unsolicited personal information 13

APP5: Notification of the collection of personal information 13

APP6: Use or disclosure of personal information 13

APP7: Direct Marketing 14

APP8: Cross-border disclosure of personal information 14

APP9: Adoption, use or disclosure of government related identifiers 14

APP10: Quality of a person's health information 15

APP11: Security of personal information 15

APP12: Access to personal information 15

APP13: Correction of personal information 15

Document Version Control

Version	Date	Reason/Comments/Approvals
1.0	24-JUN-2014	Initial Version Release. Ratified by the Steering Committee on 15-Aug-2014.
2.0	1-DEC-2016	Minor text changes. Approved by the VCOR Steering Committee on 7-FEB-2017.

1. Preface

The following policy defines how the Victorian Cardiac Outcomes Registry (VCOR) implements privacy practices into its everyday operations and specifically, how relevant privacy principles are addressed in common registry practice. Monash University has ongoing practices and policies in place to ensure that personal information is managed in an open and transparent way and relevant privacy principles are upheld. The University Privacy Compliance Framework is available at: http://www.privacy.monash.edu.au/. VCOR complies with Monash University policies and procedures.

Further to Monash's commitment, VCOR is committed to ensuring the security, privacy and confidentiality of all information collected and housed within the registry in addition to the handling of stakeholder information outside the registry's database. All patients' 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 relevant state and territory laws and regulations relating to the collection, storage and dissemination of such information. All registry activities have been approved by a National Health Medical Research Council (NHMRC) approved Human Research Ethics Committee (HREC).

2. Project Information

2.1 Purpose of VCOR

The purpose of the VCOR is to improve the safety and quality of health care provided to patients with cardiovascular disease. Key clinical information from individual healthcare encounters is collected to allow for risk-adjustment of outcomes to facilitate benchmarking of performance and quality improvement in the delivery of health care services. VCOR monitors the safety and quality of care given to patients with cardiovascular disease undergoing specific cardiac procedures or with specific cardiac conditions. Selected risk-adjusted outcomes are reported back to stakeholders. This has been achieved by undertaking a Victoria-wide clinical quality registry: a proven mechanism for data analysis, reporting and benchmarking quality in the provision of health services.

2.2 Project Overview

Monash University in conjunction with the Cardiac Clinical Network and funding from the Victorian Department of Health and Human Services have developed and maintain a secure, online data collection tool and data storage mechanism for analysis and reporting. The success of relevant treatments and procedures performed on patients presenting in Victorian hospitals with cardiovascular symptoms is assessed and reported. This is achieved by capturing data about patient demographics; symptoms; clinical presentation and diagnosis; treatments they receive and related clinical outcomes.

VCOR is designed to collect a minimised, standard set of information from all patients undergoing specific cardiac procedures or treatments at participating hospital sites. The data is gathered using predetermined procedures and standardised definitions and includes collecting patients' identifying information, presenting and treatment details and related clinical outcomes. Data is collected at baseline (time of presentation for procedure), 30 days and potentially 12 months, with the additional potential for ongoing annual follow up in the future. Data is captured electronically in an online data entry system.

Data is stored securely within Monash University servers and retained indefinitely. The project conforms to national operating principles for clinical quality registries (CQRs) as set out by the Australian Commission on Safety and Quality in Health Care (ACSQHC). As such, the governance of the registry is in keeping with these principles. All project matters are governed by the VCOR Steering Committee (SC) by way of liaison with two subcommittees: The Clinical Quality Committee (CQC); and the Data Access, Research & Publications Committee (DRP). Monash University's Centre of Cardiovascular Research and Education in Therapeutics (CCRET) acts as the coordinating data management centre, answering to the Steering Committee. A Clinical Director has been appointed as the Chair of all three committees and site liaison.

Monash University, eSolutions, under the guidance of CCRET is responsible for developing and maintaining the data entry system. CCRET is responsible for performing data quality controls, and reports for providing structured feedback to participating sites. Feed-back is provided quarterly to each participating hospital. Emphasis is on performance relative to other hospitals and performance over continuous reporting periods. An annual report is published yearly.

All hospital data remains the property of that institution. All collective registry data and data management systems operate under the custodianship of Monash University.

3. Information and Privacy

3.1 What is personal information?

Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether or not the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.

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

3.2 What information is collected in VCOR?

Sensitive and personal information will only be collected where reasonably necessary to conduct essential registry functions, or other activities as approved by a Human Research Ethics Committee (HREC). VCOR collects information about patients and their health status before, during and after hospital admission for relevant procedures, treatments and interventions. For example:

- Hospital Identification Number
- Name
- Date of Birth
- Contact Information (Phone Number and Postcode)
- Medicare or Department of Veterans Affairs Number
- The name of the hospital
- The reason for the treatment received

- Basic information about health status before, during and after the procedure
- Details about the treatment
- Complications (if any)
- Discharge information
- Health and quality of life information up to 30 days after discharge (where relevant)

In order to achieve the primary function of VCOR, other personal information may be collected, held and disclosed to support the registry's day to day operations. This includes collecting contact information about stakeholders, other researchers, hospitals and health services, service providers and other individuals or groups who may be involved or correspond with VCOR in order for the registry to function effectively.

3.3 How is information collected?

Every patient who undergoes a relevant procedure or treatment in a participating VCOR hospital will have their data entered into VCOR by local hospital staff.

Registry data is taken directly from hospital medical records (by local hospital staff) and entered into the secure VCOR web-based data entry system. Where relevant, hospital staff may contact patients or their doctor directly to follow-up on patients' health status after discharge.

The registry employs an opt-out approach to consent, where all patients included in the registry are afforded the right to not have their information recorded. This is done by delivering a patient information sheet (PIS) to all patients during their time in hospital (except for situations where a Human Research Ethics Committee has approved a waiver of consent, in specific situations). Hospital staff must make every best effort to ensure that a sound process is documented and implemented for PIS delivery, unless ethical approval to waive consent has been granted. This PIS explains the function of the registry and explains the process for opting out of the registry. More general information about the registry, the data collection procedure and opting off the registry can also be found on the VCOR website at: http://vcor.org.au/

It is important to note that the only time personal information may be collected form a patient outside the usual function of the registry data collection is when a patient decides not to participate in VCOR. Some personal information may be required for VCOR staff to identify the correct patient record within the database and ensure that all the relevant information is completely removed from the registry, as requested.

3.3.1 Why collect identifiable, personal information?

It is important that VCOR collects identifiable, personal information about cardiac patients. Having this information allows hospital staff to link back to the patient's medical records and to follow-up on the patients' health status following their procedure (where appropriate). VCOR may also link to hospital administration, ambulance services and Department of Health databases to check whether patients have been readmitted to other hospitals or to assess for longer-term mortality. In the future, it is intended that VCOR, like other registries, will link data with the Australian Institute of Health and Welfare's (AIHW) National Death Index (NDI), the Department of Health and Human Services Victoria's Admitted Episodes Database and Ambulance Victoria's Cardiac Arrest Registry (and other databases) for this purpose. This will help determine long-term outcomes and mortality rates. This information will be used to benchmark hospital performance with a view to improving the quality of care provided to cardiac patients. In addition to linkages, information collected in the registry may also be used for further research relating to the standard of care provided to patients undergoing cardiovascular treatments and interventions in Victoria.

To protect patient's privacy, all linkage or further research activities using VCOR data are bound by privacy legislation and must meet specific privacy and security conditions before ethical approval is granted.

No research or data linkage activity will occur without approval from an NHMRC approved HREC. Please refer to section 3.4.1 below for more information about how patients' privacy will be protected.

3.4 Security of personal information

3.4.1 How will the privacy of patients be protected?

While hospital staff access patient records and enter the data into the registry, all data stored within Monash University's "Red Zone" for data security. Monash University is the first Australian University to achieve accreditation for its Information Security Management System (ISMS) for research systems under ISO/IEC 27001 certification. ISO/IEC 27001 formally specifies a requirement for adopting ongoing ISMS. Certification requires an overarching management framework through which an organization identifies analyses and addresses information security risks and responds to changing security threats, vulnerabilities and business impacts.

In 2014, VCOR was incorporated into Monash University's ISMS which is ISO/IEC 27001 certified.

The architecture of the VCOR online system and database housed at Monash University is compliant with all aforementioned legislation and guidelines. Please refer to the *VCOR Data Security Policy* for more information about how data is encrypted and stored securely. All VCOR policies are publicly available on the VCOR website at: http://vcor.org.au/Policy-documents.

All information collected about patients is treated as confidential. Identifying information is protected by privacy legislation and would only be disclosed with the patient's permission, or in compliance with the law. All data is safeguarded by State and Commonwealth privacy laws. No identifiable information will be shared. No personal information about patients will ever be disclosed in any publication or report. Any known breach of privacy will be reported to the Coordinating Principal Investigator and relevant ethics committee(s) as soon as possible.

In the event where the registry may need to communicate with sites about individual cases or patient information, VCOR does not use identifiable or potentially re-identifiable hospital or patient identifiers when referencing individual cases. A unique, registry identifier is given to every case and this identifier is used in all correspondence. It is practice to never email any potentially re-identifiable or sensitive information or data (such as name, date of birth or hospital UR number). Any VCOR operation that may use potentially re-identifiable or sensitive information is done by way of a Secure File Transfer Protocol (SFTP) to avoid any breaches of patient privacy or confidentiality of sensitive information. SFTP is a network protocol that provides file access, transfer and management functionalities over a secure data stream. Users are given a secure access log in to retrieve files that have been stored securely for download (instead of emailing or faxing information). All SFTP transferred files are available for a limited time and archived automatically.

Access to VCOR data is strictly limited and user's identities must be authenticated upon registration for VCOR access. All user accounts are password-protected, have expiration dates and are limited to personnel who have been authorised by relevant delegates (e.g. Principal Investigators or Data Managers).

Access to the registry data is site specific. Users cannot add/view/manage or report on data unless they have specific permissions to do so. That is, if a patient has data in the registry for two procedures at two different

hospitals, each hospital can only see the data relevant to their site. Similarly, if two different doctors treat a single patient at different times, each doctor can only see data for the patients/procedures that they themselves were assigned to. VCOR data management staff can, however, see all data in the registry.

3.4.2 How will VCOR information be shared?

VCOR 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 may use unidentified, aggregate group data for future research projects. Information collected in the registry, may be used for further research relating to the standard of care provided to patients undergoing cardiovascular treatments and interventions in Victoria. This includes ongoing linkage to other hospital, ambulance services and Department of Health databases to verify if patients have been readmitted to hospital. Linkage to administrative datasets such as the Australian Institute of Health and Welfare's (AIHW) National Death Index (NDI), the Department of Health and Human Services Victorian Admitted Episodes Database and Ambulance Victoria's Cardiac Arrest Registry (and other databases) helps determine long-term outcomes and mortality. To protect the privacy of patients, all linkage activities are bound by privacy legislation and must meet specific privacy and security conditions before ethical approval is granted. Any further research outside the registry's initial scope undertaken using VCOR data will require approval by a Human Research Ethics Committee.

Currently, any internal registry activity that may require transfer of potentially re-identifiable information (either within the VCOR project team or between VCOR and participating hospitals) follows a secure file transfer protocol (SFTP). Please refer to section 3.4.1 for more information about this process.

The VCOR Data Security Policy states that *"no identifiable research data and/or health information should ever be sent via email or fax or transported on a portable disk or disk drive".* Please refer to the *VCOR Data Security Policy* for more information about how data is encrypted and stored securely. All VCOR policies are publicly available on the VCOR website at: http://vcor.org.au/Policy-documents

4. ACCESS TO INFORMATION

4.1 Accessing information in VCOR

Patients do have the right to request access to personal information stored in VCOR. Individuals may request a copy of their personal information at any time. Individuals that request information must identify themselves and be able to provide sufficient proof of identity. This includes providing five points of identification over the phone. For example, patients would be asked to provide their full name, date of birth, Medicare number or postcode, the date of their procedure and/or at which hospital the procedure was performed. The provision of this information will assist VCOR staff in identifying patient's data correctly within the registry and ensure that information is not disclosed in error. Upon confirming the patient's identification, copies of the requested information will be sent via traceable post within a reasonable timeframe, negotiated with the patient at the time of their request. This information cannot be sent electronically.

Obviously, this identification process precludes patients from using a pseudonym and/or from being anonymous in communication with the Registry for these types of requests. Information will not be released until Registry staff are satisfied that sufficient identification has been provided.

Patients are free to contact VCOR if they become aware that any information is inaccurate and/or incomplete (refer to section 6 for VCOR contact details). The Project Manager will take reasonable steps to either correct the information, or, if necessary discuss alternative action with the patient. VCOR would also recommend that patients contact the participating hospital to ensure that their records are up to date with their treating health service (all data in VCOR comes directly from hospitals).

5. ADDRESSING CONCERNS

5.1 General concerns

If patients or stakeholders have any questions or concerns about general project operations, they can contact the VCOR Project Manager or Principal Investigator (refer to section 6 for VCOR contact details). General comments or questions may have already been addressed on the VCOR website's frequently asked questions page: http://vcor.org.au/FAQs_general.

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 research conduct, enquiries should be directed to the approving Human Research Ethics Committee (HREC) for the relevant hospital or health service. A list of the HREC contact details for participating sites can be viewed on the VCOR website at:
http://vcor.org.au/Contact.

5.3 Complaints handling

A complaint can be made by any stakeholder, partner organisation, community or individual with whom VCOR has an established relationship, in addition to any member of the public whether an individual, organisation or other entity. VCOR takes privacy and data management obligations seriously and welcomes any feedback in order to improve the quality of our work. Complaints will be handled in the timely and sensitive manner protecting the privacy of respective parties.

VCOR will request that any complaint or concern be submitted in writing (via email, fax or post: refer to section 6 for contact details). A member of the VCOR Project Team will acknowledge all correspondences within one week of receipt. VCOR will attempt to resolve any complaint within 15 working days, however, if this is not possible, VCOR will contact the complainant to advise of the status of the matter. The VCOR Project Manager and Principal Investigator will be notified of all complaints and issues will be escalated accordingly. HREC committees will be notified of any complaints and/or adverse events as per the conditions of each HREC approval.

If patients or other stakeholders are unsatisfied with the outcome of complaints relating to privacy or confidentiality, VCOR will advise further options including, if appropriate, review by the Office of the Australian Information Commissioner.

6. CONTACTING VCOR

Patients and other external stakeholders can contact the registry to update their details and/or opt out of participation or subscription to communications from the registry by contacting the VCOR Project Manager on the details below:

Mail to: **VCOR Project Coordinator**
Department of Epidemiology & Preventative Medicine, Monash University
Reply Paid 86460
99 Commercial Rd, Melbourne VIC 3004

Email: vcor@monash.edu

Patient Hotline: 1800 285 382 (free call)

Office Telephone: +61 3 9903 0302

7. CHANGES TO THE VCOR PRIVACY POLICY

This Privacy Policy was updated and ratified by the VCOR Steering Committee in November 2016. VCOR reserves the right to update the policy at any time, as long as it complies with the Privacy Act and other relevant state and commonwealth legislation. The most up to date version of all VCOR policies are publicly available on the VCOR website at: http://vcor.org.au/Policy-documents.

APPENDIX A: The Australian Privacy Principals

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 single set of principles that apply to both agencies and organisations, which are together defined as APP entities. These APPs replace both the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs). The APPs regulate the handling of personal information by Australian government agencies and some private sector organisations, covering the collection, use, disclosure and storage of personal information. They allow individuals to access their personal information and have it corrected if it is incorrect. How VCOR addresses each of these privacy principles is explained in greater detail 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 defined as a type of sensitive information. Permitted health situations that allow collection, use and/or disclosure of health information in certain research and other purposes include the following 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 impracticable 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 diseases.

VCOR therefore qualifies as a permitted health situation as the registry's primary function is is to improve the safety and quality of health care provided to patients with cardiovascular disease in Victoria and is relevant to public health and safety. It is not possible for the registry to function if identifiable health information is not collected. It is impracticable to obtain individual consent from individuals based on the sheer number of cases that will be included in the registry (>10,000 annually, when fully operational). However the registry has adopted an HREC approved 'opt out' approach to consent. This process minimises recruitment bias and ensures that all groups are well represented in outcome assessment, while affording patients the right to not participate in the registry should they wish to withdraw their data from inclusion.

APP1: Open and transparent management of personal information

An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the management of personal information that is open and transparent.

VCOR is committed to open and transparent management of personal patient information. As such, no identifiable patient data is ever reproduced in public reports or documentation. VCOR has a public facing website where information about the registry, its primary functions and reporting practices are available (https://vcor.org.au/).

All VCOR policies and procedural documentation are publicly available on the VCOR website at http://vcor.org.au/Policy-documents.

VCOR also chooses to adopt an 'opt-out consent' process to ensure, where possible, all patients are adequately informed about data collection, their rights and the process for not participating should they wish to withdraw their consent for their data to be collected and used.

APP 2: Anonymity and pseudonymity

Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

VCOR is actually unable to offer patients anonymity and/or the option of a pseudonym within the registry as this would impact on the registry's ability to carry out key functions (e.g. data linkage). VCOR does, however, provide patients the opportunity to have their data removed from the registry, should they wish for their identifiable information not be stored in VCOR. Any request from a patient to remove personal information will actually result in all data relating to that individual being removed from the database. Generally, this is the only contact the registry has with patients (all contact is made by hospital staff, generally as part of the usual episode of care). As such, it is impracticable for the central registry to deal with patients who do not identify themselves, as it necessary for individuals to identify themselves for this request to be processed (in order for their details to be removed effectively). Similarly, if a patient requests access to their data within the registry, they must first be identified to protect the confidential nature of the information.

In situations where individuals are contacting the registry for general information, there is no requirement for them to identify themselves and VCOR acknowledges this right.

APP3: Collection of solicited personal information

The entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities. The information handling requirements imposed by APP 3 does not apply to an organisation if a 'permitted health situation' exists. It is open to an organisation to comply with the APP requirements even though an exception applies.

VCOR, as a permitted health situation, is in fact exempt from complying with APP3, however, the registry does not collect any information about patients that is not used for general registry function.

VCOR does collect and house contact details for relevant industry stakeholders to engage in general communications and to facilitate the Registry's reporting obligations. This includes contact details for participating clinicians and other engaged health service staff, hospital CEO's and financial stakeholders.

Any communications that are sent by way of a mailing list (e.g. a registry newsletter) clearly provide an opportunity for recipients to unsubscribe. These types of communications are never sent to patients. Any VCOR related communication with patients is undertaken by the health service where they were treated and

is generally considered a part of the usual episode of care and health-care follow-up. No patient information in the registry will be used outside of the function of the registry itself.

APP4: Dealing with unsolicited personal information

If the entity receives personal or sensitive information that was not solicited, they must, within a reasonable period after receiving the information, decide whether this was information they have collected under APP3. If not, the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

VCOR has processes in place to ensure that if any unsolicited information is received, the information will be deleted or destroyed and the sender notified that personal or sensitive information was received in error. It is unlikely that this will occur in terms of registry data, as data is transferred via the online data entry system and access to this system is strictly limited (refer to section3.4.1 for more information).

APP5: Notification of the collection of personal information

At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances to notify the individual or ensure that the individual is made aware.

Where possible, all patients are informed about the registry, their rights and the process for not participating should they wish to withdraw their consent for their data to be collected and used. This is done at the hospital level, as part of the opt-out approach to consent, where hospital staff deliver a patient information statement to every eligible patient - except in situations where a Human Research Ethics Committee has approved a waiver of consent for certain patient subgroups. This PIS explains the function of the registry and explains the process for opting out of the registry. For more information about the opt-off process, see refer to http://vcor.org.au/opt_out. It is understood that hospital staff will make the best possible attempt to deliver a patient information statement to every eligible patient. In cases where patients may need access to the PIS at another time, they can contact the registry for a copy of the relevant document.

APP6: Use or disclosure of personal information

If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless: the individual has consented to the use or disclosure of the information.

VCOR, as a permitted health situation, is in fact exempt from complying with APP6, however, the Registry will never disclose personal information about an individual for purposes unrelated to the key function of the registry.

VCOR has measures in place to protect the privacy of patients as outlined in section 3.3 of this policy. VCOR also has Data Security and Data Access policies which describes the data security measures for VCOR. This includes the collection, use and access of data and the VCOR online system in accordance with legal, ethical and national best practice guidelines. All VCOR policies are publicly available on the VCOR website at: http://vcor.org.au/Policy-documents.

APP7: Direct Marketing

If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

VCOR, as a permitted health situation, is exempt from complying with APP7, however, personal information about any individual whose data is stored within the registry will never be used or disclosed to another entity for direct marketing purposes. All reasonable measures will be taken to ensure that this information is stored securely in accordance with section 3.4 'Security of Personal Information' and the *VCOR Data Security Policy*. All VCOR policies are publicly available on the VCOR website at: http://vcor.org.au/Policy-documents.

APP8: Cross-border disclosure of personal information

Before an APP entity discloses personal information about an individual to an overseas recipient; and who is not the entity or the individual, the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than APP1) in relation to the information.

Data entered into VCOR is stored on a secure Monash University server located at the University's Clayton campus. VCOR does not send or store any data outside of Australia. In the unlikely event that registry data may be shared with an international body in the future, say for the purposes of data linkage, no identifying personal information will be shared with the international entity. All data shared or reported on would be of a de-identified nature.

VCOR also has processes in place to avoid accidental cross border data transfers: Hospital staff engaged with the VCOR project are aware (and regularly reminded) that any personal information or potentially re-identifiable data should never be sent via email. This is a preventative measure VCOR has put in place to avoid cross border data transfers, as email servers (for example Gmail servers) are often located overseas. As previously outlined in section 3.4.1, VCOR uses a secure file transfer protocol to ensure that all identifiable or potentially re-identifiable information is transferred securely and remains within Australian borders.

APP9: Adoption, use or disclosure of government related identifiers

An organisation must not adopt a government related identifier of an individual as its own identifier of the individual.

VCOR uses a unique automatically generated, registry identifier for every patient and every case that is entered onto the Registry. These identifiers are used in all correspondence about patient information. Therefore, whilst Government identifiers are collected in VCOR and serve a purpose (Medicare number, Department of Veteran Affairs number, etc.) they are not adopted by the registry as a unique identifier and never will be.

The VCOR data entry system will not disclose government identifiers to third parties unless it is for the purposes of a linkage with government databases who use this information to facilitate HREC approved data linkages. These organisations generally use secure data transfer protocols of their own. VCOR will never email, fax or save to an external hard drive any potentially identifiable or re-identifiable patient information. Any other research organisation or registry requesting data linkage with VCOR other than government organisations will never be provided with patient identifiers from the VCOR database.

APP10: Quality of a person's health information

An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

VCOR aims to ensure that all information is accurate, complete and up to date. VCOR data is entered and updated by participating hospital staff, so to ensure data integrity, VCOR monitors the quality of data entry at every site after the first twelve months of data entry, and once every three years thereafter. Any queries or discrepancies raised in this process will be sent back to local Data Managers for review. Ongoing quality monitoring is also part of general VCOR operations. Data discrepancies that arise are dealt with on a case by case basis.

Sites have an important role in ensuring the accuracy of patients' personal information and also have a responsibility in ensuring that Registry data is regularly cross-checked against local hospital information systems in order to confirm complete ascertainment of cases from each participating site. Where omissions are discovered, it is expected that the Data Manager would ensure that these are corrected.

APP11: Security of personal information

If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Please refer to Section 3.4 of this policy, 'Security of Personal Information' and the *VCOR Data Security Policy* for more information about how data is encrypted and stored securely and what steps are made to protect information from misuse. All VCOR policies are publicly available on the VCOR website at: http://vcor.org.au/Policy-documents.

APP12: Access to personal information

If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Please refer to section 4 of this policy 'Access to Information' for the processes in place to allow patient access to information stored within the registry.

APP13: Correction of personal information

If an entity holds personal information about an individual and the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading or the individual requests the entity to correct the information, the entity must take such steps (if any) as are reasonable in the circumstances to correct that information.

If a patient wishes to correct data held by VCOR they will be advised to contact the VCOR Project Manager. The Project Manager will take reasonable steps to either correct this information, or, if necessary discuss alternative action with the patient. Please refer to sections 4 and 5 above 'Access to Information' and 'Addressing Concerns'.