VCOR
VICTORIAN CARDIAC OUTCOMES REGISTRY

VICTORIAN CARDIAC OUTCOMES REGISTRY

Data Security Policy

Version 2.0
1 December 2016

MONASH University

Table of Contents

Document Version Control

Version	Date	Reason/Comments/Approvals
1.0	26-FEB-2014	Initial Version Release. Approved by the VCOR Steering Committee on 11-MAR-2014
1.1	6-JULY-2015	ISO Certification Updated.
2.0	1-DEC-2016	Updated section 2.1, 2.2, 3.1, and added section 5.2. Minor updates throughout report. Approved by the VCOR Steering Committee on 7-FEB-2017.

1. Preface

This policy document describes the data security measures for the Victorian Cardiac Outcomes Registry (VCOR) including the collection, use and access of data and the VCOR online system in accordance with legal, ethical and national best practice guidelines. Data security is imperative for this project as VCOR stores personal identifying information about patients, with data hosted centrally within secure servers at Monash University. The VCOR online data collection tool and database are accredited with ISO/IEC 27001 certification, a formal Information Security Management System (ISMS) accreditation.

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) will act 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. Data Security Policy

3.1 Secure data collection and housing

Data is collected via the VCOR online data entry system and hosted by Monash University, the data custodian. All activities are in accordance with Monash University's Information Technology Services Security Framework policy, which can be viewed in full here: http://www.policy.monash.edu/policy-bank/management/its/ict-security-risk-policy.html. Security of the data is ensured in the following ways:

1. The web application has been developed in Microsoft ASP.NET 2.0 and is hosted on an IIS Web Server by the eSolutions IT team at Monash Clayton. All data storage is in a Microsoft SQL™ Server 2008 database farm located in the Monash Clayton campus secure (Red Zone) server room. Access to this server room is available only to the Systems IT Administrators.

2. All traffic between the data collector's browser and the web server uses a SSL secure certificate to encrypt data to 2048 bits.

3. All traffic between the web server and the database server is passed through an IPSEC tunnel that encrypts data to 2048 bits.

4. All user accounts are password-protected and limited to authorised personnel who have completed a registration form for access. The authentication processes for user access to the registry involves formal registration including identity checks and verification from an existing authorised user (e.g. VCOR Administrator, Principal Investigator or Data Manager). When VCOR is notified that a staff member has left the project, their access to the system is removed. All user accounts are audited every six months to ensure the user list is up-to-date and obsolete accounts are removed. All systems access is attached to an individual user account and all access to the server logged.

5. Disaster recovery processes are built into Monash's security framework policies, and are in place to minimize the effects of major incidents on business activities. For example, in the case of fire or loss of data, the database server is mirrored each day to a backup facility at the Monash Noble Park campus. Backups of the system are stored in a secure location with limited access and numbered seals are used on the storage container to detect any unauthorised access. Access to the storage media by staff is logged.

6. Individual hospital sites will manage and secure any paper-based data records in accordance with the Health Records Act (2001). Sites will archive and destroy any paper records according to site-specific general record retention schedule(s). This is the responsibility of the Principal Site Investigators who oversee each site's registry operations.

Any registry staff or investigators with access to data are trained by VCOR Project Managers (or delegates) according to Good Clinical Practice guidelines, state and federal privacy legislation and the NHMRC's National Statement on Conduct in Human Research. Only the VCOR Project Manager and Monash staff working directly with the Project Manager will have access to raw VCOR cohort data. All registry staff with access to data are trained according to Good Clinical Practice guidelines, state and federal privacy legislation and the NHMRC's National Statement on Conduct in Human Research.

4. Use of the VCOR online system and protection of data

The VCOR online data entry system comprises of five types of user accounts with different levels of authority to limit access to specific system functions. User access is provided by the VCOR Project team and will only be activated once the VCOR User Registration Form (see appendix a) is completed and authorised by a relevant project member (e.g. Principal Investigator or approved VCOR project staff). All users are issued with a unique username and password that will determine their level of access to the system and also ensure that an audit trail exists.

4.1 User access levels

The type of access depends on what type of data can be viewed, edited and/or downloaded from the system. Various functions include the ability to view, enter, edit, save and submit (lock) data and to extract data/run reports. Access is granted to VCOR users as one of the following roles:

Level of Access	Role	Accessibility
Open Access	***Administrators*** Project Manager Project Team Project Developer	View/Edit/Delete all data Extract raw data (all sites) View summary reports (all sites) View de-identified Operator Codes
Limited Access	***Site Data Managers***	View/Edit/Submit/Delete own data View identifiable Operator Codes Extract raw data for own site Generate summary hospital reports
	Site Data Collectors	View/Edit own hospital data
Restricted Read-only Access	***Clinicians*** *(where relevant)*	View own patient data (multiple sites) Generate summary clinician reports
	Site Report Managers	View own hospital data Generate summary hospital reports Extract raw data for own site

4.2 User Role Matrix

The matrix below shows each user's access to specific functions of the online data collection system:

Function	Admin	DM	DC	RM	Clin
	All data	Local hospital data only			*
Log On	Y	Y	Y	Y	Y
Manage Personal Account (Change Password, Security Question and Email)	Y	Y	Y	Y	Y
Reset Forgotten Password (Automated - Requires Security Question)	Y	Y	Y	Y	Y
Add User Account (New User)	Y				
Manage Account (Edit, Lock, Unlock, Activate/Deactivate)	Y				
Add Site (New Site)	Y				
Manage Site (Edit, Lock, Unlock, Activate/Deactivate)	Y				
Dashboard (Review Unsubmitted/Unlocked Data)	Y	Y	Y		
Dashboard (Review Outstanding Follow-Ups)	Y	Y	Y		
Patient List (View, Search, Review)	Y	Y	Y	Y	Y
View Patient Details (Patient Home)	Y	Y	Y	Y	Y
Add New Patient	Y	Y	Y		
Edit Patient Details	Y	Y	Y		
Match Existing Patient Records	Y	Y	Y		
Delete Patient Record	Y	Y			
View Event Data	Y	Y	Y	Y	Y
Add Event	Y	Y	Y		
Edit Event Data	Y	Y	Y		
Submit (Lock) Event	Y	Y			
Unlock Submitted Event Data	Y	Y			
Delete Event Data (Data must be unlocked)	Y	Y			
View Identifiable Primary Operator Clinician Codes		Y			
View Online Documents	Y	Y	Y	Y	Y
Generate Hospital Summary Reports (Own Site Data Only)	Y	Y		Y	
Generate Clinician Summary Reports (Own Patient Data Only)	Y	Y			Y
Extract Raw Hospital Data	Y	Y		Y	
Patient Opt-Out (Remove all Patient and Event Data)	Y				

* Clinicians can only view patient records linked to their Primary Operator Code (own patients, multiple sites).

Adm	**Administrator**	Access to all VCOR data (all sites, Primary Operator Codes de-identified)
DM	**Data Manager**	Access to local site data (own site, including Primary Operator Codes)
DC	**Data Collector**	Access to local site data (own site)
RM	**Report Manager**	Access to local site data (own site)
Clin	**Clinician**	Access to 'own patient' data (own patients only, across multiple sites)

5. Secure Transfer of Information

No identifiable or potentially re-identifiable research data and/or health information should ever be sent via email or fax or transported on a portable disk or disk drive. Some electronic communications between Monash and VCOR stakeholders may take place (e.g. coordination of data audits, meetings, and/or report dissemination, data queries, etc.) however this will pose no risk to research participants, as identifiable patient level data will not be transferred in these communications.

5.1 Secure File Transfer Protocol (SFTP)

Any transfer of registry data that contains identifiable or potentially re-identifiable information will follow a Secure File Transfer Protocol (SFTP). SFTP is a network protocol that provides file access, file transfer and file management functionalities over a secure data stream. It encrypts channels for sending data and is ideal for sensitive information being transmitted over networks. It uses SSL (Secure Socket Layer) to encrypt private documents in transmission. SFTP subsequently provides 'end to end' data security during transmission. Users are granted a username and password to access the SFTP website. They are notified via email when files are available for download. Files will only appear for a limited period before access is removed and the file is archived. In addition to manually transferring files using this protocol, automated file transfer processes (e.g. SQL Server Integration Services) are able to use this SFTP transmission protocol.

5.2 Secure Unified Research Environment (SURE)

SURE, the Secure Unified Research Environment, is a high-powered computing environment developed to help make best use of our national knowledge base. It is helping to bring researchers together from across Australia and the world to collaborate on large-scale projects tackling major health and social issues such as population ageing, diabetes and mental health. It has been purpose-built as Australia's only remote-access data research laboratory for analysing routinely collected data, allowing researchers to log in remotely and securely analyse data from sources such as hospitals, general practice and cancer registries. SURE was established with funding from the Australian Government National Collaborative Research Infrastructure Strategy (NCRIS) as part of the Population Health Research Network (PHRN).The PHRN is a collaboration that was set up in 2009 to further develop Australia's data linkage capabilities.

Monash University, through CCRET has established a contract with SURE. The benefit of using SURE is that the data is not able to be downloaded and is accessible only via the secure research environment. There are costs involved in accessing SURE which will be passed onto researchers. Information related to SURE related costs will be provided as needed.

6. Ethics and Privacy

Approval of the VCOR protocol by a Human Research and Ethics Committee constituted according to the NHMRC National Statement on Ethical Conduct in Human Research (March 2007) must be obtained prior to a site contributing to the registry. All VCOR activities are undertaken in accordance with the current protocol, the provisions of the reviewing Human Research Ethics Committee (HREC) and must be compliant with relevant local and national privacy regulations, including, but not limited to HPP 7 of the Records Act 2001 (Vic) and VIPP 7 in the Information Privacy Act 2000 (Vic) and NPP 7 in section 95A of the Commonwealth

Privacy Act 1988 (Cth). All relevant APPs within the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* were applied from 12 March 2014.

The architecture of the VCOR online system and database housed at Monash University is compliant with such legislation(s).

All personnel with access to the VCOR online system and all identifiable VCOR data are required to make the following declaration prior to access being granted (refer to the VCOR User Access Form, appendix a):

> *"I have read and understood the National Statement on Ethical Conduct in Human research (2007) and agree to undertake all VCOR related activities in accordance with the current protocol and provisions of the reviewing Human Research Ethics Committee (HREC), keeping with the Therapeutic Goods Administration's Guidelines for Good Clinical practice. I also agree to abide by national and local privacy regulations set out in all relevant privacy legislation relating to handling and managing health information (e.g. HPP 7 in the Health Records Act 2001 (Vic), VIPP 7 in the Information Privacy Act 2000 (Vic) and NPP 7 in section 95A of the Privacy Act 1988 (Cth)."*

7. Access to Data

All information held in the VCOR database is confidential. All staff with access to raw data must be aware of and compliant with all relevant ethical conditions and privacy regulations set out in section five of this document.

Contributing sites have 'real-time' access to their local site data by way of the online system. Permission to access and download summary reports and raw data extracts are based on the user access (refer to section three of this document). VCOR imposes no limitations on the use of this data, except that it complies with HREC conditions and relevant privacy legislation, as set out in section five of this document).

Any requests for access to VCOR cohort data for research or other purposes are considered according to the *VCOR Data Access Policy* and applications must be submitted in writing and approved by the VCOR Data Access, Reports and Publications Committee. Approved requests will never include transfer of identifiable patient information.

This document should be read in conjunction with the *VCOR Data Access Policy* for more information.

8. Technical Security Standards

VCOR operations are compliant with the operating principles for Clinical Quality Registries as set out by the Australian Commission on Safety and Quality in Health Care (ACSQHC). Data management systems are developed in accordance with the Australian Code for the Responsible Conduct of Research.

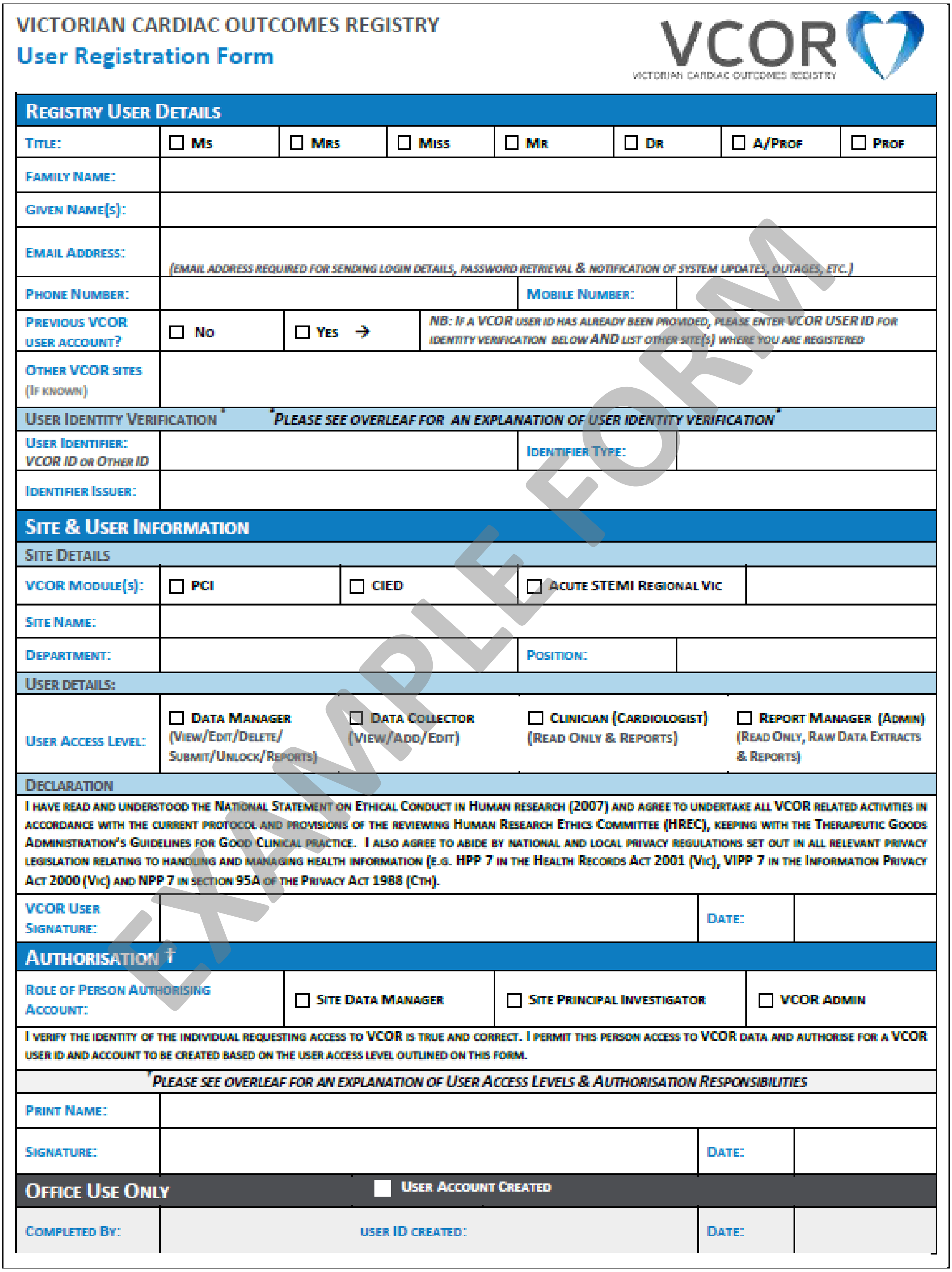
Database systems developed with identifiable or derived clinical data are always deployed into the Monash 'Red Zone' for data security. Secure Socket Layering (SSL) is used for all pages once the user is logged in to the online system. The user roles are maintained by the application and govern the authorisation of the exposed functionality (refer to section four of this document). Monash Policy secures the firewall so that access to the online system is restricted.

Monash University was 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.

Appendix A

VCOR User Registration Form



VICTORIAN CARDIAC OUTCOMES REGISTRY

User Registration Form

VCOR
VICTORIAN CARDIAC OUTCOMES REGISTRY

Registry User Details

Title:	□ Ms	□ Mrs	□ Miss	□ Mr	□ Dr	□ A/Prof	□ Prof

Family Name:	
Given Name(s):	
Email Address:	*(Email address required for sending login details, password retrieval & notification of system updates, outages, etc.)*

Phone Number:		Mobile Number:	

Previous VCOR user account?	□ No	□ Yes →	*NB: If a VCOR user ID has already been provided, please enter VCOR USER ID for identity verification below AND list other site(s) where you are registered*
Other VCOR sites (If known)			

User Identity Verification* *Please see overleaf for an explanation of user identity verification*

User Identifier: *VCOR ID or Other ID*		Identifier Type:	
Identifier Issuer:			

Site & User Information

Site Details

VCOR Module(s):	□ PCI	□ CIED	□ Acute STEMI Regional Vic	

Site Name:			
Department:		Position:	

User details:

User Access Level:	□ Data Manager (View/Edit/Delete/Submit/Unlock/Reports)	□ Data Collector (View/Add/Edit)	□ Clinician (Cardiologist) (Read Only & Reports)	□ Report Manager (Admin) (Read Only, Raw Data Extracts & Reports)

Declaration

I have read and understood the National Statement on Ethical Conduct in Human research (2007) and agree to undertake all VCOR related activities in accordance with the current protocol and provisions of the reviewing Human Research Ethics Committee (HREC), keeping with the Therapeutic Goods Administration's Guidelines for Good Clinical practice. I also agree to abide by national and local privacy regulations set out in all relevant privacy legislation relating to handling and managing health information (e.g. HPP 7 in the Health Records Act 2001 (Vic), VIPP 7 in the Information Privacy Act 2000 (Vic) and NPP 7 in section 95A of the Privacy Act 1988 (Cth).

VCOR User Signature:		Date:	

Authorisation †

Role of person authorising account:	□ Site Data Manager	□ Site Principal Investigator	□ VCOR Admin

I verify the identity of the individual requesting access to VCOR is true and correct. I permit this person access to VCOR data and authorise for a VCOR user ID and account to be created based on the user access level outlined on this form.

† *Please see overleaf for an explanation of User Access Levels & Authorisation Responsibilities*

Print Name:			
Signature:		Date:	

Office Use Only

■ User Account Created

Completed By:	user ID created:	Date:	