ANZICS Centre for Outcome and Resource Evaluation

Privacy & Security Assessment

ANZICS COMET

Version 1.6
April 2026

Table of Contents

Document Version Control

Date	Version	Summary of Revision	Approved By
March 2017	1.0	Initial Version	CORE Management Committee
November 2017	1.1	Review of Disclaimer	CORE Management Committee
April 2019	1.2	Updated Content	CORE Management Committee
July 2019	1.3	New datasets and eCRF Registration Form	CORE Management Committee
August 2019	1.4	Inclusion of ECMO Dataset	CORE Management Committee
June 2024	1.5	Domain URL change Update of secure file transfer to Microsoft SharePoint Secure Portal Inclusion of 2023 Renewal of Qualified Privilege Removal of reference to AORTIC COMET inactivity time change	CORE Management Committee
April 2026	1.6	COMET hosting environment changes Reorganisation of document	CORE Management Committee

1. Preface

This document describes the privacy and security assessment for the COMET software provided by the Australian and New Zealand Intensive Care Society (ANZICS).

2. The ANZICS CORE Auditing and Benchmarking Program

The Australian and New Zealand Intensive Care Society (ANZICS) is the leading advocate on all intensive care related matters across Australia and New Zealand. The ANZICS Centre for Outcome and Resource Evaluation (CORE) manages the bi-national auditing and benchmarking program through the following 5 ICU datasets:

- The Adult Patient Database (APD) commenced in 1992 with data submitted on ICU admissions related to patient outcomes and severity of illness. There are currently over 2 million individual ICU admissions in the database, making this one of the largest repositories of ICU patient information in the world. The longevity and high contribution to the database have provided important trend analysis since 2000. These data are patient-level data.
- The Australian and New Zealand Paediatric Intensive Care Registry (ANZPICR) collects data from all dedicated paediatric ICUs bi-nationally and paediatric data from mixed adult/paediatric units. These data are patient-level data.
- The Critical Care Resource (CCR) Survey annually collects resources and activity data, presently from over 80% of Australian and New Zealand ICUs. These data document service provision information, related to staffing, services, bed numbers, and quality and safety process activity. These data are unit-based data.
- The Central Line Associated Bloodstream Infection (CLABSI) commenced in July 2013 to monitor rates of CLABSI in Australian ICUs. These data are unit-based data.
- The Critical Health Resource Information System (CHRIS) commenced in March 2020 with the aim to monitor and share ICU resources during COVID-19 pandemic throughout Australia and New Zealand and has continued to be an important real-time monitoring tool for ICU activity since.

Intensive care units contributing to the ANZICS CORE Registries undertake local data collection complying with the minimum data sets for each respective registry. Detailed data dictionaries and data collections forms are available online at https://www.anzics.org/comet-core-outcome-measurement-and-evaluation-tool/

3. ANZICS CORE Data Collection Application (COMET)

CORE Outcome Measurement and Evaluation Tool (COMET)

COMET is the purpose-built software used to support the collection and submission of data to the ANZICS CORE Reporting System.

Overview:

COMET is intended to hold identified personal health information so that the intensive care units (ICU) can collect information for audit and benchmarking purposes.

ANZICS is acting as a software supplier, providing an efficient means for ICUs to collect information, and then submit/transfer some of that de-identified information to the ANZICS CORE registries.

In assessing the privacy and security of COMET it is important to differentiate it from the ANZICS CORE registries.

The ANZICS CORE registries are hosted in the Microsoft Azure cloud with Australia East (Sydney) as the primary region and Australia Southeast (Melbourne) as secondary region set up for ANZICS. The data is used for quality assurance and benchmark reporting. De-identified data is submitted on a regular basis by contributing ICUs, through the CORE Portal. Only ANZICS staff have access to the data.

COMET is a software application available to be used by ICUs. It has been developed as a web-based application that is hosted in the Microsoft Azure cloud with Australia East (Sydney) as the primary region and Australia Southeast (Melbourne) as secondary region set up for ANZICS. Its purpose is to allow the collection of information about patient admissions to an ICU, and for that information to be submitted to the ANZICS CORE registries. The application is structured into compartments for each ICU. An individual ICU only has access to patient information for their ICU. Each ICU has a system administrator role which can allocate access to other members of that ICU.

Information is exported from COMET to the CORE registries by the individual ICUs. No personal identifiers are exported except in the case where there is a specific pre-existing agreement with the contributing hospital.

ANZICS staff do not have access to any patient data.

There are some export and reporting functions available to individual ICUs to manage their patient's/unit's information but there is no reporting or exporting function that combines data from more than one unit.

ANZICS staff do not have access to any identified patient level reporting or exporting functionality.

Security:

The following section outlines the security and the technical information applied for the hosting of the ANZICS COMET data collection tool.

Details related to COMET Data Collection Application

Elements	Activity
Hosting Environment	• Hosted on Microsoft Azure Cloud Services.
Security	• Sites wishing to use COMET as their data collection tool are requested to check their hospital policies with regards to inclusion of personal information on the COMET database. • Once sites are registried by ANZICS to access COMET software, all site-user permissions are controlled by a nominated administrator at each contributing ICU. It is the responsibility of the site administrators at each to manage access to their site data. • The ability to extract data, modify users and access reports is granted to users on a granular basis and is managed by the ICU site administrator. ANZICS staff cannot access the patient data unless specific permission is provided by the ICU site adminstrator. • All data held in COMET are stored and protected in accordance to the the Australian Government Protective Security Policy Framework (PSPF) and the Information Security manual (ISM). • All data within COMET are encrypted at rest and in transit.
Users	• Password strength: must be at least 8 characters long, contain upper and lower case, contain a number and contain a non-alphanumeric character. • Password renewal: There is no time limit or expiry on passwords. • Only a site administrator or the user can reset a password that requires email authentication by the end user.
File & Data Transfer	• APD or ANZPICR compliant datasets can be extracted and downloaded from COMET for submission to the ANZICS CORE Registries.

Elements	Activity
Backup & Restore Processes	• Back-up processes, and agreed time out periods as per the Industry best practice guidelines.
Disaster Recovery	• As per Microsoft Azure best practice guidelines for protected data.

Privacy:

The information held in COMET is a copy of information that is held by the individual ICUs. COMET is not a Clinical Information System and it is not intended to be used to provide direct clinical care to patients. COMET is not a research study or clinical trial. Information can be extracted by the submitting unit, for the purposes of audit or research. Information extracted from COMET by an individual unit (e.g. for a local research project), is the responsibility of that individual unit which must comply with local governance, security, privacy and ethics requirements. This is not the responsibility of ANZICS or of the COMET software.

Australian Privacy Principles:

ANZICS is acting as the software/application provider and does not have access to any of the patient information. This means that the majority of the Privacy Principles are the responsibility of the contributing ICUs.

Consent to hold the personal health information of a patient by an individual ICU is the responsibility of the individual ICU and is managed by the privacy policies and practices of the hospital for that ICU.

Principle 1: An entity must take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints.

This is the joint responsibility of ANZICS and the ICU using COMET.

ANZICS has an application form for an ICU wishing to use COMET that makes it clear that the unit must comply with their local privacy policies and procedures.

Principle 2: Individuals must have the option of dealing anonymously or by pseudonym with an entity.

This is the responsibility of the ICU using the application. They can choose to use a pseudonym if they wish. We ask that incorrect information not be submitted such as a false date of birth, or gender as this degrades that quality of data submitted to ANZICS CORE.

Principles 3, 4 and 5: These deal with the collection of information, dealing with unsolicited information and notification of the collection.

These are the responsibility of the individual units, regardless of whether that information is collected by paper record, locally installed software or remotely hosted software. ANZICS recommends that ICUs advise patients and /or families of the data collection and submission to ANZICS CORE registries.

Principle 6*: *Use or disclosure of personal information.

ANZICS does not have direct access to personal information held within COMET and thus does not have the ability to use or disclose it.

It is possible that an ANZICS staff member may be given temporary access by a site administrator to that ICU's patient information for the purpose of problem-solving a data or software issue. This is covered by the ANZICS COMET Access Policy for Staff members.

Information is "disclosed" from COMET to ANZICS CORE using the data submission function. This is done by the individual ICUs, but the information is de-identified and so complies with the APP.

ANZICS staff members do not have the ability to export patient identifiable information from COMET, or submit data to the CORE registries on behalf of the ICUs.

Principle 7: Direct marketing.

ANZICS does not have access to any patient identifiable information within COMET. ANZICS cannot and will not use any patient information for direct marketing.

Principle 8: Cross-border disclosure of personal information.

ANZICS makes the COMET application available to Intensive Care Units overseas (outside Australia). This would mean the overseas unit would enter data into the system from their country. The information from the overseas unit may be exported, by the overseas unit, for their own purposes. This complies with the intention of this APP.

The main issue for the overseas units would be compliance with the privacy legislation within their own country. This is outside the scope of the ANZICS privacy assessment.

COMET does not have the functionality for ANZICS staff to extract, export or link the patient data to any overseas agency or organisation.

Principle 9: Adoption, use or disclosure of government related identifiers.

Individual ICUs may include the patient medical reference number or hospital identifier within the patient's record held in COMET. This information is not available to anyone outside that ICU.

The individual units are permitted to use these identifiers and their use within COMET is an extension of this. This information is encrypted and cannot be viewed outside of the application. Patient identifiers are not exported or submitted to the CORE registries except in the case where there is a specific pre-existing agreement with the contributing hospital.

Principle 10: Quality of personal information.

The quality or accuracy of the patient information held within COMET is the responsibility of the individual units entering the data. ANZICS does not have any access to the patient information and so cannot check, validate or correct the data. COMET includes validation rules to assist unit staff entering data, to ensure the best accuracy.

Principle 11: Security of personal information.

The assessment of security of the patient information contained within COMET is covered by the separate section in this document. Most of this security section is technical in nature and relates to the software, programming and hardware infrastructure.

The second part of the security assessment relates who has access to the data for a particular unit. The management of users for a unit, is the responsibility of the site administrator for each unit. The site administrator approves access and creates the user account for a unit. ANZICS does not have the ability to manage user accounts within units, except for the creation of the initial site administrator.

There is an increased potential risk with COMET as a web-based application compared to the prior application, which was hosted within a hospital's IT system/network. Poor management by the administrator may allow inappropriate people access to the data, and poor password management by users can increase risk of inappropriate access. However, any inappropriate access will be limited to one ICU and not any other ICUs. Guidance is provided by ANZICS CORE to unit directors and administrators to help minimise this risk and is included in the application process for a unit.

Units must follow their local hospital privacy policies when deciding who can have access to COMET.

Principle 12 and 13: Access and correction of personal information.

ANZICS does not have access to any patient information within COMET and so cannot provide access to the information for a patient and consequently cannot assist with any correction.

Individual units can provide information to patients if requested and may correct information if requested.

Any patient enquiry made directly to ANZICS will be forwarded to the relevant ICU administrator role or ICU clinical director.

4. Storage of health information

The ANZICS CORE Registry Program was declared a quality assurance activity in July 2016 under the Health Insurance (Quality Assurance Confidentiality) Amendment Act 1992. This provides protection to the overseeing committee from subpoena and gives confidentiality for identifying matters which become known through declared QA activities. For Australia, renewal of qualified privilege (5 years) was declared in late 2023 for the Australian and New Zealand Intensive Care Society (ANZICS) Centre for Outcome and Resource Evaluation (CORE) Intensive Care Registries to be a quality assurance activity to which Part VC of the Act applies.

5. Security Compliance

The hosting environment has been configured using industry standard architecture including separation of webservers and databases. All servers are hosted in Microsoft Azure which is ISO/IEC 27001:2022 certified.

ANZICS follows the guidance of the Australian Commission on Safety and Quality in Health Care, Australian Framework for National Clinical Quality Registries 2024.

Further information available on request.

6. Complaints

A complaint can be made by any stakeholder, partner organisation, community or individual with whom ANZICS has an established relationship, in addition to any member of the public whether an individual, organisation or other entity. ANZICS 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. ANZICS will request that any complaint or concern be submitted in writing (via email or post): refer to the ANZICS Webpage https://www.anzics.org/contact-us/

ANZICS will attempt to resolve any complaint within 15 working days. However, if this is not possible, ANZICS will contact the complainant to inform them of the status of their complaint. If patients or other stakeholders are unsatisfied with the outcome of complaints relating to privacy or confidentiality, ANZICS will advise further options including, if appropriate, review by the Office of the Australian Information Commissioner.

Appendix 1: ANZICS Disclaimer – COMET

Security of the Application

This application applies a range of security controls to protect its website from unauthorised access. However, users should be aware that connecting to COMET via an insecure public network raises the potential risk that a user's transactions are being viewed, intercepted or modified by third parties. ANZICS does not warrant that our website is free from computer viruses, worms, Trojan horses, or other destructive features.

It is the responsibility of the users of the site to protect their logon information and take measures to avoid misuse of their access to the site. This includes not sharing their logon information with other users and logging off from the site when not in use.

Privacy

ANZICS do not have access to any patient data entered into COMET that have not been extracted and submitted through the CORE portal. No patient identifiable data is included in the data that are extracted for submission to ANZICS except in the case where there is a specific pre-existing agreement with the contributing hospital.

Appendix 2: Unit Application Form to Use COMET

COMET IMPLEMENTATION FORM

To proceed with implementation, we kindly request your authorisation to register your ICU to have access to COMET. COMET is hosted in Microsoft Azure. The COMET Privacy and Security Assessment document information is available at the ANZICS website.

I *(ICU Director)* _____ Authorise

Site *(Hospital)* _____to be setup in COMET ready for Data Collection.

I nominate _____as the Site Administrator who will be responsible for setting up other authorised end-users and ongoing user management.

Site Administrator's email _____ Contact No: _____

Signature _____ *(ICU Director)*

Date_____

COMET IMPLEMENTATION FORM FOR NEW SITES SUBMITTING DATA TO ANZICS CORE

To proceed with implementation, we kindly request your authorisation to register your ICU to have access to COMET. COMET is hosted in Microsoft Azure. The COMET Privacy and Security Assessment document information is available at the ANZICS website.

I *(ICU Director)* _____ Authorise

Site *(Hospital)* _____to be setup in COMET ready for Data Collection.

I nominate _____as the Site Administrator who will be responsible for setting up other authorised end-users and ongoing user management.

Site Administrator's email _____ Contact No: _____

Signature _____ *(ICU Director)*

Date_____

Registration to Contribute Data to New Data Sets or Specific Projects Using the COMET eCRF Functionality

COMET is the software that ANZICS will use for new data collections that may include extension to the current ANZICS ICU Registries or specific projects that have been approved through the CORE Management Committee. To proceed with implementation, we kindly request your authorisation to register your ICU to have access to COMET. COMET is hosted in Microsoft Azure. The COMET Privacy and Security Assessment document information is available at the ANZICS CORE website.

As an existing COMET user, this registration will be to authorise access to the specified Data Collection page.

As a non-COMET user for APD or ANZPIC, this registration is required following review of the COMET Privacy and Security\ Assessment document.

I *(ICU Director)* _____ Authorise

Site *(Hospital)* _____to be setup in COMET ready for Data Collection.

I nominate _____as the Site Administrator who will be responsible for setting up other authorised end-users and ongoing user management.

Site Administrator's email _____ Contact No: _____

☐ Tick if an existing COMET user

☐ Tick if not an existing COMET user

Signature _____ *(ICU Director)*

Date_____