AUSTRALIAN COMMISSION ON SAFETY AND QUALITY IN HEALTH CARE

Security compliance guideline

Australian Clinical Quality Registries

Final consultation draft

Version 1.5

October 2013

Final consultation draft

Version 1.5

October 2013

Document Control

Preparation

	Name	Title	Company	Date
Prepared:	Robyn Bailey	Senior Consultant	Business Aspect	04/03/12
	Sharon Sweeney	Senior Consultant	Business Aspect	
	Gil Carter	Principal Consultant	Business Aspect	
Reviewed	Brendon Taylor	Director	Business Aspect	05/03/12

Distribution

Version	Date	Organisation	Details
1.1	March 2012	ACSQHC	
1.2	May 2012	ACSQHC	
1.3	July 2012	ACSQHC website	Consultation draft
1.3	July 2012	NEHTA, Monash DEPM	Consultation draft for review
1.4	March 2013	ACSQHC website	Final consultation draft
1.5	October 2013	ACSQHC website	Final consultation draft

Revision History

Ver	Date	Author	Details	Changes
1.0	05/03/2012	Business Aspect	Client Draft	
1.1	16/03/2012	Business Aspect	Post review by ACQSHC and NEHTA	Various
1.2	11/05/2012	Business Aspect	Post review by ACQSHC	Various
1.3	23/05/2012	Business Aspect	Post review by ACQSHC	Various
1.4	March 2013	ACSQHC	Post review by NEHTA and ACQSHC	Multiple changes
1.5	October 2013	ACSQHC	Updated review by NEHTA and ACQSHC	Various

Contents

List of Tables

List of Figures

1. Introduction

This document provides a ‘consultation draft’ of the Clinical Quality Registry Security Compliance Guideline. The intention is to provide registry operators with a draft guideline to assist with the continuous assessment of the compliance of their registry and/or registry centre against a set of security standards.

The Australian Commission on Safety and Quality in Health Care welcomes feedback from users of this document on the guideline’s content, usability and effectiveness.

1.1. Purpose

The purpose of the *Security Compliance Guideline for Clinical Quality Registries* (the *Guideline*) is to outline a checklist approach for Australian clinical quality registries, operating either as standalone entities or co-located with other registries in centres of excellence, to be assessed and certified against a standardised methodology derived from accepted standards and techniques.

1.2. Intended audience

The *Guideline* is intended to be used by individuals and organisations wishing to assess the compliance of a new or established clinical quality registry against appropriate security standards and techniques.

1.3. About the *Guideline*

The *Guideline* builds on the work of the National eHealth Transition Authority’s National eHealth Security and Access Guideline (NESAF) which provides guidance to businesses engaged in electronic health (eHealth) on how to establish an information security infrastructure using a risk-based approach.

The *Guideline* has been developed in consultation with the Commission Clinical Quality Registries Advisory Group and a group of CQR experts from key Australian clinical quality registries.

Section 1.4 ‘National arrangements for clinical quality registries’, provides context for the development of the *Guideline* and outlines its importance and use under future national arrangements.

Section 2 ‘Considerations in Securing Clinical Quality Registries’ defines the key elements of information security and outlines some of the common threats to CQRs.

Section 3 ‘Infrastructure Models and Risk Profiles’ identifies two distinct infrastructure configurations or ‘models’, and risk profiles for clinical quality registries.

Section 4 ‘Security Assessment Approach’ describes a high-level approach to the assessment of CQR security compliance, including the measures to be taken to address any identified security gaps.

Section 5 ‘Security Compliance Checklists for CQR ‘Good Practice’’ provides the checklists to be used for the assessment of organisations requiring security certification. Each organisation is assessed across a number of key security domains for minimum ‘good practice’ requirements.

Section 6 ‘Detailed Guidance on Controls’ provides detailed guidance and explanation on each security control, categorised by security domain. The guidance provided is a blend of detail from relevant security guidelines and specific detail to suit CQR environments. The guidance provided borrows heavily from the National eHealth Security and Access Guideline and ISO/IEC 27002.

A description of clinical quality registries, including their core business functions and suggested architecture, is included in Appendix A.

1.4. National arrangements for clinical quality registries

In November 2010, Health Ministers noted that the Australian Commission on Safety and Quality in Health Care (the Commission) will draft national arrangements for clinical quality registries (CQRs). Accordingly, minimum requirements concerning data custodianship, reporting, security, assessment and accreditation are being drafted for CQRs under future national arrangements.

To augment national arrangements, the Commission is documenting the following technical resources for Australian clinical quality registries:

- Infrastructure and Technical Standards (version 2)
- Technical and Operating Requirements Specification
- Logical Architecture and Design
- Security Compliance Guideline (this document)

A key element of CQR operation under national arrangements is the appropriate treatment of information security, with suitable measures to manage the confidentiality, integrity and availability of information.

The *Security Compliance Guideline for Clinical Quality Registries* provides an approach for CQRs operating under national arrangements (and those operating outside national arrangements) to be assessed against a standardised methodology derived from accepted standards and techniques.

2. Considerations in Securing Clinical Quality Registries

This section sets out the context for information security for a clinical quality registry – key considerations such as confidentiality, integrity and availability. It discusses possible threats to a CQR, requirements to be managed and relevant influences from legislation. The content in this section has been refined in collaboration with key stakeholders.

2.1. Key elements of information security

The information held by CQR's is a core asset. The protection of this asset in terms of its confidentiality, integrity and availability is the focus of information security. These three key elements of information security are defined below1:

Confidentiality	Refers to ensuring that information is only accessible and available to those authorised to have access.
Integrity	Refers to being able to store, use, transfer and retrieve information with confidence that the information has not been tampered with or altered, other than through authorised transactions. Information integrity also contributes to the maintenance of confidentiality through the protection of access control data, audit trails and other system data that enable the identification of breaches in confidentiality.
Availability	Ensures that information is accessible to authorised individuals when and where it is required.

2.2. Common threats to information

Threats are not only capable of exploiting vulnerabilities in information systems, but also the vulnerabilities in the processes and people that support or use the information within those systems. Threats may come from internal or external sources. They may be accidental or deliberate, malicious or well intending. Threats may impact on each of the elements of information security individually or on all of the elements concurrently.

In general, the information contained within clinical quality registries is not required to be available on a time-critical basis to end users; for example, to clinicians for clinical decision-making purposes. This document therefore prioritises the security elements of *confidentiality* and *integrity* over the element of information *availability* for the protection of CQR information.

The process of identification, categorisation and assessment of threats to CQRs is an important part of this Guideline. In essence, a threat 'catalogue' lists the set of potential ways that the information and functions of a CQR may be compromised. The listing of threats in Table 1 (below) identifies a set of common threats and associated vulnerabilities that may exist within the CQR environment. Section 6 of this Guideline details the controls that will facilitate secure operation in an environment characterised by such threats.

[1] National E-Health Transition Authority. *National E-Health Security and Access Framework – Release 3*.

It is hoped that readers of this ‘consultation draft’ of the Guideline will participate in the on-going development of the Guideline by identifying and contributing threats that are additional to those listed in Table 1.

Table 1: Sample threats to CQRs

Threat Category	Threat	Example Vulnerabilities	Example Potential Consequences
Deliberate	Denial of Service	Inappropriate securing of external connections (internet or other third parties) Inadequate network management Lack of OS update management, leading to exploitation Lack of alerting and incident response processes	Loss of availability
	Eavesdropping	Unencrypted communications over public networks Lack of physical security over data communications equipment Inappropriate network configuration, i.e. shared Ethernet broadcast traffic to any machine	Loss of confidentiality
	Fire	Lack of physical security Lack of fire detection devices Lack of fire suppression devices	Loss of availability
	Malicious Code	Lack of anti-virus software Lack of anti-virus software update processes Inadequate staff awareness and education on virus issues Lack of Security policy Uncontrolled downloading and use of files off the Internet	Loss of integrity Loss of availability
	Malicious destruction of data and facilities	Lack of physical security Lack of logical access control leading to damage to / deletion of data Lack of processes to ensure terminated employees accounts are disabled from system access	Loss of availability Loss of integrity
	Masquerade	Lack of identification and authentication mechanisms Unprotected passwords Lack of identification of sender and receiver	Loss of confidentiality Loss of integrity
	Social Engineering	Lack of security policy Lack of awareness of staff allowing unauthorised people into QIC premises or giving information over the phone	Loss of integrity Loss of availability Loss of confidentiality
	Repudiation	Lack of proof of sending or receiving a message Lack of digital signatures	Loss of integrity
	Sabotage	Lack of physical security Lack of logical access controls Lack of change management Inappropriate access controls	Loss of integrity Loss of availability

Threat Category	Threat	Example Vulnerabilities	Example Potential Consequences
	Theft & Fraud	Lack of physical security Lack of application integrity controls Lack of authentication Lack of access controls Lack of change management	Loss of integrity Loss of confidentiality
	Unauthorised Physical Access	Lack of physical security controls Poor awareness of 'shoulder surfing' risk Lack of monitoring	Loss of integrity Loss of availability Loss of confidentiality
	Unauthorised Data Access	Lack of logical access controls Inability to authenticate requests for information Transmission of unencrypted confidential data Lack of physical security over communications equipment	Loss of integrity Loss of confidentiality
	Unauthorised Software changes	Lack of change management policy and procedures Lack of appropriate change control system Inadequate segregation of duties between developer and operations staff Inadequate reporting and handling of software malfunctions Lack of backups	Loss of integrity Loss of availability
	Website Intrusion	Lack of Perimeter network defences Inappropriate firewall rules / access controls Lack of system hardening Lack of processes to install OS and application security fixes Inadequate software development standards	Loss of integrity Loss of availability
Environmental	Natural Disaster Earthquake Fire Flood Storm	Location in an area susceptible to threat Lack of back-up processes Back-up media not available Lack of BCP or procedures for recovery of data and IT Lack of detection devices and monitoring Lack of appropriate fire suppression mechanism	Loss of availability
	Environmental Conditions Contamination Electronic interference Extremes of Temperature & humidity Failure of Power Supply Power Fluctuations	Location in an area susceptible to threat Lack of maintenance of equipment and facilities Lack of detection devices and monitoring Lack of back-up processes Back-up media not available Lack of BCP or procedures for recovery of data and IT Lack of UPS Lack of Power Conditioning equipment	Loss of availability
Accidental	Fire	Location in an area susceptible to fire Inadequate physical access control to buildings Lack of fire detection systems Lack of fire suppression systems Lack of BCP and DRP Lack of backup	Loss of availability

Threat Category	Threat	Example Vulnerabilities	Example Potential Consequences
	Failure of communications services	Lack of redundancy and backup Inadequate network management Lack of planning and implementation of communications cabling Inadequate incident handling Lack of service levels with external communications providers	Loss of availability
	Failure of outsourced operations	Unclear obligations in outsource agreements Lack of BCP and DRP Lack of backup	Loss of availability
	Loss or absence of key personnel	No backup staff Lack of cross-training Undocumented procedures Lack of succession planning	Loss of availability
	Misrouting / re-routing of messages	Sensitive data not encrypted Lack of verification of message receipt Mis-configured networks	Loss of availability Loss of confidentiality Loss of integrity
	User Error	Lack of user awareness Lack of user training Lack of documentation Inappropriate management of changes to information systems Complicated user interface	Loss of availability Loss of integrity
	Software / Programming Error	Inadequate system development lifecycle process and procedures Unclear or incomplete system specification Lack of change management Lack of policy Unskilled staff	Loss of availability Loss of confidentiality Loss of integrity
	Technical Failure	Lack of Environmental controls Lack of user awareness Inadequate maintenance of hardware Lack of backup facilities or processes Lack of network capacity through improper planning or maintenance Failure of change management processes Lack of BCP or DRP	Loss of availability
	Transmission Error	Inappropriate cabling Inadequate incident handling Lack of backup facilities or processes Lack of BCP or DRP	Loss of availability

Source reference: ISO 27799

2.3. Legislation and Regulation

Detailed coverage of information privacy from a legislative perspective is out of scope for this Guideline. However, it is important to note that Australia presently has a range of different legislation, regulation, principles and policies covering privacy of personal health information. The variance extends across the different health jurisdictions including the Commonwealth and the ACT, the States and the Northern Territory, and the private health sector.

Commonwealth Government agencies and ACT Government agencies are covered under the *Privacy Act 1988*[2] and subject Section 95 to Information Privacy Principles. *Guidelines under Section 95 of the Privacy Act 1988 state* "security standards [are] to be applied to the personal information…in a form that is at least as secure as it was in the sources from which the personal information was obtained." Additionally, Information Privacy Principle 4 is concerned with the storage and security of personal information.

Organisations in the private health sector are also covered by the *Privacy Act 1988* but are subject to Section 95A and the National Privacy Principles. National Privacy Principle 4 is specifically concerned with data security.

The States and the Northern Territory are subject to varying legislative Acts, regulations, privacy principles and policies. For up-to-date information on privacy law in the States and the Northern Territory, refer to the Office of the Australian Information Privacy Commission[3].

In addition to taking appropriate measures to adequately secure information held in CQRs, it is recommended that operators of registries seek additional advice about the privacy issues that may affect the information that they hold.

2.4. Approaches to managing risk

The approach to managing security risk can take a range of forms, and it may not be practical for an organisation to address all identified risks. Priority should be given to those threats and associated vulnerabilities that have the highest likelihood of compromising the confidentiality, integrity and availability of healthcare information and those that have the potential for greatest impact on the CQR and its information, should a compromise be realised.

Risk management options[4] can include:

- Risk avoidance – risk is avoided by deciding not to start or continue with the activity that would cause the risk.
- Risk acceptance – accept the potential risk, but put plans in place to manage the consequences of the risk should it occur.
- Changing the likelihood – through implementation of controls and preventative actions e.g. audit and compliance programs, contract conditions, policies and procedures, testing.
- Changing the consequences – through implementation of controls such as business continuity management, disaster recovery, back-up, emergency procedures, to reduce the consequences of the risk occurring.
- Risk transfer – sharing the risk with another party or parties e.g. through the use of contracts, insurance, outsourcing arrangements.

When selecting an approach and controls to manage risk, there is a balance to be struck between mitigating the risk, and the time, effort and resources required to mitigate against the risk. Figure 1 illustrates the trade-off that organisations should consider in relation to selecting and implementing appropriate controls.

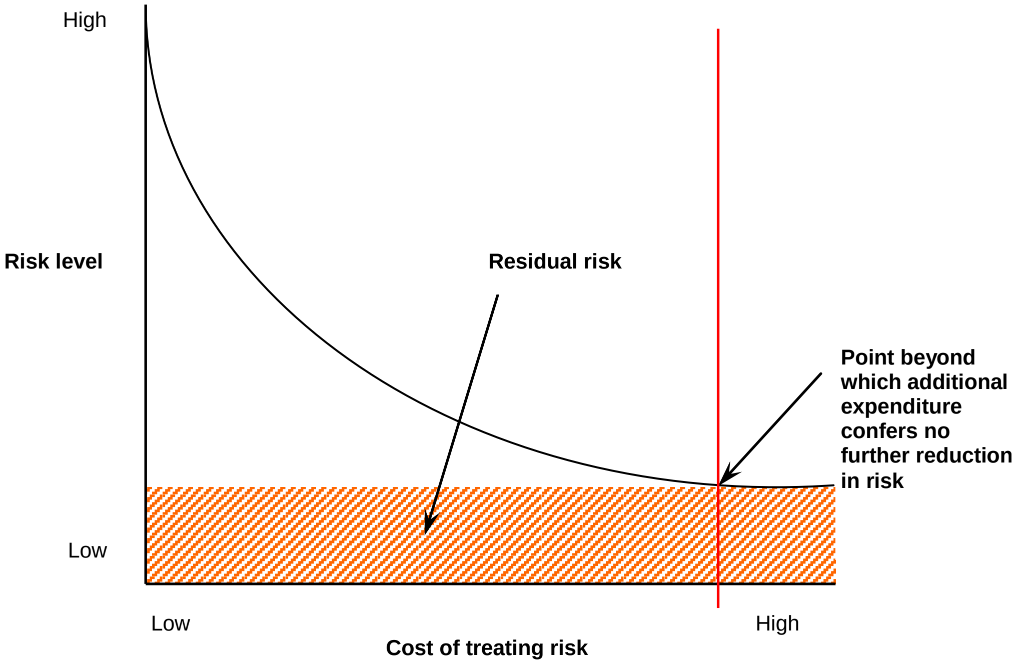
[2] http://www.oaic.gov.au/privacy/privacy-act/the-privacy-act

[3] http://www.oaic.gov.au/privacy/other-privacy-jurisdictions/state-and-territory-privacy-law

[4] Source: NESAF Business Blueprint, NEHTA 2011

The costs of implementing controls must be justified by the reduction in the level of risk or assessed against the risks associated with not implementing the control. Almost no information system is risk free and not all implemented controls can completely eliminate the risk they are intended to address, or reduce the risk level to zero. The risk remaining after implementing new controls is the residual risk.

Figure 1: Cost-benefit trade-off – risk treatment options



In developing the *Guideline*, a check-list approach for managing CQR risks has been used (Section 4 Security Assessment Approach). This approach stipulates specific measures to be used that can treat, to a particular level, the identified risks.

As highlighted in the figure above, residual risk cannot be completely removed. However, the application of the recommended controls can provide an appropriate level of risk treatment to the key areas for a CQR.

3. Infrastructure Models and Risk Profiles

To assist in assessing security risks for CQR's, two distinct infrastructure configurations or 'models', and risk profiles have been identified.

3.1. Infrastructure Models

This *Guideline* may be used to assess Australian clinical quality CQRs operating in either of two organisational 'models', depending on whether or not they are co-located with other CQRs in a centre of excellence.

3.1.1. Model 1 - Centres of Excellence

Model 1 identifies a situation in which a number of CQRs are co-located within a centre of excellence. The centre may be responsible for the implementation, development, management and operation of each of the CQRs. The specific functions of a centre of excellence may include the responsibility for the business functions of each CQR (in accordance with the directions set by the relevant board/governance arrangements for each CQR); recruitment and management of CQR staff; technical application development; support and maintenance.

Under future national arrangements, centres of excellence would employ a standardised approach to the hosting and development of the CQRs housed within them. Such an approach may involve the development and deployment of internal technical infrastructure ('data hosting platform') - see Figure 2. Alternatively, the technical infrastructure for the CQRs could be housed with an external data hosting provider (

Figure 3). The approach may vary from centre to centre.

This *Guideline* assumes that centres of excellence will be subject to greater inherent security risk than stand-alone CQRs. Larger CQR entities pose a bigger target for potential threats and carry a greater absolute risk of compromised security (see Section 3.2 Risk).

Model 1 - Centres of Excellence

Figure 2: Centre of excellence with an internal data hosting platform

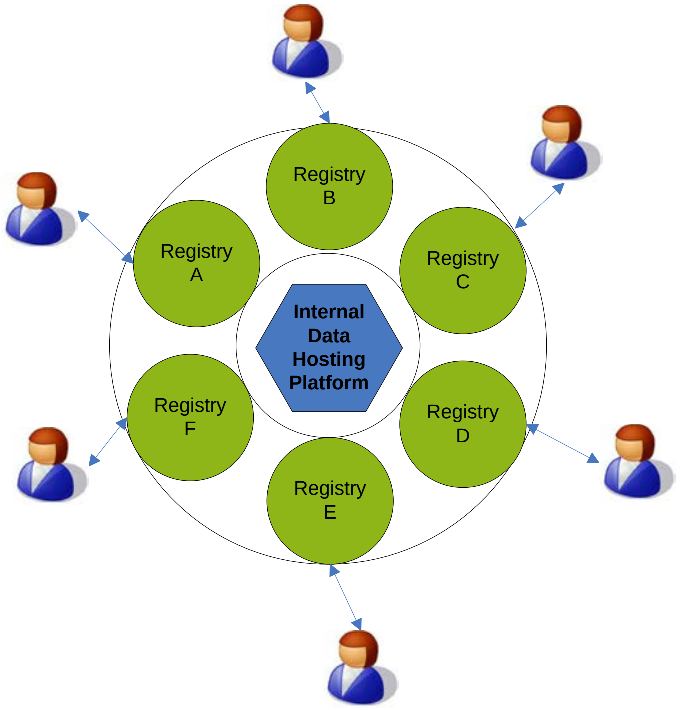
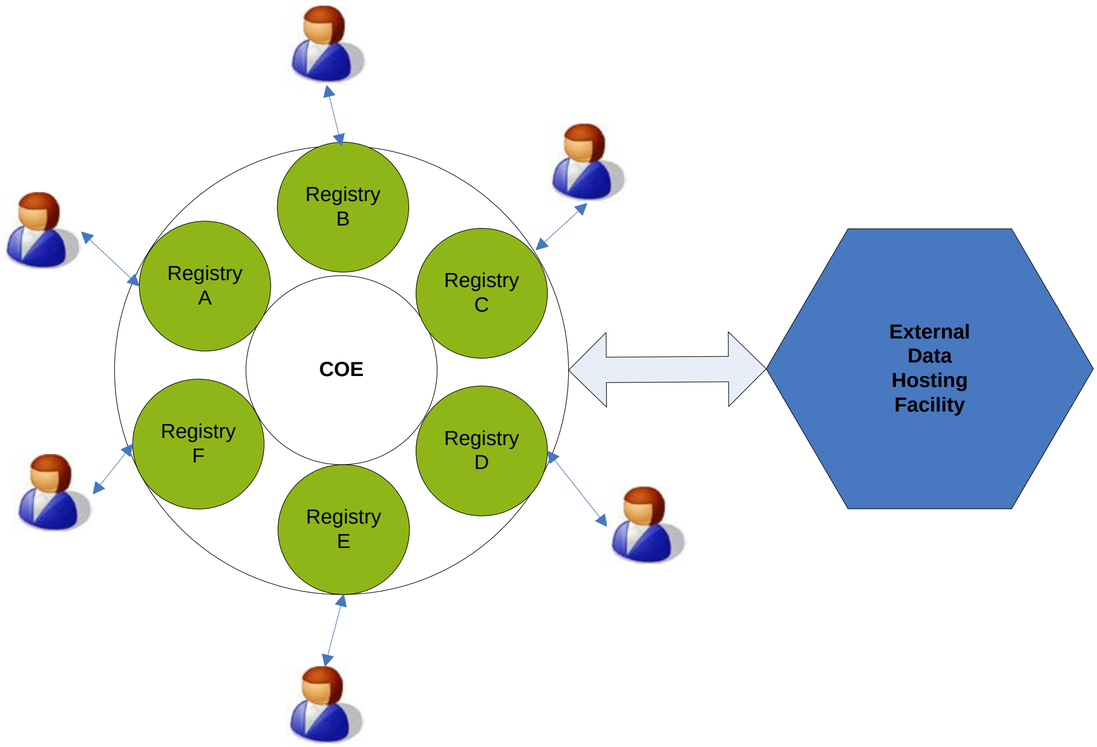


Figure 3: Centre of excellence using an external data hosting facility



3.1.2. Model 2 - Standalone CQR

Model 2 describes the situation in which a CQR is developed and operated individually and separately. The CQR may have a technology infrastructure (‘data hosting’) platform that is hosted locally and maintained internally by CQR staff (Figure 4) or externally through a third party service provider (Figure 5).

This *Guideline* assumes that stand-alone CQRs carry a lower inherent security risk than CQRs operating in centres of excellence. Smaller CQR entities pose a smaller target for potential threats and carry a smaller absolute risk of compromised security (see Section 3.2 Risk).

Figure 4: Standalone CQR with an internal data hosting platform

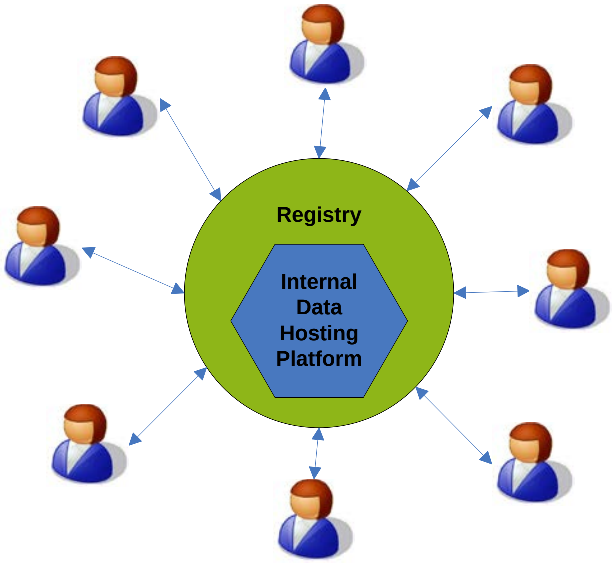
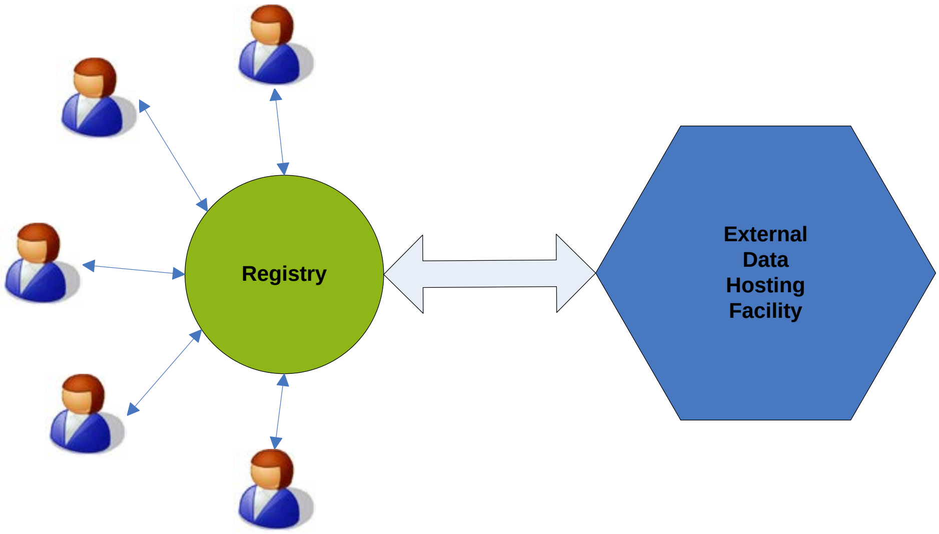


Figure 5: Standalone CQR using an external data hosting facility



3.2. Risk Profiles

This section describes the risk profiles for the two infrastructure models described in Section 3.1, and how those profiles have been determined.

The risk profiles have been used to develop the Security Compliance Checklists (Section 5 Security Compliance Checklists for CQR ‘Good Practice’).

3.2.1. Summary of Risk Profiles

The following table summarises the risk profiles for each of the infrastructure models.

Overall, of most concern to CQRs are security breaches of confidentiality and integrity of CQR information. Breaches of availability are less of a concern as the information produced by CQRs is not usually required for time-critical use; that is, for the delivery of clinical care.

Table 2: Risk profiles

Profile	Infrastructure Model Type	Number of CQRs	Inherent Risk		
			Inherent Confidentiality Risk	Inherent Integrity Risk	Inherent Availability Risk
1	Centre of excellence	Multiple	High	Medium	Medium
2	Standalone CQR	Single	Medium	Medium	Low

3.2.2. Risk profile for centres of excellence

Table 3 outlines the nature and extent of information security risks associated with centres of excellence (refer to Model 1 in Section 3.1). Generally, centre of excellence environments will have a lower tolerance for risk than standalone CQR environments and it is expected that better controls will be implemented.

The ‘security domains’ indicated in Table 3 are reflected in the security compliance checklists in Section 5.

Table 3: Centres of excellence risk profile

No.	Factor	Risk	Likelihood	Impact	Risk	Security Domain
1	Confidentiality	Loss of confidentiality of multiple records due to staff accidentally disclosing information leads to loss of privacy, embarrassment for the CQR and/or financial penalties	Unlikely	Major	High	Information Security Policy; HR Security
2	Confidentiality	Accidental breach of legislation (by Centre of excellence (CoE) staff) due to CoE's managing multiple jurisdictions	Unlikely	Major	High	Access Control; Compliance
3	Confidentiality	Loss of confidentiality of information due to staff or contractors purposely disclosing health information (likelihood is increased in CoE)	Unlikely	Major	High	Information Security Policy; HR Security; Information Security Organisation
4	Confidentiality	Changing to new CoE environment may put information at additional risk due to the difficulties in identifying users	Possible	Moderate	High	Information Security Policy; Information Security Organisation
5	Confidentiality	Loss of confidentiality of info. whilst in transit externally (e.g. from data suppliers)	Possible	Moderate	High	Communications and Operations Management
6	Confidentiality	Portable devices may store confidential information, which may then be left in public areas or stolen, leading to breach of confidentiality of multiple records	Unlikely	Major	High	HR Security; Communications and Operations Management
7	Confidentiality	Breach of legislation due to information that is used in a manner that is not in accordance with the purpose for which it has been collected (eg: violation of consent).	Unlikely	Moderate	Medium	Compliance; HR Security
8	Confidentiality	Theft of (non-portable) information systems containing multiple records of confidential information	Unlikely	Major	High	Physical Security

No.	Factor	Risk	Likelihood	Impact	Risk	Security Domain
9	Confidentiality	Authorised user inadvertently gives information to unauthorised user	Possible	Moderate	High	HR Security;
10	Integrity	Data integrity errors in bulk upload / external file transfers	Unlikely	Major	High	Information Systems Acquisition; Development and Maintenance
11	Integrity	Individual record data quality errors through data entry (transposition)	Possible	Minor	Medium	Information Systems Acquisition, Development and Maintenance; HR Security
12	Integrity	Malicious staff purposely change multiple records	Unlikely	Major	High	HR Security; Communications and Operations Management; Access Control
13	Integrity	Untrained/unskilled staff accidentally change multiple records	Unlikely	Moderate	Medium	HR Security; Access Control
14	Integrity	Database errors due to environmental factors (e.g. Loss of power causes system failure which corrupts database)	Unlikely	Moderate	Medium	Business Continuity Management; Physical Security
15	Integrity	Message received or sent from unauthorised party	Unlikely	Moderate	Medium	Access Control; Communications and Operations Management
16	Integrity/Availability	Malware/viruses resulting in loss of availability/integrity of multiple records	Unlikely	Major	High	Communications and Operations Management; Incident Management
17	Integrity	Incompatibility between data and metadata/reference tables - get out of sync over time - backwards incompatibility causing loss of integrity of many records	Unlikely	Moderate	Medium	Information Systems Acquisition, Development and Maintenance
18	Integrity	Application errors - e.g. Store dates in US format lead to multiple records becoming corrupt	Unlikely	Moderate	Medium	Information Systems Acquisition, Development and Maintenance
19	Availability	Power or other environmental issues lead to CQR becoming unavailable for more than a day	Unlikely	Moderate	Medium	Business Continuity Management; Physical Security
20	Availability	Denial of service attacks through external services (malicious or accidental)	Unlikely	Moderate	Medium	Communications and

No.	Factor	Risk	Likelihood	Impact	Risk	Security Domain
						Operations Management; Incident Management
21	Availability	Infrastructure capacity issues – e.g. low server RAM/HDD etc	Unlikely	Moderate	Medium	Communications and Operations Management;
22	Availability	Unauthorised software/hardware changes causes outages beyond acceptable period	Unlikely	Moderate	Medium	Communications and Operations Management;
23	Availability	User accidentally causes environmental issues - turns off server; spills liquid etc	Unlikely	Moderate	Medium	HR Security; Physical Security
24	Availability	Vendor fails to meet SLA for availability	Unlikely	Moderate	Medium	Information Security Organisation
25	Availability	Loss of small number of records due to reluctance by contributors to re-enter/re-provide data following loss of availability or other factors	Unlikely	Moderate	Medium	HR Security

3.2.3. Risk profile for a standalone CQR

Table 4 outlines the nature and extent of information security risks associated with a standalone CQR that may have locally hosted data or externally hosted data environments (refer to Model 2 in Section 3.1.2). Generally, these environments will have a higher tolerance for risk and lower susceptibility to threats.

The 'security domains' indicated in Table 4 are reflected in the security compliance checklists in Section 5.

Table 4: Standalone CQR risk profile

No.	Factor	Risk	Likelihood	Impact	Risk	Security Domain
1	Confidentiality	Loss of confidentiality of multiple records due to staff accidentally disclosing information	Possible	Moderate	High	Information Security Policy; HR Security
2	Confidentiality	Accidental breach of legislation (by admin staff) due to managing multiple jurisdictions leads to embarrassment or financial penalty	Unlikely	Moderate	Medium	Access Control; Compliance
3	Confidentiality	Loss of confidentiality of information due to staff or contractors purposely disclosing information	Unlikely	Moderate	Medium	Information Security Policy; HR Security; Information security Organisation
5	Confidentiality	Loss of confidentiality of info. whilst in transit externally (e.g. from data suppliers or to external hosting environment)	Possible	Moderate	High	Communications and Operations Management
6	Confidentiality	Portable devices may store confidential information, which may then be left in public areas or stolen, leading to breach of confidentiality of multiple records	Possible	Moderate	High	HR Security; Communications and Operations Management
7	Confidentiality	Breach of legislation due to Information used not in accordance with the purpose for which it has been collected (eg: violation of consent)	Unlikely	Moderate	Medium	Compliance; HR Security
8	Confidentiality	Theft of (non-portable) information systems containing confidential information	Unlikely	Moderate	Medium	Physical Security

No.	Factor	Risk	Likelihood	Impact	Risk	Security Domain
9	Confidentiality	Authorised user inadvertently gives information to unauthorised user	Unlikely	Moderate	Medium	HR Security;
10	Integrity	Data integrity errors in bulk upload / external file transfers	Possible	Moderate	High	Information Systems Acquisition, Development and Maintenance
11	Integrity	Data quality errors through data entry from data entry person (transposition)	Unlikely	Insignificant	Low	Information Systems Acquisition, Development and Maintenance; HR Security
12	Integrity	Malicious staff purposely change multiple records	Unlikely	Moderate	Medium	HR Security; Communications and Operations Management; Access Control
13	Integrity	Untrained/unskilled staff accidentally change multiple records	Unlikely	Moderate	Medium	HR Security; Access Control
14	Integrity	Database errors due to environmental factors (e.g. Loss of power causes system failure which corrupts database)	Unlikely	Moderate	Medium	Business Continuity Management; Physical Security
15	Integrity	Message received or sent from unauthorised party	Unlikely	Moderate	Medium	Access Control; Communications and Operations Management
16	Integrity/Availability	Malware/viruses resulting in loss of availability/integrity of multiple records	Unlikely	Major	High	Communications and Operations Management; Incident Management
17	Integrity	Incompatibility between data and metadata/reference tables - get out of sync over time - backwards incompatibility	Unlikely	Moderate	Medium	Information Systems Acquisition, Development and Maintenance
18	Integrity	Application errors - e.g. Store dates in US format lead to multiple records becoming corrupt	Unlikely	Moderate	Medium	Information Systems Acquisition, Development and Maintenance

No.	Factor	Risk	Likelihood	Impact	Risk	Security Domain
19	Availability	Power or other environmental issues lead to one or more CQRs becoming unavailable for more than a day	Possible	Minor	Medium	Business Continuity Management; Physical Security
20	Availability	Denial of service attacks through external services (malicious or accidental)	Unlikely	Minor	Low	Communications and Operations Management; Incident Management
21	Availability	Infrastructure capacity issues - e.g. low server RAM/HDD etc	Unlikely	Minor	Low	Communications and Operations Management;
22	Availability	Unauthorised software/hardware changes causes outages beyond acceptable period	Unlikely	Minor	Low	Communications and Operations Management;
23	Availability	User accidentally causes environmental issues - turns of server; spills liquid etc	Unlikely	Minor	Low	HR Security; Physical Security
24	Availability	Vendor fails to meet SLA	Unlikely	Minor	Low	Information Security Organisation
25	Availability	Loss of small number of records due to reluctance by contributors to re-enter/re-provide data following loss of availability or other factors	Possible	Insignificant	Low	HR Security

4. Security Assessment Approach

This section describes a high-level approach to the assessment of CQR security compliance, including the measures to be taken to address any identified security gaps.

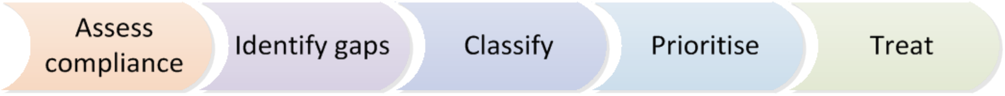
To assess security compliance, assessors should first identify the checklists that are applicable to the organisation being assessed.

4.1. Methodology

A checklist approach is employed to assess the security compliance of CQRs. Each area of the checklist is tested against the local CQR environment to assess compliance.

Gaps in compliance are identified, classified in importance, prioritised for action, and finally treated.

The chart below shows these steps in the methodology.



4.2. Assessing Compliance

4.2.1. Assessment checklists

Based on the infrastructure models (Section 3.1) and risk profiles (Section 3.2), this Guideline identifies three separate checklists:

1. CQR Business Operations Checklist
2. Standalone CQR - Local Data Hosting Checklist
3. Centre of Excellence (CoE) and External Data Hosting Checklist

The CQR Business Operations Checklist is used to identify the current status of security controls concerning the business operations of a CQR. This includes, but is not limited to, employment screening controls, authorisation of users and business continuity practices. Regardless of the underlying data hosting infrastructure of each CQR, these business operation security controls should be similar across all CQRs and hence the same level of security state is required.

The Standalone CQR – Local Data Hosting Checklist is used by standalone CQRs which operate and maintain their own data hosting infrastructure.

The CoE and External Data Hosting Checklist is used to assess centres of excellence AND other external data hosting service providers, where ISO 27001 or Australian Signals Directorate (ASD) certification does not exist.

Formally accredited by authorised certifiers, ISO 27001 is the international standard for information security management and, where satisfied, provides a high level of confidence in an organisation's security control measures. Similarly, ASD certification (formerly DSD) evaluates ICT security products used by Australian governments to protect official information. These formal independent assessments provide confidence that ICT security products perform as claimed by the vendor.

It is expected, however, that few organisations within Australia will have ISO 27001 or ASD certification, in which case the CoE or External Hosting Checklist should be used. This checklist involves best practice controls for securing CQR information within a centre of excellence or external data hosting service provider and requires an annual review.

Once an organisation becomes certified, all future CQRs may outsource their data hosting requirements to the certified provider, without further certification. It is expected however, that annual reviews of compliance are undertaken by the external data hosting service provider. Reports of annual compliance reviews should be provided to the CQRs for which data hosting services are being provided.

4.2.2. Determining the appropriate checklists

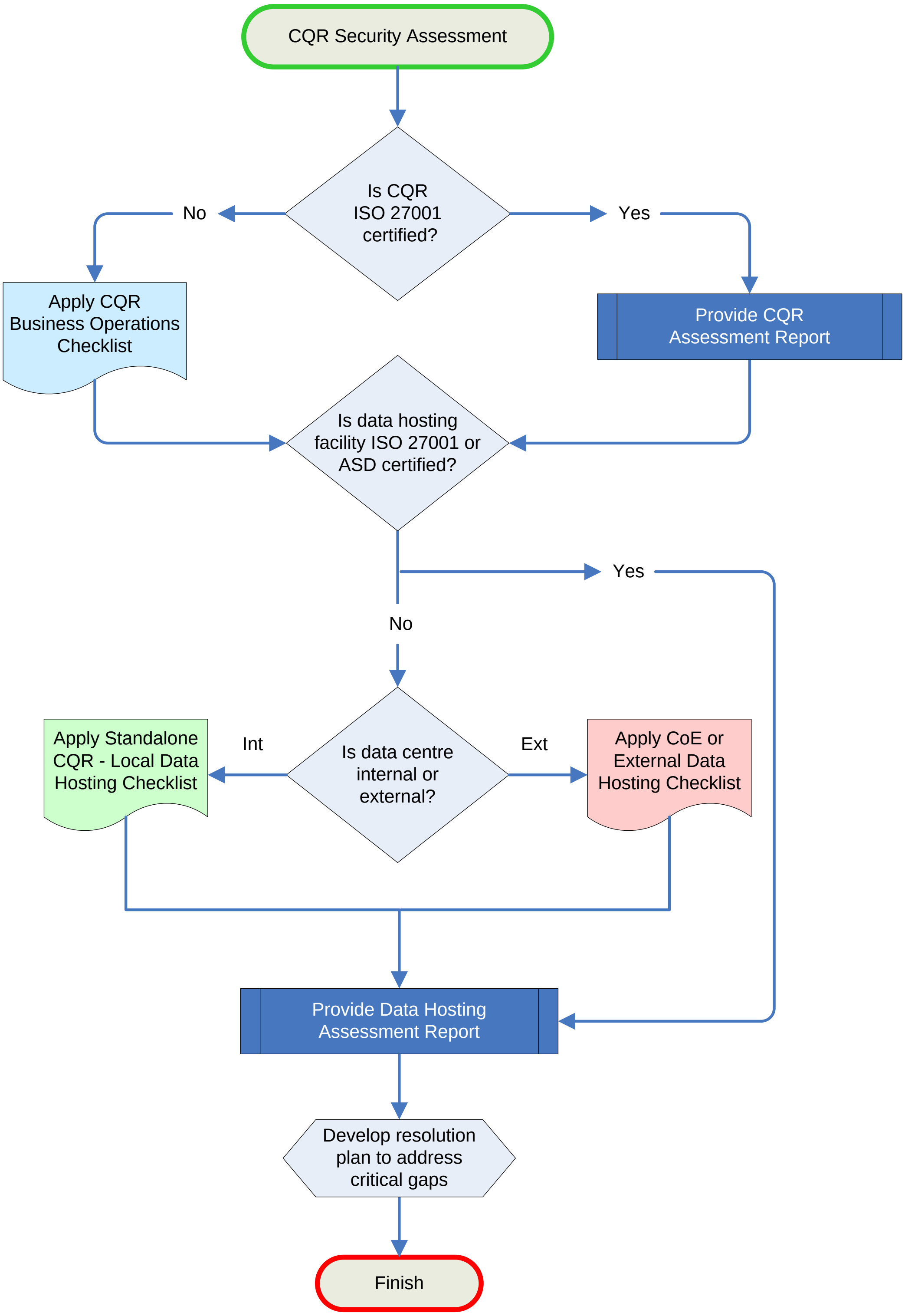
The flowchart (Figure 6) and matrix (Table 5) below should be used to determine the appropriate checklists to be used to assess an organisation's security control measures based on the two organisational infrastructure models outlined in Section 3.1:

1. Centres of excellence
2. Standalone CQRs

-- this section continued over ---------------------------------------

Figure 6: Flowchart for determining the appropriate assessment checklists

The flowchart complements Table 5: Matrix for determining the appropriate assessment checklists.


CQR Security Assessment
Is CQR ISO 27001 certified?
No
Yes
Apply CQR Business Operations Checklist
Provide CQR Assessment Report
Is data hosting facility ISO 27001 or ASD certified?
Yes
No
Int
Ext
Apply Standalone CQR - Local Data Hosting Checklist
Is data centre internal or external?
Apply CoE or External Data Hosting Checklist
Provide Data Hosting Assessment Report
Develop resolution plan to address critical gaps
Finish

CQR = Clinical Quality Registry

ISO 27001 = Information Security Management System standard

ASD = Australian Signals Directorate

Table 5: Matrix for determining the appropriate assessment checklists

The matrix complements Figure 6: Flowchart for determining the appropriate assessment checklists .

The organisation being assessed is a …	**The certification checklist(s) that the organisation needs to complete is (are)…**			
	CQR Business Operations Checklist	**Standalone CQR Local Data Hosting Checklist**	**CoE or External Data Hosting Checklist**	**Other**
Standalone CQR with an internal data hosting platform (all data and applications are hosted and maintained by CQR staff). (Refer to Figure 4).	✓	✓		
Centre of excellence that hosts information for multiple CQRs. (Refer to Figure 2).	✓ (per CQR)		✓	
Standalone CQR using an external data hosting provider (eg Cloud provider) that DOES NOT have ISO 27001 certification. (Refer to Figure 5).	✓		✓ CQR is responsible for ensuring the external provider complies.	
Standalone CQR using an external data hosting provider (eg Cloud provider) that DOES have ISO 27001 certification. (Refer to Figure 5).	✓			✓ Proof of certification to be sighted by CQR
Centre of excellence that uses an external data hosting provider who does not have ISO 27001 certification. (Refer to Figure 3)	✓ (per CQR)		✓ CQR is responsible for ensuring the external provider complies.	
Centre of excellence that uses an external data hosting provider that does have ISO 27001 certification. (Refer to Figure 3).	✓			✓ Proof of certification to be sighted by Centre of excellence
Centre of excellence that has previously attained certification using the CoE or External Data Hosting Checklist, and another CQR wishes to join the CoE (ie use the existing CoE services).	✓ (per CQR)		Not required - already certified once.	

4.3. Identify Gaps

Following assessment of compliance, identification of security control gaps may be undertaken. Areas that are noted as not meeting good practice should be recorded as security control gaps.

4.4. Classifying and prioritising gaps

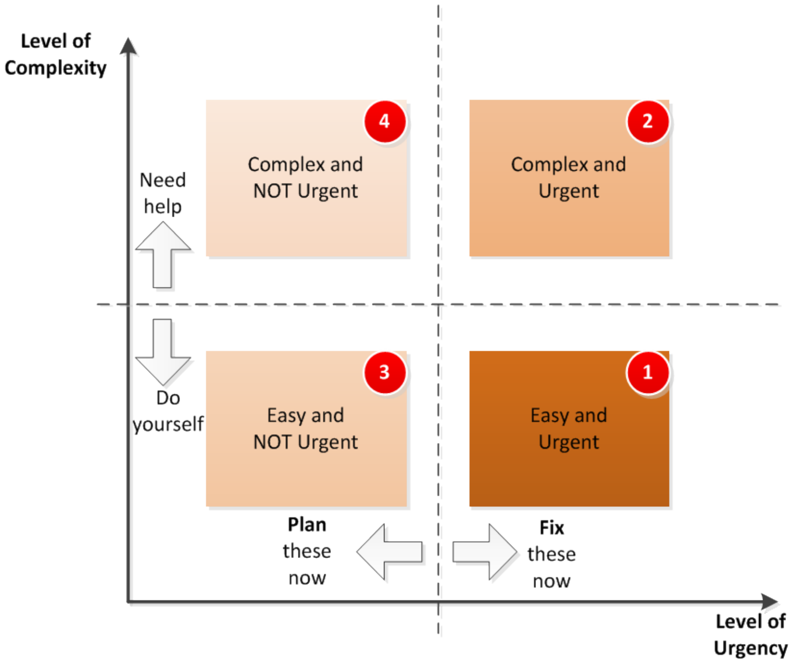
Once a security control gap has been identified, the next stage is to classify the importance of the gap in terms of urgency and complexity. Classification of security gaps provides a logical hierarchy of prioritisation for gap remediation work.

Level of urgency is based on the potential impact if a security gap or weakness was to be exploited. In other words, *the level of urgency should be measured by the level of risk that is being mitigated by the control (as referenced in the appropriate risk assessment).*

The level of complexity is measured by the expected effort and expertise required to implement a control.

The numbered quadrants in Figure 7 suggest a simple approach to prioritising any remediation work that may be needed. Any work that is urgent but simple should be top priority, and may be possible to undertake with in-house capabilities.

Figure 7: Classifying and prioritising gaps



4.5. Treat

Treatment of identified security gaps is the implementation of the required controls identified in the appropriate checklist. Clinical quality registries and external data hosting service providers should plan for the remediation of any gap areas on a priority basis as determined through the process above.

Section 6 of this Guideline contains detailed guidance on best practice controls. Other guidelines such as NESAF have a broader body of detailed information that can be used to inform the treatment of gap areas.

5. Security Compliance Checklists for CQR ‘Good Practice’

This section provides detailed checklists to be used for the assessment of organisations requiring security certification. Each organisation is assessed across a number of key security domains for minimum ‘good practice’ requirements.

Best Practice: Measures of ‘best practice’ are not included in the checklists. However, Section 6 of this Guideline provides measures of best practice for clinical quality registries in the form of detailed guidance on controls.

The checklists below should be used in accordance with the methodology and flowchart provided in Section 4.

5.1. Compliance Checklist – CQR Business Operations

To be completed by each CQR.

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Good Practice	Complies?	Date
Information Security Policy	A.1	Information security policy	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	6.1.1	Information security policy is documented.		
Information Security Organisation	B.1	Internal Organisation	To manage information security within the organisation.	6.2.1	Management are involved and interested in information security and conduct some informal discussions around information security. Some staff are aware of their information security responsibilities.		
Information Security Organisation	B.2	Third Parties	To maintain the security of the organisation's information and information processing facilities that are accessed processed, communicated to, or managed by third parties.	6.2.2	Some additional supervision of third parties is given on premises. Third parties are sign informal agreements.		

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Good Practice	Complies?	Date
Asset Management	C.1	Responsibility for health information assets	To achieve and maintain appropriate protection of organisational assets.	6.3.1	There is a designated owner or custodian of CQR information.		
Asset Management	C.2	Health information classification	To ensure that information receives an appropriate level of protection.	6.3.2	Staff are aware of what constitutes "confidential" information. Staff do not use identifiable private information for testing or any other purpose beyond which the information was intended.		
HR Security	D.1	Prior to employment	To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.	6.4.1	New employee's references and resumes are checked prior to employment.		
HR Security	D.2	During employment	To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.	6.4.2	Staff are made aware (on induction and at least annually) of the organisations information security policies and educated appropriately.		
HR Security	D.3	Termination or change to employment	To ensure that employees, contractors and third party users exit an organisation or change employment in an orderly manner.	6.4.3	User accounts are terminated after termination of employment or other change of employment status.		

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Good Practice	Complies?	Date
Communications and Operations Management	F.2	Third party Service Delivery Management	To implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements.	6.6.2	Service Level Agreements (SLA)'s are in place between CQRs and external data hosting infrastructure providers.		
Communications and Operations Management	F.4	Protection against Malicious and mobile code	To protect the integrity of software and information.	6.6.4	Antivirus software is installed on all servers, PC's and mobile devices and updates are installed as soon as possible. Staff know what to do if a virus is found.		
Communications and Operations Management	F.7	Media handling	To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.	6.6.7	CQRs have determined and documented a policy on the use of removable media and staff are aware of its contents.		
Communications and Operations Management	F.9	Electronic health information services	To ensure the security of electronic health information services, and their secure use.	6.6.9	There is a repeatable process to publish information electronically to external users which requires an approval path.		
Access Control	G.1	Requirements for access control in health	To control access to information.	6.7.1	CQR management have determined its policy on access control, including user roles (e.g. Statisticians) and the information that each role can access (e.g. statistical information).		
Access Control	G.3	User Responsibilities	To prevent unauthorised user access, and compromise or theft of information and information processing facilities.	6.7.3	Users Responsibilities for information security are documented and followed.		

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Good Practice	Complies?	Date
Access Control	G.4	Network access control and operating system access control	To prevent unauthorised access to networked services.	6.7.4	Internal access to the wired network requires authorisation. Internal access to the wireless network requires authorisation and a minimum of WPA2 with pre-shared key. External and remote access to the internal network requires authorisation and username/password authentication. Where infrastructure is shared with another organisation, CQR networks should be segregated from others. All users have unique identifiers. Passwords are enforced as a minimum of 8 characters with a combination of letters, numbers and special characters.		
Access Control	G.6	Mobile computing and teleworking	To ensure information security when using mobile computing and teleworking facilities.	6.7.6	Documented policy on the use of mobile devices and staff understand the contents.		
Information Systems Acquisition, Development and Maintenance	H.1	Security requirements of information systems	To ensure that security is an integral part of information systems.	6.8.1	Requirements for security controls are assessed for all new systems.		
Incident Management	I.1	Reporting information security events and weaknesses	To ensure that information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.	6.9.1	There is documentation for staff explaining how to identify and report suspected security events or weaknesses.		
Incident Management	I.2	Management of incidents and improvements	To ensure a consistent and effective approach is applied to the management of information security incidents.	6.9.2	At least one staff member has been assigned to co-ordinate the response to security incidents. This role has a repeatable process for responding which includes seeking specialist advice.		

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Good Practice	Complies?	Date
Business Continuity Management	J.1	Including information security in the business continuity management process	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.	6.10.1	A Business Continuity Plan has been developed. IT Disaster Recovery plans or procedures exist.		
Compliance	K.1	General	Establish a graduated compliance auditing guideline.	6.11.1	Information security environment is self-assessed for compliance.		
Compliance	K.2	Compliance with legal requirements	To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.	6.11.2	Legislative requirements (state and federal) for information security have been identified.		
Compliance	K.3	Compliance with security policies and standards and technical compliance	To ensure compliance of systems with organisational security policies and standards	6.11.3	Managers check user's compliance with security policy regularly. ICT systems are checked regularly for compliance.		

5.2. Compliance Checklist: Standalone CQR – Local Data Hosting

To be completed by CQRs implementing and managing local infrastructure

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Good Practice	Complies?	Date
Physical Security	E.1	Secure Areas	To prevent unauthorised physical access, damage, and interference to the organisation's premises and information.	6.5.1	Offices, rooms and data entry/processing facilities are secured with physical entry controls. Public access points are isolated and controlled.		
Physical Security	E.2	Equipment security	To prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.	6.5.2	File servers and networking equipment are located in a lockable area and not accessible by unauthorised people. Mobile devices are secured appropriately when off-premises. ICT assets are disposed of securely.		
Communications and Operations Management	F.1	Operational procedures and responsibilities	To ensure the correct and secure operation of information processing facilities.	6.6.1	Operational procedures are documented. Changes to ICT systems are authorised before implemented.		
Communications and Operations Management	F.3	System Planning and Acceptance	To minimise the risk of systems failures.	6.6.3	Capacity of ICT infrastructure (e.g. network bandwidth) and system components (disk space, memory) is monitored and upgraded as required.		
Communications and Operations Management	F.5	Health information backup	To maintain the integrity and availability of information and information processing facilities.	6.6.5	Data is backed up to reliable media on a daily basis and stored at a location separate to the primary site.		

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Good Practice	Complies?	Date
Communications and Operations Management	F.6	Network Security Management	To ensure the protection of information in networks and the protection of the supporting infrastructure.	6.6.6	At least one staff member has been designated as the network manager and has responsibility for controlling the CQR networks.		
Communications and Operations Management	F.8	Exchanges of Information	To maintain the security of information and software exchanged within an organisation and with any external entity	6.6.8	Data transfer agreements to or from CQRs are documented. External data transfers are encrypted. Identifiable information is sent through an approved courier.		
Communications and Operations Management	F.10	Monitoring	To detect unauthorised information processing activities.	6.6.10	Access to health information is logged and logs are secured so that they can't be changed.		
Access Control	G.2	User Access Management	To ensure authorised user access and to prevent unauthorised access to information systems.	6.7.2	A formal, documented user registration process exists for internal CQR users. External users (e.g. point of care users) are authenticated through a delegated administrator. External administrators and internal CQR users are identified at the point of registration. If not known to the CQR, external administrators are required to show photo identification.		
Access Control	G.5	Application and information access control	To prevent unauthorised access to information held in application systems.	6.7.5	External users can only view information that they enter into the CQR, and not information from other parties. Application sessions are terminated when idle for more than 10 minutes (minimum).		
Information Systems Acquisition, Development and Maintenance	H.2	Correct processing in applications	To prevent errors, loss, unauthorised modification or misuse of information in applications.	6.8.2	Systems correctly merge patient information. Data entry is validated by the application. Application processing routinely validates specific information.		

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Good Practice	Complies?	Date
Information Systems Acquisition, Development and Maintenance	H.3	Cryptographic controls	To protect the confidentiality, authenticity or integrity of information by cryptographic means.	6.8.3			
Information Systems Acquisition, Development and Maintenance	H.4	Security of system files	To ensure the security of system files.	6.8.4			
Information Systems Acquisition, Development and Maintenance	H.5	Security in development and support processes, and technical vulnerability management	To maintain the security of application system software and information and to reduce risks resulting from exploitation of published technical vulnerabilities.	6.8.5	Changes to ICT systems should be managed through repeatable change management processes. Changes or updates to systems are tested before implementing into the live environment.		
Compliance	K.4	Information systems audit considerations in a health environment	To maximise the effectiveness of and to minimise interference to or from the information systems audit process.	6.11.4	When auditing ICT systems, consideration is given to who does the audit.		

5.3. Compliance Checklist: Centres of Excellence or External Data Hosting Providers

To be completed by centres of excellence or other external data hosting providers prior to hosting CQR infrastructure or applications

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Minimum Requirement	Complies?	Date
Information Security Policy	A.1	Information security policy	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	6.1.1	The information security policy is current and endorsed by management. Processes to check and ensure compliance with the policy, and the policy is reviewed and updated at least annually.		
Information Security Organisation	B.1	Internal Organisation	To manage information security within the organisation.	6.2.1	Management show involvement and interest in information security and conduct regular forums where the status of information security is discussed. Staff are aware of their roles and responsibilities for information security.		
	B.2	Third Parties	To maintain the security of the organisation's information and information processing facilities that are accessed processed, communicated to, or managed by third parties.	6.2.2	Formal contracts are in place for when dealing with third parties.		
Asset Management	C.1	Responsibility for health information assets	To achieve and maintain appropriate protection of organisational assets.	6.3.1	There is a designated and documented custodian of CQR information.		
	C.2	Health information classification	To ensure that information receives an appropriate level of protection.	6.3.2	There is an inventory of all types of information and ICT systems and the classification is recorded against each asset. Staff do not use identifiable private information for testing or any other purposes beyond which it was intended. There is documented policy and procedure for handling of Confidential information and staff are educated in its use.		

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Minimum Requirement	Complies?	Date
HR Security	D.1	Prior to employment	To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.	6.4.1	New employee's references and resumes are checked prior to employment. User responsibilities for security are included in staff position descriptions and employment contracts.		
HR Security	D.2	During employment	To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.	6.4.2	Formal security awareness training is included in the organisation's induction process.		
HR Security	D.3	Termination or change to employment	To ensure that employees, contractors and third party users exit an organisation or change employment in an orderly manner.	6.4.3	Formal processes are in place to terminate user accounts.		
Physical Security	E.1	Secure Areas	To prevent unauthorised physical access, damage, and interference to the organisation's premises and information.	6.5.1	Offices, rooms and data entry/processing facilities are secured with physical entry controls. Public access points are isolated and controlled. Access to secure areas is logged and regularly audited.		
Physical Security	E.2	Equipment security	To prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.	6.5.2	File servers and networking equipment are located in a lockable area and not accessible by unauthorised people. Mobile devices are secured appropriately when off-premises. ICT assets are disposed of securely.		

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Minimum Requirement	Complies?	Date
Communications and Operations Management	F.1	Operational procedures and responsibilities	To ensure the correct and secure operation of information processing facilities.	6.6.1	Operational procedures are documented. Formal change management procedures are documented and all stakeholders provide authorisation before a change is made. Development, test and production networks environments are separated and used appropriately.		
Communications and Operations Management	F.2	Third party Service Delivery Management	To implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements.	6.6.2	Service Level Agreements (SLA)'s are in place between CQRs and external data hosting infrastructure providers. SLA's are monitored and reported on regularly.		
Communications and Operations Management	F.3	System Planning and Acceptance	To minimise the risk of systems failures.	6.6.3	Formal Capacity Management plans and procedures are in place and followed. Formal Acceptance Testing plans and procedures are in place and followed.		
Communications and Operations Management	F.4	Protection against Malicious and mobile code	To protect the integrity of software and information.	6.6.4	Antivirus software is installed on all servers, PC's and mobile devices and updates are installed as soon as possible. There are formal processes to respond to an outbreak of malicious software.		
Communications and Operations Management	F.5	Health information backup	To maintain the integrity and availability of information and information processing facilities.	6.6.5	Data is backed up to reliable media on a daily basis and stored at a location separate to the primary site.		
Communications and Operations Management	F.6	Network Security Management	To ensure the protection of information in networks and the protection of the supporting infrastructure.	6.6.6	At least one staff member has been designated as the network manager and has responsibility for controlling the CQR networks. Network management documentation exists, detailing security controls that protect the network, detect intrusions and corrective actions to be taken.		

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Minimum Requirement	Complies?	Date
Communications and Operations Management	F.7	Media handling	To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.	6.6.7	CQRs have determined and documented a policy on the use of removable media and staff are aware of its contents. Suitable technologies have been implemented to control the use of unauthorised removable media, and to detect when there is a policy breach.		
Communications and Operations Management	F.8	Exchanges of Information	To maintain the security of information and software exchanged within an organisation and with any external entity.	6.6.8	Formal procedures are developed and followed for information handling.		
Communications and Operations Management	F.9	Electronic health information services	To ensure the security of electronic health information services, and their secure use.	6.6.9	The process to publish information electronically is documented, well understood and requires specific controls including approval.		
Communications and Operations Management	F.10	Monitoring	To detect unauthorised information processing activities.	6.6.10	An audit log management process is documented and enforced. Logs are secured and unable to be altered. A common and automatic time source is used for systems.		
Access Control	G.1	Requirements for access control in health	To control access to information.	6.7.1	An access control policy has been documented which details each CQR's user roles and the information within that CQR that can be accessed by each user. Service providers have a separate access control policy which details their user roles and access levels.		
Access Control	G.2	User Access Management	To ensure authorised user access and to prevent unauthorised access to information systems.	6.7.2	A formal, documented user registration process exists for internal CQR users. External users (e.g. point of care users) are authenticated through a delegated administrator. Administrators and internal CQR users are identified at the point of registration. All administrators are required to show photo identification in accordance with NESAF.		

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Minimum Requirement	Complies?	Date
Access Control	G.3	User Responsibilities	To prevent unauthorised user access, and compromise or theft of information and information processing facilities.	6.7.3	Users Responsibilities for information security are documented, enforced and compliance checked at least annually.		
Access Control	G.4	Network access control and operating system access control	To prevent unauthorised access to networked services.	6.7.4	Internal access to the wired network requires authorisation. Internal access to the wireless network requires authorisation and a minimum of WPA2 with pre-shared key. External and remote access to the internal network requires authorisation and username/password authentication. Where infrastructure is shared with another organisation, CQR networks should be segregated from others. All users have unique identifiers. Passwords are enforced as a minimum of 8 characters with a combination of letters, numbers and special characters. Remote access.		
Access Control	G.5	Application and information access control	To prevent unauthorised access to information held in application systems.	6.7.5	External users can only view information that they enter into the CQR, and not information from other parties. Application sessions are terminated when idle for more than 10 minutes (minimum).		
Access Control	G.6	Mobile computing and teleworking	To ensure information security when using mobile computing and teleworking facilities.	6.7.6	Documented policy on the use of mobile devices and staff understand the contents. Documented Tele-working and Remote Access Policy and staff understand the contents.		
Information Systems Acquisition, Development and Maintenance	H.1	Security requirements of information systems	To ensure that security is an integral part of information systems.	6.8.1	Requirements for security controls are assessed for all new systems, documented and formally use as input to product selection.		

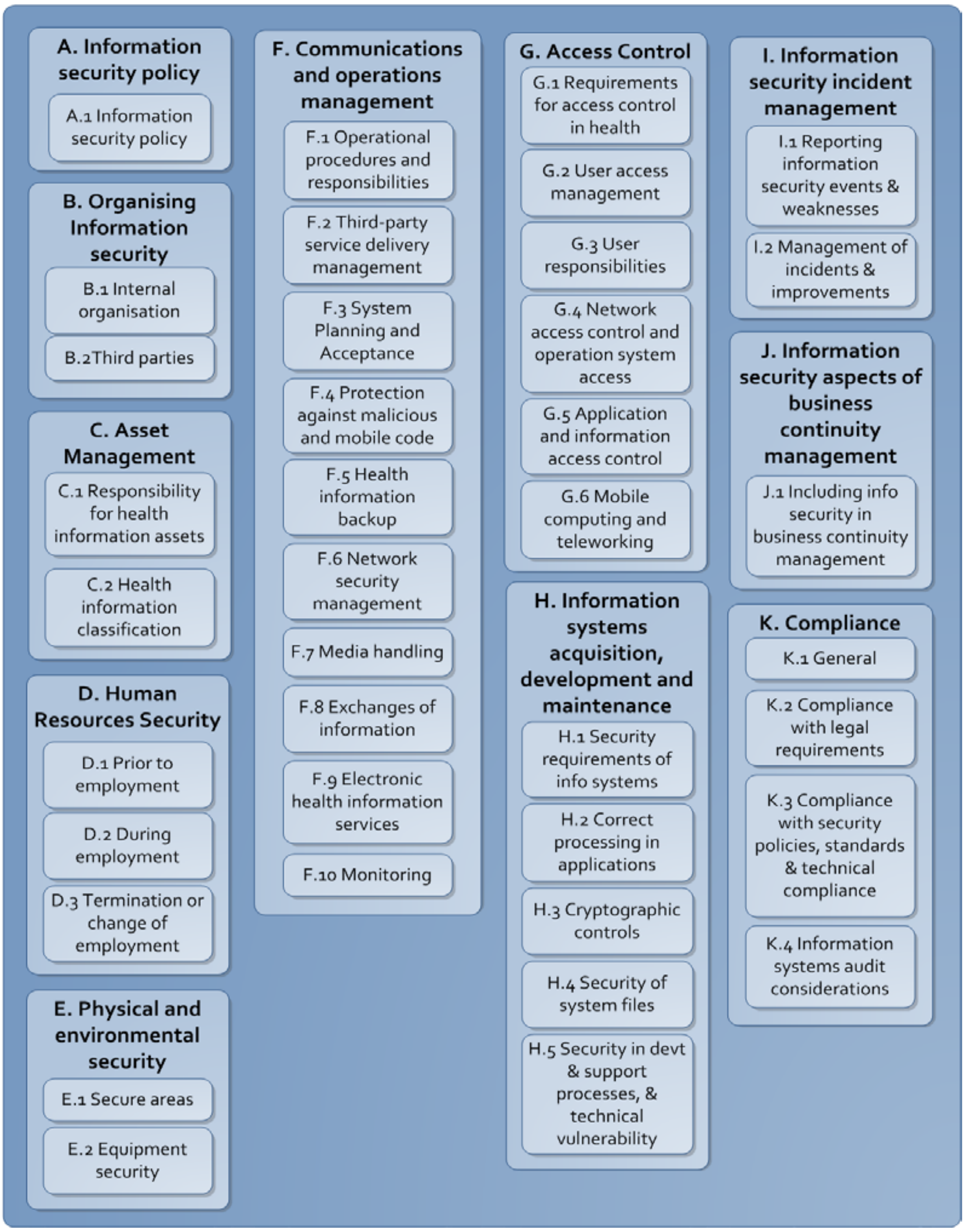
Security Domain	NESAF Ref	Control	Objective	Further Guidance	Minimum Requirement	Complies?	Date
Information Systems Acquisition, Development and Maintenance	H.2	Correct processing in applications	To prevent errors, loss, unauthorised modification or misuse of information in applications.	6.8.2	Systems correctly merge patient information. Data entry is validated by the application. Application processing routinely validates specific information.		
Information Systems Acquisition, Development and Maintenance	H.3	Cryptographic controls	To protect the confidentiality, authenticity or integrity of information by cryptographic means.	6.8.3	A policy on cryptographic controls is developed and documented. Cryptographic keys are protected.		
Information Systems Acquisition, Development and Maintenance	H.4	Security of system files	To ensure the security of system files.	6.8.4	Testing data is selected carefully and not identifiable. Application source code access is controlled.		
Information Systems Acquisition, Development and Maintenance	H.5	Security in development and support processes, and technical vulnerability management	To maintain the security of application system software and information and to reduce risks resulting from exploitation of published technical vulnerabilities.	6.8.5	Changes to ICT systems should be managed through formal, documented change management procedures. Changes or updates to systems are tested before implementing into the live environment.		
Incident Management	I.1	Reporting information security events and weaknesses	To ensure that information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.	6.9.1	There is documentation for staff explaining how to identify and report suspected security events or weaknesses.		
Incident Management	I.2	Management of incidents and improvements	To ensure a consistent and effective approach is applied to the management of information security incidents.	6.9.2	Formal security incident management procedures are developed, enforced and reviewed regularly.		

Security Domain	NESAF Ref	Control	Objective	Further Guidance	Minimum Requirement	Complies?	Date
Business Continuity Management	J.1	Including information security in the business continuity management process	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.	6.10.1	A Business Continuity Guideline has been developed through an analysis of the impact to CQR business. IT Disaster Recovery plans detail CQR prioritisations for recovery. All plans and processes within the Business Continuity Guideline are tested and updated annually.		
Compliance	K.1	General	Establish a graduated compliance auditing guideline.	6.11.1	A guideline for compliance auditing is established and documented.		
Compliance	K.2	Compliance with legal requirements	To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.	6.11.2	Legislative requirements (state and federal) for information security have been identified and legal advice has been provided to ensure the organisation meets the requirements.		
Compliance	K.3	Compliance with security policies and standards and technical compliance	To ensure compliance of systems with organisational security policies and standards.	6.11.3	Managers check user's compliance with security policy regularly, and report to the security co-ordinator. ICT systems are checked regularly for compliance.		
Compliance	K.4	Information systems audit considerations in a health environment	To maximise the effectiveness of and to minimise interference to or from the information systems audit process.	6.11.4	When auditing ICT systems, an audit plan is developed and documented.		

6. Detailed Guidance on Controls

Each security control is explained in more detail in this section, categorised by security domains. The guidance provided is a blend of detail from relevant security guidelines and specific detail to suit CQR environments. The guidance provided borrows heavily from the National eHealth Security and Access Guideline and ISO/IEC 27002.

The following diagram[5] represents the domains of information security.


A. Information security policy
A.1 Information security policy
B. Organising Information security
B.1 Internal organisation
B.2Third parties
C. Asset Management
C.1 Responsibility for health information assets
C.2 Health information classification
D. Human Resources Security
D.1 Prior to employment
D.2 During employment
D.3 Termination or change of employment
E. Physical and environmental security
E.1 Secure areas
E.2 Equipment security
F. Communications and operations management
F.1 Operational procedures and responsibilities
F.2 Third-party service delivery management
F.3 System Planning and Acceptance
F.4 Protection against malicious and mobile code
F.5 Health information backup
F.6 Network security management
F.7 Media handling
F.8 Exchanges of information
F.9 Electronic health information services
F.10 Monitoring
G. Access Control
G.1 Requirements for access control in health
G.2 User access management
G.3 User responsibilities
G.4 Network access control and operation system access
G.5 Application and information access control
G.6 Mobile computing and teleworking
H. Information systems acquisition, development and maintenance
H.1 Security requirements of info systems
H.2 Correct processing in applications
H.3 Cryptographic controls
H.4 Security of system files
H.5 Security in devt & support processes, & technical vulnerability
I. Information security incident management
I.1 Reporting information security events & weaknesses
I.2 Management of incidents & improvements
J. Information security aspects of business continuity management
J.1 Including info security in business continuity management
K. Compliance
K.1 General
K.2 Compliance with legal requirements
K.3 Compliance with security policies, standards & technical compliance
K.4 Information systems audit considerations

[5] Source: National eHealth Security and Access Framework and ISO/IEC 27002.

6.1. Information Security Policy

6.1.1. Information Security Policy

Objective: To provide management direction and support for information security in accordance with CQR business requirements and relevant laws and regulations.

Guidance: Security policies are the foundation of a CQR's security infrastructure. They provide direction and support for CQR information security; identify the security and access controls that will be implemented within the CQR at a high level, and serve as a point of reference for all CQR staff, staff in participating institutions and external service providers in relation to their information security responsibilities.

Changes made to the CQR, ICT systems or other internal or external factors that may affect the CQR's risk profile may need to be reflected in the policy.

Reviews of the usefulness of the policy (through reviews or regular feedback) should be undertaken and changes made where required.

Useful references for obtaining guidance for developing an Information Security and Access policy is included in Appendix A of the NESAF Business Blueprint[6], and the RACGP Computer Security Standards[7].

Architectural Impact: All aspects of a CQR's architecture.

6.2. Organising information security

6.2.1. Internal Organisation

Objective: To manage information security within the CQR and its external data hosting infrastructure providers.

Guidance: Responsibilities for information security governance and operations should be clearly documented within the information security policy (refer to Section 6.1.1). CQRs and external data hosting infrastructure providers may assign a role for managing information security to one of the positions within their organisation. CQRs and external data hosting infrastructure providers should seek guidance and support from qualified external information security experts as required.

A sample of Role Descriptions within a health organisation is contained in the NESAF Business Blueprint[8].

All new software, applications and hardware should be authorised by an approved management representative prior to connection of any new system to existing ICT systems or networks.

Managers should ensure that all employees and third parties, that may access health or personal information as part of their job, sign confidentiality agreements and are aware of the penalties that are possible for a breach of the agreement or the information security policy.

[6] http://www.NEHTA.gov.au/implementation-resources/ehealth-foundations/EP-1005-2012/NEHTA-1004-2012

[7] http://www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/

[8] http://www.NEHTA.gov.au/implementation-resources/ehealth-foundations/EP-1005-2012/NEHTA-1004-2012

Agreements should include, but not be limited to:

- definition of the information is to be protected (e.g. all patient information).
- duration and termination of agreement.
- responsibilities of the signatories to the agreement.
- permitted use of information protected under the agreement.
- the right to audit and monitor the signatory's access to the protected information.

The RACGP Computer and Information Security Standards[9] contain a sample Confidentiality Agreement.

Organisations should have procedures in place that specify when and by whom authorities (e.g. law enforcement, Privacy or Health Services Commissioners) should be contacted, and how information security incidents should be reported in a timely manner if it is suspected that laws may have been broken.

Channels with external, reputable user groups (for example, the Australian Information Security Association) should be established by the person responsible for information security within an organisation so as to stay up to date with relevant information security practices.

External, reputable information security sources should be used for information on current vulnerabilities and patches (for example, vendors or AusCERT).

Periodic independent reviews of the CQR and external data hosting infrastructure providers' approach to managing information security should be conducted. The review may be by an external information security assessor, the organisation's internal audit function or other party not directly involved with the information security function.

The review should be documented and a report provided to the person responsible for the organisation's information security with recommendations on any improvements that need to be made.

Architectural Impact: All aspects of a CQR's architecture.

6.2.2. Third parties

Objective: To maintain the security of the CQR's information and information processing facilities that are accessed, processed, communicated to, or managed by third parties (for example access by participating institutions/units/clinicians, third party hosting services).

Guidance: The risks of giving external, often untrusted, parties access to health information should be identified so that a CQR can implement appropriate protection mechanisms.

Importantly, an assessment of any 'cloud' or other externally hosted service should be undertaken, as there may be legislative restrictions on the hosting of information - for example, the Privacy Act currently restricts personal information from being transmitted outside of Australia.

Risks assessed when third parties (including information providers, data recipients – clinicians, clinical colleges, government agencies and funders,

[9] http://www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/

vendors, integrators) request access to information or when information is hosted externally should be treated before any access is granted. Specific considerations should include, but not be limited to:

- description of the reason for the access
- ensuring third parties only receive access to that which they require and no more
- access control methods
- responsibilities for support (include in Service Level Agreements)
- agreements (confidentiality and penalties etc)
- identification of external users
- auditing of third party access.

An efficient method of providing access to third parties may be to group like third parties together and develop procedures and protocols for implementing access for each.

CQRs should assure themselves that suitability checks have been undertaken by third party organisations in relation to anyone that will be granted access to CQR information. The granting of CQR system access by third parties to their employees/contractors (e.g. information providers, data recipients – clinicians, clinical colleges, government agencies and funders) should be revoked following termination or change of employment/contract as soon as system access is no longer required.

Architectural Impact: All aspects of a CQR’s architecture.

6.3. Asset Management

6.3.1. Responsibility for health information assets

Objective: To achieve and maintain appropriate protection of CQR and external data hosting infrastructure provider information assets.

Guidance: Information assets describe any information, or set of information, which has value to the organisation.

An information asset in a CQR context may include, but not be limited to:

- CQR databases
- IT hardware
- internet connection software
- staff information
- participating institution/unit/clinician information.

The information asset custodian should be a Manager or other stakeholder with a designated responsibility for maintaining the asset's currency and security.

Architectural Impact: This domain is linked to the business function of data custodianship and affects all aspects of a CQR’s architecture.

6.3.2. Health information classification

Objective: To ensure that information receives an appropriate level of protection.

Guidance: All personal health information is confidential and should be treated accordingly.

Subjects of care that may be at elevated risk of unauthorised access (for example, CQR staff; heads of government; celebrities) may have their records tagged accordingly so that access can be closely monitored. However, their personal health information is not innately more confidential than that of other subjects of care.

Not all health information is confidential and not all health information systems provide users with access to personal health information. Users of health information systems need to know when the data they are accessing contains personal health information. The Technical Standard (ISO/TS 14265:2011) Health Informatics – Classification of purposes for processing personal health information provides a guideline for the classification and consistent management of information in the delivery of health care services and for the communication of electronic health records across organisational and jurisdictional boundaries.[10]

The privacy of personal information or health information should be maintained in accordance with any requirements under applicable privacy law when used for purposes other than clinical care, for instance, research or statistical purposes.

De-identification of personal health information is more than simply removing the patient's name. Whenever the information is in the form of individual data sets, there is a risk that the data set could be linked to a particular individual on the basis of details of age, postcode and medical condition. The more information included in the data set, the greater the risk of identification. Even where data is aggregated, care should be taken that the number of people in each ‘cell’ or sub-group is sufficient to ensure that the privacy of the individuals involved is not compromised.

If de-identification is not possible or impractical, the *NHMRC Guidelines approved under Section 95A of the Privacy Act 1988,* should be used.

Architectural Impact: Data Extraction Service; Information Publishing Service; Reporting Service; Ad Hoc Query Service.

6.4. Human resources security

6.4.1. Prior to employment

Objective: To ensure that employees, contractors and third party users understand their responsibilities and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

Guidance: Involvement in processing personal health information, and security roles and responsibilities, should be documented in relevant job descriptions within CQRs and centres of excellence.

Position Descriptions should include general responsibilities for information security, including, but not limited to, maintaining the confidentiality of health and personal information.

[10] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=54547

Special attention should be placed on the position descriptions of temporary, casual and other short term staff.

CQRs and centres of excellence should conduct criminal history checks and confirm professional qualifications for all employees, contractors and third parties (e.g. external data hosting infrastructure providers) requiring access to the CQR's information.

The terms and conditions of employment should include the penalties incurred if the information security policy is breached and specify the rights that the employee/user will have to access health information and information systems.

Architectural Impact: Authentication Service; Authorisation Service; External User Management Service.

6.4.2. During employment

Objective: To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.

Guidance: Managers within a CQR or a centre of excellence should ensure that employees and third party users are:

- properly briefed on their information security roles and responsibilities prior to being granted access to the system
- provided with guidelines to state security expectations of their role within the CQR or in accessing CQR systems
- motivated to fulfil the security policies of the CQR or external data hosting infrastructure provider to the CQR.

Management should implement security awareness training programs for all employees of the organisation and third parties that access health or personal information. Plans to review the effectiveness of the training should be developed and implemented by management.

Management should develop the disciplinary process and ensure that all employees are aware of the penalties for breaching the information security policy. Users should also be aware of legislative penalties due to breaches of the Privacy or other Health Act/s.

Architectural Impact: Authentication Service; Authorisation Service; External User Management Service

6.4.3. Termination or change of employment

Objective: To ensure that employees, contractors and third party users exit an organisation or change employment in an orderly manner.

Guidance: Changes in employment e.g. progression through training programs and other 'rotations' where access rights can change fundamentally, should be processed in the same way as for individuals leaving the CQR or centre of excellence's employment.

Consider linking the information security termination process with the human resource termination process to minimise delay with the return of assets and disabling employee or third party credentials.

Terminated CQR or centre of excellence employees should not have access to health or personal information after leaving the organisation.

Transferred or rotated employees or third parties should not have access to health or personal information, beyond that which is required for their current role in relation to accessing CQR information.

Access credentials should not be deleted in case of future creation. It is important to not re-issue credentials (e.g. user names) of an employee that has been terminated to another employee.

Architectural Impact: Authentication Service; Authorisation Service; External User Management Service

6.5. Physical and environmental security

6.5.1. Secure areas

Objective: To prevent unauthorised physical access, damage, and interference to the organisation's premises and information.

Guidance: Central information and communications facilities within a CQR or external data hosting infrastructure provider to a CQR (computer or communications rooms) should house file servers and core network infrastructure equipment and have a defined perimeter with entry controls (e.g. locks on doors).

CQRs and their external data hosting infrastructure providers should take sensible steps to ensure that unauthorised personnel are only as accessible to IT equipment (servers, storage device, terminals and displays) as physical constraints demand.

When employees or external data hosting infrastructure providers are working in secure areas (computer or communications rooms), access to these rooms should be monitored and auditable.

Public areas within participating institutions where CQR information is gathered through interview or that contain systems where CQR data are entered or viewed on screen should take sensible steps to ensure that the public are only as accessible to terminals and displays as physical constraints and clinical processes demand. For example, placing notices in these areas that remind employees to curtail discussion of patient cases in public areas.

Architectural Impact: Hosting Service

6.5.2. Equipment Security

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the CQR’s activities

Guidance: CQRs or their external data hosting infrastructure providers should situate any workstations allowing access to personal health information in a way that prevents unintended viewing or access by unauthorised personnel. Organisations should ensure that the siting and protection guidelines for IT equipment minimise exposure of health and personal information, for example through the attaching a privacy filter to screens that may be viewable by unauthorised personnel.

Some geographic areas susceptible to power failures or loss should consider the use of generated power as a backup.

CQRs, or their external data hosting infrastructure providers, that regularly utilise equipment containing health or personal information off-premises should consider developing a Portable Device Policy and procedures to guide employees in the use and security of such equipment.

Only approved, reputable organisations should be used to resell or dispose of any equipment that may contain, or has transmitted health or personal information.

Electronic records that are no longer needed should be deleted. However, it is very difficult to reliably remove all traces of electronically stored information. Organisations will need to be aware that deletion may only remove the file-reference but leave all the other information intact.

Architectural Impact: Hosting Service; Hardware Service

6.6. Communications and Operations Management

6.6.1. Operational procedures and Responsibilities

Objective: To ensure the correct and secure operation of information processing facilities

Guidance: CQRs and external data hosting infrastructure providers should have documented and maintained operating procedures. These should specify the instructions for the detailed execution of each job, including scheduling and any interdependencies, special data processing, specific backup requirements, error handling, specialised support team where available, start-up and stop processes and handling of log information including audit trails.

Inadequate or inappropriate testing of changes to information processing facilities and systems is a common cause of system or security failures and can have disastrous consequences for CQRs.

Organisations should document change management processes that describe how to asses and identify the risks to the operational environment, especially when transferring a system from development to operational stage.

Large organisations commonly use a service management guideline such as ITIL (the IT Infrastructure Library). These guidelines will commonly describe a robust change management process that can support the effective management of the information processing environment as business needs require.

CQRs and external data hosting infrastructure providers should, where possible, segregate areas of responsibility to reduce the possibility of unauthorised access, modification or misuse of personal information.

Standalone CQRs may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate duties, other controls including monitoring of activities, audit trails and management supervision should be considered. It is important that security audit remains independent.

Although implementing this control area may commonly be realised by using more than one person in a role to ensure that operations can be monitored, the control needed is often finer-grained. For example, it is good practice to prevent database administrators from being able to also administer the system that audits access to the database. A malicious attacker who might gain access to the database would seek to hide their activities by altering log files or access logs; separating these roles (and systems) is prudent and can provide additional detection capabilities in the event of an attack.

Architectural Impact: All aspects of a CQR's architecture.

6.6.2. Third party service delivery management

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements.

Guidance: Any contract that describes a service delivery by a third party should include the agreed security arrangements, service definitions, and aspects of service management. It should also describe how the third party will maintain sufficient service capability to ensure that agreed service continuity levels are maintained following major service failures or disaster

When outsourcing CQR information or ICT systems to an external data hosting infrastructure provider, CQRs should ensure that the security and integrity of CQR information is maintained throughout the transition period and during the outsourcing contract.

CQRs or service providers should assign a designated individual or service management team the responsibility for managing the third-party. The third party should assign responsibilities for checking for compliance and enforcing the requirements of the contractual agreements. Resources should be made available to monitor that requirements of the contractual agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies are identified.

CQRs should maintain overall control and visibility into all security aspects for information processed or managed by a third party and ensure they have tools and resources to maintain control of change management, identification of vulnerabilities, and information security incident reporting/response.

The ultimate responsibility for health information processed by an outsourcing party remains with the CQR.

Architectural Impact: All aspects of a CQR's architecture.

6.6.3. System Planning and Acceptance

Objective: To minimise the risk of systems failures.

Guidance: Systems should be monitored to ensure the availability of systems and to plan for system upgrades. Key system components, especially those with specialist or extended procurement processes, should have regular updates to future projections of requirements, identifying trends in usage.

CQRs and service providers should have documented acceptance criteria including the formal testing that must be performed and formal sign-off processes. Testing should exercise all aspects of the new system or upgrade and include the operation, user, business continuity and security functions. The extent and rigour of the testing should reflect the risks identified in the risk assessment associated with the change.

Acceptance criteria should also ensure that there are agreed and documented security controls, business continuity plan and operations/user manuals.

[Source for guidance: NESAF]

Architectural Impact: All aspects of a CQR's architecture.

6.6.4. Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

Guidance: CQRs and service providers should ensure they have anti-malware software running on all devices as well as any network boundary; and that processes are in place to ensure that the anti-malware software and signatures are kept up to date, preferably by automated procedures. The anti-malware software should scan the computer hard-disk on a regular basis (i.e. once per week); as well as any removable storage devices (e.g. USB drives, optical media, etc). It should also monitor other ingress point such as email, and web browsing.

CQRs should document clear policies prohibiting the download and/or installation of unauthorised software, and the use of the organisation's computers for accessing Internet sites for non-work related activities, as this could expose the computer to malicious code. Users should be trained and made aware of the policies.

CQRs and service providers should have documented procedures for how to deal with an infected computer, including business continuity plans and how to recover any log files or audit records to determine if there was any compromise.

Mobile code is software code which transfers from one computer to another and then executes automatically. It normally performs a specific function without any user interaction and is often associated with middleware services.

CQRs and service providers should ensure that any legitimate mobile code that is used within their environment is signed by a trusted code-signing certificate. They should then disable the download and execution of all other mobile code; and should enforce a policy on an exception basis.

Architectural Impacts: Presentation Service; Application Service; Infrastructure Security Service

6.6.5. Health information backup

Objective: To maintain the integrity and availability of information and information processing facilities.

Guidance: Processes that support the back-up of CQR information and essential software so that it can be recovered in the event of a disaster or system failure should be documented and tested. These processes should include what items are to be backed-up; how often the back-up is run; what media is used and how it is to be rotated; and where the back-ups are to be stored.

The information that is backed-up should be encrypted to ensure its confidentiality. The keys used for the back-up should be changed on a regular basis and should be secured at a separate location to the back-up media.

The physical and environmental protection features implemented at the storage site should be consistent with those at the main data centre.

Architectural Impacts: System Management Service; Repository Service

6.6.6. Network Security Management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure

Guidance: CQRs or service providers should document clear procedures and responsibilities on the management of network equipment and services including controls to ensure the confidentiality and integrity of data passing over the network, especially public and wireless networks; appropriate monitoring and logging to enable clear auditing of events on the network; and clearly defined operational responsibilities, especially if part of the network is provided by a third-party.

CQRs should ensure business continuity plans are in place in case of extended network failure.

CQRs should ensure they have documented agreed service features including the security features, service levels and management of the network service. They should have the ability to monitor the network service and should have clearly defined escalation paths if issues are identified.

The security features that are identified should include controls for accessing the network, maintaining confidentiality and integrity across the network, and monitoring and reporting on network activity.

Architectural Impacts: Network Service

6.6.7. Media Handling

Objective: To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.

Guidance: CQRs and service providers should have documented processes for the management of removable media (including tapes, floppy disks, USB and flash drives, removable hard-disk drives, and optical disks (CDs and DVDs).

When media is no longer required it should be destroyed so that the information is un-recoverable. All media should be used and stored in accordance with the manufacturers' recommendations; and where necessary media should be refreshed if the storage period exceeds the manufacturers' recommendation.

Disable the use of removable media on computers where there is no business need.

A process to control the disposal of unwanted or expired media should be in place. All media containing health information, including storage media within a computer or medical device; should be disposed of in a manner which maintains the security of the data.

There are programs that can be used to securely remove the information from computer media. These should be used on media before it is removed from the computer device. Organisations should destroy media so that it can no longer be used (e.g. incinerate or shred) before it is securely disposed of.

Some organisations offer services to collect and securely dispose of media that could be used.

When accumulating media of a less sensitive nature, organisations should consider that the aggregation of the less sensitive information can have a significant impact. Organisations should consider whether the better approach might be to securely dispose of all media.

Procedures for the storage, handling, processing and communication of information should be documented. Where health information is stored electronically, either permanently or temporarily it should be encrypted or physical protections should be in place to prevent unauthorised access.

Removable media should be marked with the classification and type of data, identified with a unique reference, and if appropriate the recipient's name.

Records should be kept of where the media is stored and who/when the media was accessed.

Unencrypted health information, including printed copies, should be clearly marked with the authorised recipient's name, date; and be monitored, including a receipt from the recipient acknowledging acceptance of the media.

When the media is no longer required or expired it should be securely destroyed.

System documentation may contain a range of sensitive information, e.g. descriptions of applications processes, procedures, data structures, authorisation processes. System documentation should be securely stored and access should be kept to a minimum and authorised by the application owner.

System documentation held on a public network, or supplied via a public network, should be appropriately protected from unauthorised access.

Architectural Impacts: All aspects of a CQR’s architecture.

6.6.8. Exchanges of Information

Objective: To maintain the security of information and software exchanged within an organisation and with any external entity.

Guidance: CQRs and service providers should ensure that all information exchanges are done in accordance with agreed policies and are subject to audit controls. The security of information exchanges should be documented in mutually agreed information exchange agreements.

All personnel that have access to sensitive information should understand their responsibilities for ensuring the confidentiality and integrity of that data, including:

- not divulging information to unauthorised parties by means of conversation in a public place, or misplacing or misdirecting media such as print outs or email communications
- not opening of unsolicited or SPAM emails which may contain malicious code
- not using insecure communication methods, such as facsimile, voicemail, instant messaging.

Information could be vulnerable to unauthorised access, misuse, loss or corruption during physical transport. A list of approved and reliable couriers that meet their security requirements should be created.

Only approved couriers should be used to transport media that contains sensitive information. Couriers should be identified before the package is handed over and when the package is received.

Media should be transported in secure containers that are tamper evident and should protect the media from any damage that might occur during transit, including environmental factors (e.g. moisture, heat, sunlight, electromagnetic fields).

Electronic messaging has different risks to paper based messaging because of the ease and speed of dissemination.

When messages are sent electronically, CQRs and service providers should ensure that there are sufficient systems and user education to prevent any sensitive information from being disclosed to an unauthorised party. This should include ensuring that only authorised users can send sensitive information by approved services; and also putting in place systems and processes to ensure correct addressing. Any unapproved messaging services should be disabled, either at the computer or at the network level. Steps should be in place to ensure the confidentiality and integrity of the information within the message.

CQRs should consider whether there is any requirement for authentication of the sender, by using a digital signature for example.

Systems should have the ability to restrict access to some records or information when transferring information to another system. All interconnected systems should maintain the same level of protection of the information that has been ascertained in the risk assessment. CQRs and service providers should consider whether different levels of access to information is required for different categories of user (consumer, administrative staff, nurse, health practitioner) and also different types of employee (employee, temporary employee, contractor, vendor etc).

Architectural Impacts: Data Load Service

6.6.9. Electronic health information services

Objective: To ensure the security of web publishing services, and their secure use.

Guidance: Any web publishing system should be implemented so as not to divulge health information unless it is determined necessary. If health information is divulged then the systems should implement controls to maintain the confidentiality and integrity of the health information. Systems that this may affect include billing, invoicing and requisitions.

Consideration should also be given as to whether there is a requirement that the originator and/or recipient of the transaction is authenticated, and how authorisations are checked.

CQRs should have formal approval processes before information can be published publically. There should also be processes that review the publication to ensure that it does not divulge protected information and that it is accurate.

Once published processes should ensure the integrity of the publication and identify the author(s).

Any sensitive information should be de-identified within the publication.

Architectural Impacts: Information Publishing Service

6.6.9.1. Monitoring

Objective: To detect unauthorised information processing activities

Guidance: An audit log should uniquely identify the user, date, time and details of the event. Events that should be recorded in an audit log include successful and unsuccessful access attempts, changes to system configurations, use of privileges, activation of alarms or alerts (e.g. anti-virus, intrusion detection systems), and access, creation, update or archive of personal health information.

When the audit log event is related to access, creation, update or archive of a personal health record the log should also uniquely identify the subject of care; and if appropriate a record of the former information.

Audit logs may contain personal information and should therefore be protected from unauthorised access. It is also important that the integrity of the audit log should be maintained.

Systems should be able to provide an easy to understand report containing the required information whom to identify when and by whom a healthcare record was accessed.

Monitoring systems should include details of information systems, such as when the system was started and stopped, use of privileged system accounts, configuration changes, operating system and application alerts, access to system files, installation (or removal) of software, I/O device attachment/removal, access violations and alerts from network gateways, firewalls, intrusion detection systems and other security systems.

CQRs and service providers should have documented processes for how often the monitoring log files are reviewed, which should be related to the risks identified in the information system.

CQR information systems should be able to present monitoring log information so that the following can be determined:

- the identification of all users who have accessed or modified a particular subject of care's health record(s)
- the identification of all subjects of care whose records have been accessed by a particular user.

Audit logs should be tamper evident, to ensure that log entries cannot be added or deleted or modified. The logs should also be backed up. Systems should also monitor the space available on storage media for the audit log and manage the storage capacity for the audit log file(s).

Audit records related to personal health records could be used for evidentiary purposes. Therefore, such logs should be recorded so as to provide integrity of the log and all of the required data. These logs should also be archived.

Useful reference: ISO/DIS 27789 Audit Trails for electronic health records.

These logs should contain the user account, time of the event, information about the event and which processes were involved. The logs should be tamper evident and should be monitored by a party outside of the normal operations team (e.g. IT security team or internal audit).

System logs can monitored automatically for certain known events and alerts raised to specific teams and individuals, larger organisations should consider implementing such a system.

Faults detected by system programs or reported by users related to information systems should be logged. The organisation should have processes that identify how the fault is managed, including how the fault was corrected to ensure that no controls have been compromised; and what state the reported fault is in (e.g. open, resolved, awaiting vendor patch).

Where an information system utilises a real-time-clock, this clock should be synchronised to a recognised time source and set to an agreed time standard, Coordinated Universal Time (UTC) is recommended.

Time is a key part in the audit records system, which for personal health records access could be used for evidential purposes. Therefore, systems should ensure that the clocks utilised by such systems are synchronised regularly.

Architectural Impacts: All aspects of a CQR’s architecture.

6.7. Access Control

6.7.1. Requirements for Access Control in Health

Objective: To control access to information.

Guidance: Access control rules for healthcare practitioners accessing health information systems should be identified to mitigate the risks identified to the health information. These access control rules should consider both the logical and physical controls.

CQRs and service providers should have documented policies that include the requirements for registration of new users, the assigning (and removal) of authorisations, and roles within the organisation.

Segregation of the roles that perform the registration of users and assign the authorisations should be considered.

Access control rules should identify rules that must always be enforced and guidelines that are optional. The policy should identify the rules that govern the monitoring of access control rule enforcement.

Architectural Impacts: External User Management Service; Authentication Service; Authorisation Service.

6.7.2. User Access Management

Objective: To ensure authorised user access and to prevent unauthorised access to information systems.

Guidance: All healthcare professionals who require access to healthcare information about patients must be uniquely identifiable either by an HPI-I or the relevant HPI-O and local ubiquitous identifier. The local registration process should issue a user with a unique user ID after they have satisfied an evidence of identity check. The registration process should also assign the user ID authorisations to access information and perform functions within applications and services.

The registration process should also ensure that the user is aware of any specific organisational access policies, and should include a record of the user's acceptance of such policies, possibly by recording a signed statement. It should also maintain formal records of approved users, and include processes to revoke registration, when a user leaves the organisation for example.

CQRs and service providers should consider grouping users into access roles and assigning authorisations to the roles, as opposed to the individual user.

National Privacy Principle 8. Anonymity, states that 'Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation'.

Useful reference: ISO/TS 25237:2008 Pseudonymisation

Clinical quality registry systems should have the allocation of privileges controlled through a formal authorisation process, including the access privileges associated with each component of the system (operating system, database, application); privileges should only be granted when needed; and use of privilege should be monitored and recorded.

Where possible systems should utilise routines and programs that do not require the use of privilege.

Inappropriate use of system privileges can assist in the breach of system security controls and therefore should be actively discouraged.

When users are first registered they should be given in a secure manner a temporary password that is unique to them. The user should be forced to change the temporary password at first use.

If a user is to be issued with another temporary password, (e.g. when they forget their password), then the users identity should be validated prior to the issuance of the new password.

Passwords should never be stored on a computer system in an unprotected form. Default application passwords should never be used and should be changed as soon after implementation as possible.

User access right should be reviewed at frequent periods, e.g. yearly, and after any major change such as change of role or termination of employment. User access right should be reviewed and re-allocated if the user changes roles within the same organisation.

Authorisations for higher privileged access should be reviewed more often, e.g. monthly, and allocations should be checked to ensure that unauthorised privileged rights have not been obtained.

Architectural Impacts: External User Management Service; Authentication Service; Authorisation Service.

6.7.3. User responsibilities

Objective: To prevent unauthorised user access, and compromise or theft of information and information processing facilities.

Guidance: All users should be advised to keep their passwords secret and not keep a record. CQRs and service providers should have a policy that identifies how often a password should be changed and the complexity of the password. Care should be taken to ensure that the policy does not place undue burden upon the user which may cause them to record their passwords.

Password rules should encourage longer passwords, which utilise special characters and numbers, and cannot be recycled.

Users should be made aware that computer equipment should not be left unattended with an active user session still logged in.

Users should be encouraged to log off the computer system or utilise an appropriate locking mechanism, e.g. screen lock.

Screen locks should enable an override by another user in the event that the computer is required by another user.

CQRs and service providers should ensure that no identifying information is left unattended, either in printed form or electronic form. All printed media should be securely destroyed or locked away. All electronic storage media should be secured when not being used, and healthcare information should be removed securely from the media as soon as it is no longer required.

Computer screens should be angled so that they are not visible from public areas, privacy guards should be used to reduce the ability for someone to overlook the screen.

Architectural Impacts: External User Management Service; Authentication Service.

6.7.4. Network and operating system access control

Objective: To prevent unauthorised access to networked services.

Guidance: An organisation should have a policy concerning the use of networks and network services. This policy should identify:

- the networks and network services which are allowed to be accessed
- authentication and authorisation procedures for determining who is allowed to access networks and networked services
- management controls and procedures to protect access to network connections and network services
- Any remote methods to access the network (e.g. virtual private network).

This control is particularly important for network connections to applications or services that process health information and to users accessing from high-risk locations, e.g. public Internet, which is outside the organisation's security management and control.

The connection should use a virtual private network (VPN) or dedicated private lines to provide assurance of the source of connections.

Authentication of the end-point device should be used if only permitted devices are allowed to connect to the network. The device should be issued with a credential that is unique to it. Once the device is successfully authenticated and connected to the network the user should be authenticated and authorised access to the application or service.

Diagnostic and configuration ports should only be available to authorised users and by approval from the manager of the computer service. Ports, services, and similar facilities installed on a computer or network device, which are not specifically required for business functionality, should be disabled or removed.

Many computer systems, network systems, and communication systems are installed with a remote diagnostic or configuration facility for use by maintenance engineers. If unprotected, these diagnostic ports could provide a means of unauthorised access.

Networks should be segregated into domains based on the access control policy and access requirements, and should also take into account the relative cost and performance impact of incorporating additional network routing or gateway technology.

In addition, segregation of networks should be based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption. Networks processing health information should be segregated from those networks used for operational purposes (e.g. back-up).

Consideration should be given to the segregation of wireless networks from internal and private networks. As the perimeters of wireless networks are not well defined, a risk assessment should be carried out in such cases to identify controls (e.g. strong authentication, cryptographic methods, and frequency selection) to maintain network segregation.

The access control policy should identify what services should be available to users on a network, and from where the user can access the service.

Any un-necessary or unauthorised services should be blocked at the network gateway, e.g. file transfer services, by closing the network port.

The access control policy should identify networks that can be connected to particular applications and which functions on that application can utilise or connect to that network.

For example, if a segregated back-up network is identified, then no users should be connecting to the application from that network.

The procedure for logging into a system should be designed to limit unauthorised access. The log-on procedure should therefore disclose the minimum of information about the system, in order to avoid providing an unauthorised user with any assistance. A log-on procedure should not display system or application identifiers until the log-on process has been successfully completed and display a general notice warning that the computer should only be accessed by authorised users.

The log-on procedure should not provide any messages during the log-on procedure that might aid an unauthorised user and should only validate the log-on information upon completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect.

The log-on procedure should limit the number of unsuccessful log-on attempts allowed and should record unsuccessful and successful attempts. Consideration should be given to enforcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorisation.

Consideration should be given as to display the following information on completion of a successful log-on:

- date and time of the previous successful log-on
- details of any unsuccessful log-on attempts since the last successful log-on.

All users that need to access an information system should have their own unique user ID. This includes privileged users, such as technical support teams, operators, system administrators and application users. The user ID should be able to assist with tracing the activities to an individual. Users should not log-on to systems using privilege accounts, and should use their own user ID and temporarily uplift their session to the privilege account.

Users accessing health information should be uniquely identified by a user ID.

In exceptional circumstances where there is a clear business benefit the use of a shared user ID for a small, defined group of users, can be used. This should be documented and the members of the group should be reviewed and if necessary the password changed to ensure that the shared user ID is not compromised. Additional controls to maintain accountability to an individual may be required.

Generic or anonymous access should only be used where the functions being used do not need to be traced, (e.g. read only access to public health information).

If privileged user IDs are to be used then they should only be issued to a known individual one user at a time and a record should be kept of the time and date when the individual used the privilege user ID. The password should be changed after each use so that the record is an accurate copy of when the specific individual used the privilege user ID

A password management system should:

- enforce the use of individual user IDs and passwords to maintain accountability
- allow users to select and change their own passwords and include a confirmation procedure to allow for input errors
- enforce a choice of quality passwords (see NESAF Framework and Controls[11])
- enforce password changes (see NESAF Framework and Controls)
- force users to change temporary passwords at the first log-on (see NESAF Framework and Controls)
- maintain a record of previous user passwords and prevent re-use
- not display passwords on the screen when being entered
- store password files separately from application system data
- store and transmit passwords in protected (e.g. encrypted or hashed) form.

System utilities should be limited to the minimum practical number of trusted authorised users. All system utility use should be monitored and recorded and should require authentication of the user.

CQRs and service providers should document the policy and procedures for authorising ad-hoc use of system utilities. Ad-hoc use of a system utility is required then it should be authorised by a responsible authority and the authorisation should be recorded. The user should only have access to the utility for the duration that has been authorised.

System utilities should be segregated from applications software and where segregation of duties is required they should not be available to application users.

All unnecessary software utilities should be removed or disabled.

A time-out facility that clears the screen, and possibly closes the application after a defined period of time should be implemented on computers that are in insecure environments and have access to health information.

Consideration should be given to the type of use and environment that the computer is in, for example this control may be less appropriate in the emergency department.

Connection time controls should be considered for information systems that access health information, especially if access is from a remote connection. The types of restrictions that should be considered are:

- using predetermined time slots, e.g. for batch file transmissions, or regular interactive sessions of short duration
- restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation
- considering re-authentication at timed intervals.

Architectural Impacts: External User Management Service;

Authentication Service; Authorisation Service; Network Service

[11] http://www.NEHTA.gov.au/implementation-resources/ehealth-foundations/EP-1005-2012/NEHTA-1007-2012

6.7.5. Application and information access control

Objective: To prevent unauthorised access to information held in application systems

Guidance: Restrictions to health information should be based upon the role the individual plays within the information system and the consent settings that have been set by the health record owner.

Applications should only output health information that is relevant and authorised for the user. Access restrictions may also differ depending upon from where (and even what device) the user is access the application from.

If an information system manages sensitive health information then it may be necessary to isolate it from other information system at the discretion of the system owner after a risk analysis. Additional controls should put into place to control access and monitor activity.

Architectural Impacts: Application Service; Authorisation Service

6.7.6. Mobile Computing and Teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities

Guidance: CQRs and external data hosting infrastructure providers should have a documented mobile computing policy that identifies requirements that users of such devices should consider. These additional requirements should include physical security of the mobile device; access controls on the mobile device; health information data protection; and anti-malware protection.

The policy should outline when and where mobile devices should be used and should give advice to the user in how to ensure that the health information accessed is not compromised.

Teleworking should only be authorised if it is believed that sufficient controls are in place to secure the health information being accessed and that a legitimate business benefit is realised.

Teleworking can cross national borders, e.g. a health practitioner could be connecting from a hotel in a foreign country, and these legal and ethical considerations need to be taken into account when designing and deploying CQR information systems.

Architectural Impacts: Infrastructure Security Service; System Management Service

6.8. Information systems acquisition, development and maintenance

6.8.1. Security requirements of information systems

Objective: To ensure that security is an integral part of information systems.

Guidance: Security requirements should be addressed in the specifications, analysis and/or design phases and expert advisors should be consulted when implementing new or significant changes to health information systems.

Accurate records should be maintained to show traceability from original business requirements to actual configuration and implementation, including appropriate justification and authorisation.

System requirements for information security and processes for implementing security should be integrated in the early stages of information system projects.

Controls introduced at the design stage are significantly cheaper to implement and maintain than those included during or after implementation.

Architectural Impacts: Application Service; Channel Service; Software Service.

6.8.2. Correct processing in applications

Objective: To prevent errors, loss, unauthorised modification or misuse of information in applications.

Guidance: There may be cases when duplicate records have been created for a subject of care. For future -heath purposes, it is best to merge these records. Merging of records must be performed with the greatest of care so should use skilled personnel to do so, and it is preferred if the systems used support tools that facilitate merging with low susceptibility to error.

Software applications used in a health organisation need to be capable of providing automatic validation of input. For example, a date field should be defined to only contain dates, and the format of the date should be defined; a name field should not be capable of having numeric characters. The actual validation required for each health organisation may vary, and should be defined through the analysis phase of an implementation project.

As well as providing an ongoing record of client care, medical records are an important legal document. Consequently, documentation errors should be identified, but information should not be deleted from a healthcare record.

National Privacy Principle 6. Access and Correction states that:

- If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation must take reasonable steps to correct the information so that it is accurate, complete and up-to-date
- If the individual and the organisation disagree about whether the information is accurate, complete and up-to-date, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to do so
- An organisation must provide reasons for denial of access or a refusal to correct personal information.

The design and implementation of applications should ensure that the risks of processing failures leading to a loss of integrity are minimized. Specific areas to consider include:

- the use of add, modify, and delete functions to implement changes to data
- the procedures to prevent programs running in the wrong order or running after failure of prior processing
- the use of appropriate programs to recover from failures to ensure the correct processing of data
- protection against attacks using buffer overruns/overflows.

An assessment of security risks should be carried out to determine if message integrity is required and to identify the most appropriate method of implementation.

At a minimum, message integrity should be used when transferring health information between organisations or other untrusted entities.

Before relying on information presented by a health information system, health professionals should be shown sufficient information to ensure that the subject of care they are treating matches the information displayed.

Specific requirements for identifying subjects of care should be based on the assessment of risk.

Health information hard copies should make it possible to confirm that the printout is complete - e.g. printing the number of pages expected "Page 3 of 5".

In providing data for non-clinical care purposes, organisations should ensure that they have an appropriate authority for doing so. Healthcare organisations should also consider stipulating the terms and conditions of use, storage and destruction of the data.

Architectural Impacts: Application Service; Channel Service; Software Service

6.8.3. Cryptographic Controls

Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

Guidance: A policy on the use of cryptographic controls for protection of information should be developed and implemented. This should include, but not be limited to, guidance on the use of digital certificates in healthcare and the management of cryptographic keys.

Keys to digital certificate should be protected. If the key is compromised, it is possible to obtain access to health information secured by any certificate.

Certificate issuing authorities or holders of private keys should ensure keys are protected accordingly. The following are examples of considerations:

- audit logs
- key management - how keys are stored, revoked, transferred, installed
- maintenance
- objectives of the keys and their use
- system description
- topology.

For further information, see the Secure Messaging Component of the NESAF Implementer Blueprint.

Architectural Impacts: Data Encryption Service

6.8.4. Security of system files

Objective: To ensure the security of system files.

Guidance: There should be procedures in place to control the installation of software on operational systems. Procedures should include, but not be limited to:

- testing before implementing into production
- a rollback strategy in case of error in the software release
- documentation of software versions

- authorisation to install.

Where possible, identifying information should be de-identified prior to being used for testing purposes. If personal or health information is used for testing purposes, all sensitive details and content should be removed or modified beyond recognition before use. The following guidelines should be applied to protect health or personal information, when used for testing purposes:

a) the access control procedures, which apply to operational health information systems, should also apply to test application systems

b) there should be separate authorisation each time operational information is copied to a test application system

c) operational information should be erased from a test application system immediately after the testing is complete

d) the copying and use of operational information should be logged to provide an audit trail.

To prevent the introduction of unauthorised functionality and to avoid unintentional changes to applications, source code of an application should be controlled. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries on secured storage.

Architectural Impacts: Application Service; Channel Service; Software Service

6.8.5. Security in development and support processes, and technical vulnerability management

Objective: To maintain the security of application system software and information and to reduce risks resulting from exploitation of published technical vulnerabilities.

Guidance: Changes to CQR or external data hosting infrastructure provider information or ICT systems should be managed through formal processes which include an assessment of the impact (positive or negative) that the change may have on the organisation, the responsibilities and method of approval.

Without change management, it may be possible for inexperienced employees or third parties to make an unauthorised change to a system that has unknown disastrous impacts.

The change management process described previously should also include a post-implementation review of the status of the change prior to confirmation of the change's success.

One or several user representatives should be assigned to test the availability and performance of the system.

If the change does not pass the technical review, it should be rolled back to the previous state.

Except for specifically customisable fields and configuration settings, other modifications to software are discouraged. If an application does need to be modified then strict quality and security testing should be implemented to ensure the same, or higher level of quality as the original software. All original software should be retained in its original version in case of rollback.

The following should be considered to limit the risk of information leakage

- scanning of outbound media and communications for health information

- making use of reputable systems and software
- regular monitoring of personnel and system activities, where permitted under existing legislation or regulation
- monitoring resource usage in computer systems.

CQRs should consider the following points when using external data hosting infrastructure providers:

- licensing arrangements, code ownership, and intellectual property rights
- certification of the quality and accuracy of the work carried out
- escrow arrangements in the event of failure of the third party
- rights of access for audit of the quality and accuracy of work done
- contractual requirements for quality and security functionality of code
- testing before installation to detect malicious and Trojan code.

The management of vulnerabilities in a CQR's infrastructure is an important part of the overall information security management guideline. A CQR's vulnerability management process should incorporate:

- asset inventory and security baseline - identify the organisation's systems and define a baseline (minimum acceptable standard of security controls) for each group of assets or technology
- monitor for vulnerability announcements, patch updates and other remediations. This information can be obtained by subscribing to reputable sources such as the Australian Computer Emergency Response Team (AusCERT) or the Common Vulnerabilities and Exposures (CVE) http://cve.mitre.org/)
- analyse and Prioritise the remediations for specific information systems. For instance, an internet facing system which has been determined to have a Critical vulnerability should be prioritised for remediation
- remediate - apply the patch or other remediation and verify that the vulnerability has been remediated
- report on the status to information security governors.

Architectural Impacts: Application Service; Channel Service; Software Service; Infrastructure Security Service

6.9. Information Security Incident Management

6.9.1. Reporting information security events and weaknesses

Objective: To ensure that information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Guidance: Organisations should inform the subject of care whenever their personal information has been unintentionally disclosed.

Amongst other areas of interest, Information Security Incident Management Procedures should cover:

- planning and preparing for information security incidents

- detection and reporting of information security events or weaknesses which may become incidents.

Consider referring to *Australian Standard for Information Security Incident Management AS27035* for further guidance.

Architectural Impacts: Infrastructure Security Service; System Management Service

6.9.2. Management of incidents and improvements

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.

Guidance: Information Security Incident Management Procedures should cover:

- planning and preparing for information security incidents
- detection and reporting of information security events or weaknesses which may become incidents
- assessment of the incident and decision making
- response - both immediate and later responses, which may include forensic analysis
- lessons learnt
- reporting and review.

Consider referring to Australian Standard for Information Security Incident Management AS27035 for further guidance.

The analysis of "Lessons Learnt" should include:

- an analysis of the underlying (root) cause of the incident
- any requirements for new or changed information security controls (consider both technical and non-technical including policy guideline changes)
- any required update to the Information Security Risk Register
- any required changes to the Incident Management Procedure including any required tools or capabilities.

Where identified as required for forensic purposes, some further investigation may be required after the incident has been controlled.

The analysis should involve the use of IT-based investigative/monitoring techniques and tools, which are accompanied by supporting documented procedures. The aim of the forensic analysis is to review the designated information security event or incident in more depth. External assistance (through certified Forensic Analysts or law enforcement organisations) will usually be required to ensure that any chain of evidence is maintained.

Architectural Impacts: Infrastructure Security Service; System Management Service.

6.10. Information security aspects of business continuity management

6.10.1. Including information security in the business continuity management process

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

Guidance: Business continuity management within CQRs may include health crisis management planning as appropriate.

In an e-health environment, planning for the continuity of IT services becomes especially important. The organisation should look at any single points of failure of the electronic services and determine how they would conduct health care in the event of an IT outage. There are often manual workarounds in place which should be documented and tested regularly.

Risks to business interruptions, specifically through the unavailability information or information systems, should be formally identified and assessed in accordance with the NESAF Business Blueprint.

The Australian Standard for Risk Management, AS31000, contains further detailed guidance on Risk Management.

The Australian Standard for Business Continuity - Managing Disruption Related Risk may provide further information.

The business continuity planning process should include:

a) identification and agreement of all responsibilities and business continuity procedures

b) identification of the acceptable loss of information, services or people

c) implementation of the procedures to allow recovery and restoration of CQR operations and availability of information in required time-scales; particular attention needs to be given to the assessment of internal and external business dependencies and the contracts in place

d) operational procedures to follow pending completion of recovery and restoration

e) documentation of agreed procedures and processes

f) appropriate education of staff in the agreed procedures and processes, including crisis management

g) testing and updating of the plans.

A business continuity guideline within a CQR would usually consist of:

1. The organisation's Business Continuity Plan. This should be the main document and include when to activate the plan (disaster declaration) and other governance details.
2. Larger CQRs may also have specific BCP's for each division or unit, for instance IT Service Continuity Plan; HR Continuity Plan.
3. Emergency Response Procedures - this is a legislative requirement and includes evacuation and other facility specific information.

4. Disaster Recovery Plans - usually IT specific, these are plans and procedures advising how to recover IT services in the event of a disaster.

CQRs need to make sure the plans are tested on a regular basis. The tests should build upon one another, starting from desktop testing (all test personnel sitting at a desk) to modular testing (testing individual components of the plan) to a full rehearsal (testing that the organisation, personnel, equipment, facilities, and processes can cope with interruptions).

Results of the testing may result in an update of the plan/s.

Architectural Impacts: Infrastructure Security Service; System Management Service

6.11. Compliance

6.11.1. General

Objective: Establish a graduated compliance auditing guideline.

Guidance: In the regulated and audited environment of CQR organisations, those responsible for the governance of information security should set a goal to establish a multi-tiered compliance guideline.

At the bottom layer is self-audit by process owners and managers. Thereafter, there should be an independent internal audit followed by external audits by qualified auditors or assessors.

6.11.2. Compliance with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

Guidance: As each state and territory may have differing legislative requirements, each health care organisation needs to specifically identify legislation or other regulatory or contractual requirements and procedures that support the organisation's compliance to such.

Health records should be protected from misuse and loss and from unauthorised access, modification or disclosure.

The *NESAF Security and Access Guideline, Implementer Blueprint* contains specific details around Compliance within each Service Component.

Relevant Privacy (state or federal) legislation should be complied with at all times by health organisations.

Refer *NESAF Implementer Blueprint for Consent Management Service Component.*

Management should approve the use of information processing facilities.

If any unauthorised activity is identified by monitoring or other means, this activity should be brought to the attention of the individual manager concerned for consideration of appropriate disciplinary and/or legal action.

Consider seeking legal advice prior to implementing monitoring of employee activities.

At log-on, a warning message should be presented to indicate that the information or information system being accessed is owned by the organisation and that unauthorised access is not permitted.

6.11.3. Compliance with security policies and standards and technical compliance

Objective: To ensure compliance of systems with organisational security policies and standards

Guidance: Managers should be responsible for ensuring that the employees and third parties that report to them are compliant with information security policies. This should be both proactive (regular reviews) and reactive (reporting of weaknesses or events when they happen).

If any non-compliance is found as a result of a review, managers should:

a) determine the causes of the non-compliance

b) evaluate the need for actions to ensure that non-compliance do not reoccur

c) determine and implement appropriate corrective action

d) review the corrective action taken.

Employees or third parties responsible for the maintenance and operation of IT systems should ensure that checks are run regularly. Such testing may be performed internally or by external assessors, using automated tools or manually.

Where vulnerability scanning or penetration testing techniques are used, the assessor should be qualified as damage may be caused if not used correctly

6.11.4. Information systems audit considerations in a health environment

Objective: To maximise the effectiveness of and to minimise interference to or from the information systems audit process.

Guidance: When a CQR's systems are being audited, the following need to be considered to protect health or personal information.

- audit requirements and scope should be agreed with appropriate management
- checks should be limited to read-only access to software and data
- access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements
- resources for performing the checks should be explicitly identified, made available and authority documented and approved
- all access should be monitored and logged to produce a reference trail and the use of timestamped reference trails should be considered for critical data or systems
- all procedures, requirements, and responsibilities should be documented
- the person(s) carrying out the audit should be independent of the activities audited.

7. Glossary

Term	Definition
Access Control	A means of controlling access by users to computer systems or to data on a computer system.
THE COMMISSION	Australian Commission on Safety and Quality in Health Care.
Asset	Anything that has value to an organisation. [AS27799]
Authentication	Means that one can verify whether the sender is who they say they are. [RACGP1]
Availability	Refers to the property of being accessing and usable on demand by an authorised entity. [NESAF; AS27799]
Centre of excellence	A small set of providers (e.g. Universities) that may be responsible for the implementation, management and operations of a discrete number of CQRs. Their functions would include responsibility for the business functions of each CQR in accordance with the directions set by the relevant board/governance arrangements for each CQR; recruitment and management of CQR staff; ICT application development, support and maintenance. Each of these centres would employ a standardised approach to the hosting / creation of the CQRs under their control which may involve internal development and deployment of ICT infrastructure, or contracting an external ICT data hosting provider through a third party agreement to support this function. This approach may vary from centre to centre.
CoE	Centre of excellence.
Confidentiality	Refers to the property that information is not made available or disclosed to unauthorised individuals, organisations, entities or processes.
CQR	Clinical Quality Registry.
Data Hosting Infrastructure	For the purpose of this document, data hosting infrastructure refers to capacity and/or capability of ICT infrastructure such as data hosting services, hardware and software applications.

Term	Definition
Denial of service	An attack that results in preventing authorised access and availability of organisational information/services/resources.
External data hosting infrastructure provider	In the context of this document, an external data hosting infrastructure provider refers to organisations that provide technology infrastructure such as hosting services, hardware or applications, to CQR cenres of excellence and standalone clinical quality registries through a third party service provider arrangement.
Encryption	Data is electronically 'scrambled' so that it cannot be read unless the information is decrypted. [RACGP1]
Firewall	Device(s) designed to prevent unauthorised transmission to or from a private network based upon a set of rules. Used to protect networks from unauthorised access while permitting legitimate communications to pass through
Health information system	Repository of information regarding the health of a subject of care in computer-processable form, stored and transmitted securely, and accessible by multiple authorised users. [AS27799]
Healthcare	Any type of service provided by professionals or paraprofessionals with an impact on health status. [AS27799]
Healthcare organisation	Generic term used to describe many types of organisations that provide healthcare services.[AS27799)
Information security	Preservation of confidentiality, integrity and availability of information.
Integrity	Refers to the property that data has when it has not been altered or destroyed, or a system has when it can perform its intended function in an unimpaired manner, free from deliberate or accidental unauthorised manipulation of the system. [NESAF; AS27799]
NEHTA	National eHealth Transition Authority.
NESAF	National E-Health Security and Access Guideline.

Term	Definition
Malicious code	Programs such as viruses and worms designed to exploit weaknesses in computer software and replicate and/or attach themselves to other software programs on a computer or a network.
Personal health information	Information about an identifiable person which relates to the physical or mental health of the individual or to provision of health services to the individual. [AS27799]
Register	The file of data concerning all cases of a particular disease or other health-relevant condition in a defined population such that the cases can be related to a population base. With this information, incidence rates can be calculated. If the cases are followed up, information on remission, exacerbation, prevalence and survival can also be obtained.
Registration	The system of ongoing registration for individuals entered into a register. For the purpose of this document, the functions performed by a CQR are defined in Figure 8 in Appendix A and include data custodianship, provider enrolment, data collection, data quality management and data analysis and outcome reporting.
Risk	The probability that a given threat will exploit a given vulnerability. [HB174]
Risk assessment	The process of identifying risks to a business and determining the probability of occurrence, the resulting impact, and identifying actions that would treat the risk.
Threat	An action or event that may result in a detrimental outcome to a system or information asset. [HB174]
Vulnerability	A weakness that can be exploited that may cause damage to a system or information assets.[HB174]

Appendix A. - Clinical Quality Registries

A.1. Overview (what is a clinical quality registry?)

Clinical quality registries are clinical databases that systematically collect health-related information on the quality, safety and outcome of care provided to individuals who are:

- treated with a particular surgical procedure, device or drug, e.g. joint replacement;
- diagnosed with a particular illness, e.g. stroke; or
- managed via a specific healthcare resource, e.g. treated in an intensive care unit.

The purpose of clinical quality registries is to improve the quality of health care by routinely collecting, analysing and reporting on information about the care provided to patients and how well that care is being provided. In particular, clinical quality registries provide specific information about:

the appropriateness of health care (whether the care delivered to patients is based on the best available evidence) and,

the effectiveness of health care (measured by the degree to which the care benefits the patient).

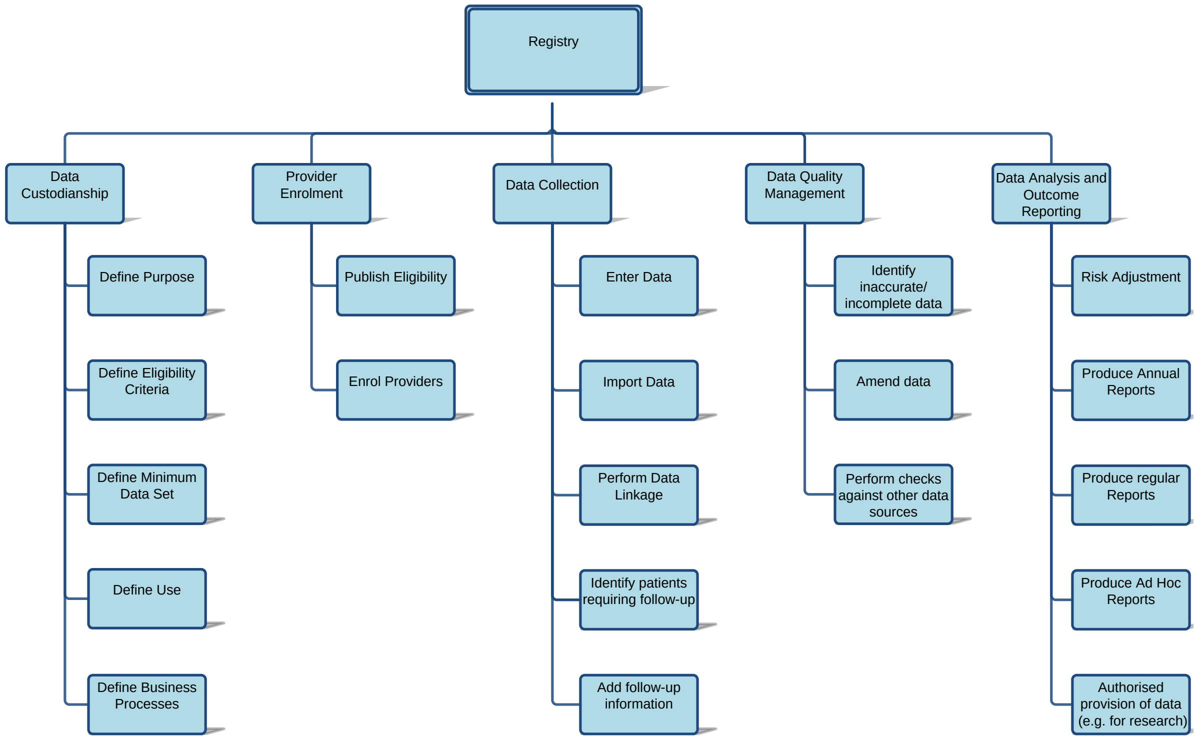
This information is used to inform improvements in the healthcare system.

The Centre of Research Excellence in Patient Safety (CREPS) at Monash University supports a Registries Interest Group, and provides information on clinical quality registries on their registries web page.

A.2. CQR functions (what does a CQR do?)

The high level functions ordinarily undertaken by clinical quality registries are illustrated in Figure 8 and brief descriptions of the main functions are provided below.

Figure 8: Functions of clinical quality registries



A.2.1. Data Custodianship

Australian clinical quality registries are developed with a clear and precisely defined purpose that relates to questions the CQR stakeholders want answered through the CQR, both immediately and in the future. The function of data custodianship incorporates:

- clearly and precisely defining the purpose of the CQR
- defining the eligibility, or common circumstance, that determines inclusion in the CQR
- defining the minimum data set required to meet their core purpose;
- defining how data will be used, through clear statements of data ownership and custodianship and establishing data access and reporting policies that take account of requirements imposed by Ethics Committees and legislation
- defining and developing the business processes and procedures that will be used for data collection, lodgement, storage, management and reporting.

A.2.2. Provider enrolment

Provider enrolment relates to enrolling participating institutions, units and/or clinicians as providers of data to an Australian clinical quality registry. The function incorporates:

- the publication of eligibility criteria that identifies the purpose of the CQR to prospective participating institutions or clinicians
- enrolling providers to enable participating institutions and/or clinicians to access the system.

A.2.3. Data collection

Data collection relates to the capture of information from eligible patients within a defined clinical population. Some clinical registries collect data for only a short time period, such as for a single episode of care (e.g. following admission to an Intensive Care Unit), while others follow patients until they no longer present for treatment or die (e.g. in the case of people with bleeding disorders or cystic fibrosis).

Out of hospital outcomes are commonly determined by contacting participants at a defined time after discharge and asking a small number of key questions. Alternately, registries contact the participating hospital or clinician to obtain outcome information.

Data collection incorporates:

- entering data into the CQR e.g. through the use of electronic forms entered through a CQR portal, or offline forms which are uploaded securely to the CQR in a batch
- importing data through batch uploads, direct feeds from data collected as part of a patient's medical record and hospital administration systems (e.g. from pathology reports, operating theatre systems, emergency department systems and, patient administration systems) and receipt of information through messages (e.g. HL7 pathology reports)

- performing data linkage to other information sources that can provide additional outcome information that cannot be derived from the CQR along e.g. the National Death Index, infection surveillance systems
- identifying patients who need to be followed up in order to collect additional information relating to the outcome of clinical care
- adding follow-up information to the CQR obtained through data linkage or through contact with patients, participating institutions or clinicians.

A.2.4. Data quality management

A strong and ongoing focus on data quality is a fundamental function of the work undertaken by Australian clinical quality registries. To facilitate the use of CQR data for benchmarking outcomes and assessing compliance with best practice guidelines, data must be accurate and reliable in order to maintain the confidence of providers and recipients of CQR information. Key components of data quality management include:

- identification of inaccurate/incomplete data to enable feedback to be provided to data collectors to assist them to improve data collection accuracy and reliability
- enabling CQR users to amend inaccurate or incomplete data that are identified
- performing checks against other data sources, such as routine administrative collections, to determine the completeness of the CQR's collection and to validate information contained in the CQR.

A.2.5. Data analysis and outcome reporting

Timely analysis of data and the provision of outcome data without delay to health care providers, hospitals, health jurisdictions, professional accreditation bodies and the public, underpin the purpose of clinical quality registries. To be effective in driving healthcare improvements, clinical quality registries must be able to provide reports as soon as possible to ensure that the findings are relevant to contemporary clinical care. This function incorporates:

- risk adjustment – the statistical process of identifying and adjusting for variation in outcomes resulting from differences in patient characteristics or risk factors
- production of annual reports that detail CQRs' clinical and corporate findings
- production of regular reports to clinicians and relevant stakeholders to enable proactive monitoring of the provision of care
- production of ad hoc reports by enabling authorised users to specify defined report parameters and produce reports on their own unit's/patient's data
- authorised provision of data for approved purposes such as the secondary use of data for research, or for use in statistical software packages to support complex data analysis.

A.3. CQR architecture (how is a CQR constructed?)

As part of the development of national arrangements for Australian clinical quality registries, the National E-Health Transition Authority and the Australian

Commission on Safety and Quality in Health Care have developed a reference architecture and a logical design for Australian clinical quality registries in order to provide pragmatic guidance to organisations wishing to embark on developing or upgrading a clinical quality registry.

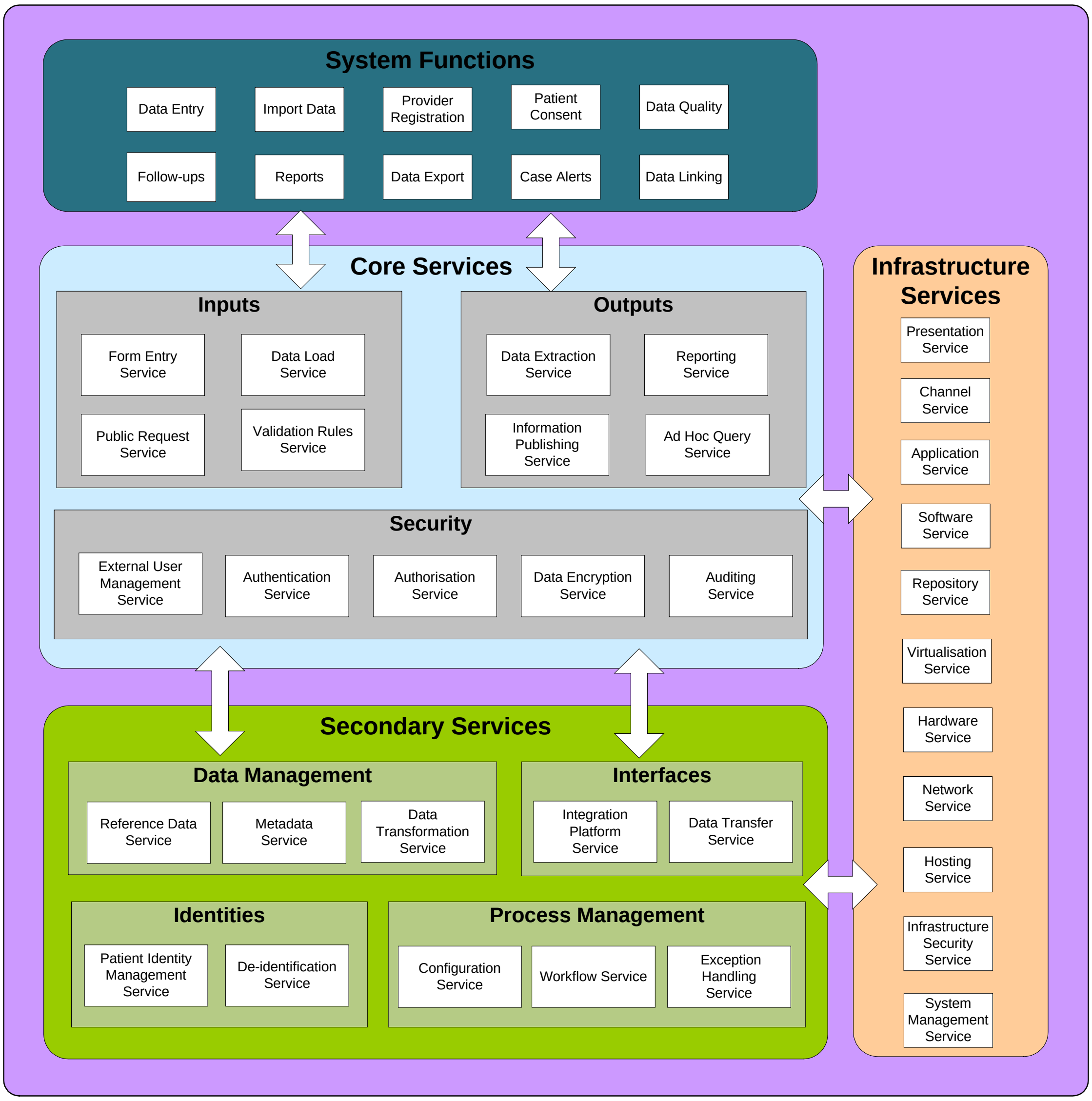


Figure 9: Conceptual system services

The conceptual system services identified in the reference architecture that fulfil the business requirements for Australian clinical quality registries are illustrated in Figure 9. System functions at the top of the diagram represent the main areas of functionality that a clinical quality registry system provides for its users. The system functions are delivered by a number of services.

1. The core services consist of input services (that support data entering the system), output services (that support the data being retrieved or exported from the system) and security services (that provide user management, authentication, authorisation and data encryption functionality).
2. The secondary services provide data management functionality, interfaces with external systems, patient identity management and process management functionality.

3. The infrastructure services provide the underlying platform that the clinical quality registry system operates on.

Each of the services contained in Figure 9 are described fully in the CQR Reference Architecture document[12].

Figure 10 represents the logical deployment proposed in the Clinical Quality Registries Logical Design document[13].

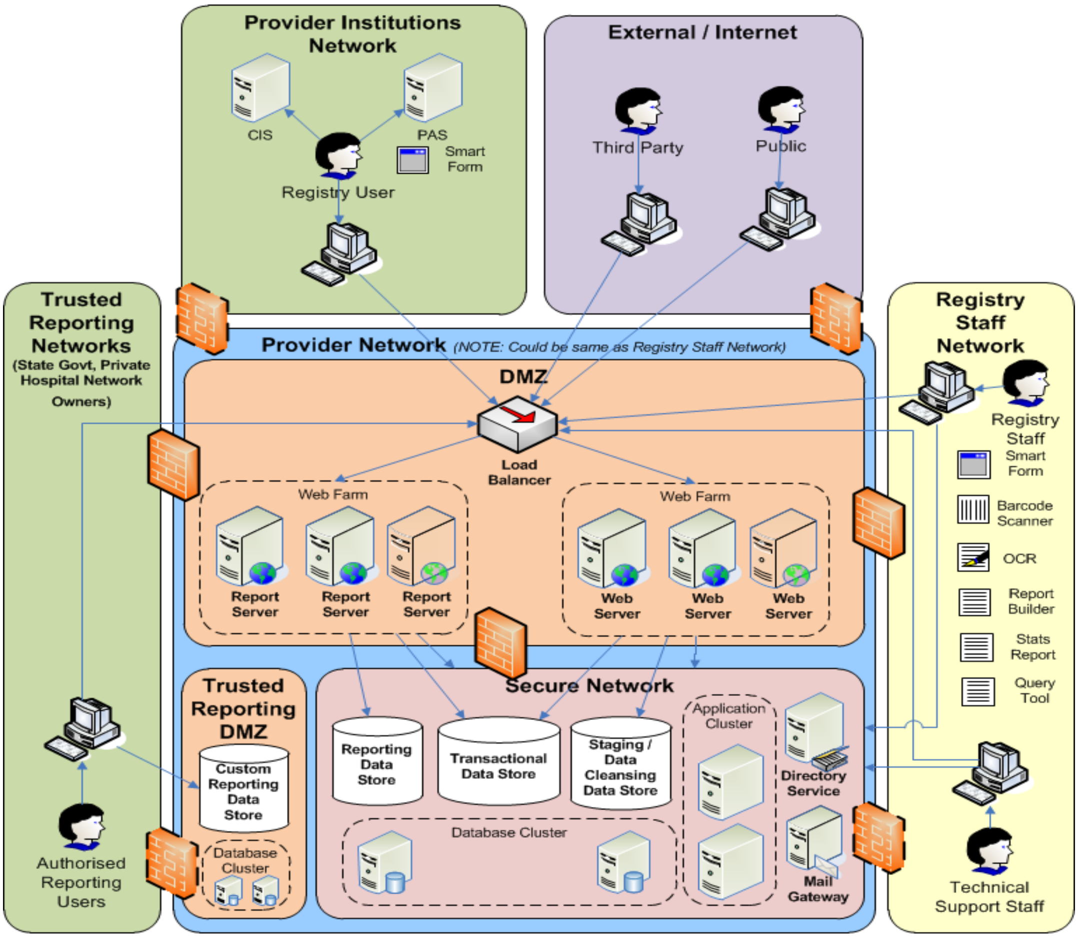


Figure 10: Proposed CQR logical deployment

[12] Australian Commission on Safety and Quality in Health Care. Reference Architecture: National Clinical Quality Registries (CQR1132). October 2011.

[13] Australian Commission on Safety and Quality in Health Care. Clinical Quality Registries. Logical Design. Draft. February 2012.

Key features of the logical infrastructure design include:

- hosting of the database tier and other infrastructure services (such as the mail and directory services) within a secure sub-network within the data centre which cannot be accessed directly by external clients
- web and reporting services hosted in a sub-network, known as a DMZ (de-militarised zone) or perimeter network, which acts as a security buffer between external clients and the secured sub-network
- a set of firewalls to ensure that only servers within the DMZ can communicate with servers in the secured sub-network
- CQR staff users access the CQR servers from the CQR Staff Network. This network may be part of the DMZ sub-network, but in most cases will be a separate network
- to facilitate automatic contribution of data from authorised hospital systems, a trust relationship can be established between the External System's network and the CQR data centre via firewall configuration. Web server certificates can also be used to authenticate external contribution systems
- to support the direct connection from third-party reporting tools to the reporting database in a secure manner, a copy of the reporting database can be hosted in a Trusted Reporting DMZ sub-network. A firewall will be used to ensure that only authorised users and workstations are permitted to connect to the Trusted Reporting DMZ sub-network.

Appendix B. CQR Principles

Strategic Principles for a National Approach to Australian Clinical Quality Registries[14]

Principle 1: Consumers, clinicians, management and governments receive regular reports from Clinical Quality Registries on appropriateness of care (process and compliance with guidelines), and effectiveness of care (patient outcomes) to support ongoing improvement of health care in Australia.

Principle 2: Clinical Quality Registries, operating in close coordination with expert national clinical groups, provide an effective mechanism for:

- design of indicators of quality of care
- comprehensive data collection and analysis, and
- outlier management within a sound clinical governance guideline.

Principle 3: National data governance arrangements and best practice infrastructure provide support for comprehensive reporting, monitoring and management of clinical practice variance.

Principle 4: Where existing data flows do not support analyses of quality of care, Australian Clinical Quality Registries are efficient and effective in providing consumers, clinicians, management and government with information for managing and improving delivery of health services.

Principle 5: Dedicated investment in Australian Clinical Quality Registries supports infrastructure, data cleansing, reporting and analysis of quality of care, based on succinct datasets captured routinely by clinicians at the point of care.

Principle 6: Australian Clinical Quality Registries have sound governance arrangements with strong clinical leadership and a demonstrated guideline for quality improvement.

Principle 7: Prioritisation of Australian Clinical Quality Registry support is premised on gaps in existing data flows, the significance of the national burden of disease and the cost of interventions, the existence of variation in practice and outcomes, the ability to improve quality of care including reduction in practice variation, availability of national clinical leadership and consideration of existing data, and cost/benefit options.

Principle 8: Data governance for the collection, holding and analysis of patient-level, Australian Clinical Quality Registry information is managed as part of the national health information agenda, in a guideline that protects patient privacy and complies with regulation. National data governance arrangements are essential to making the data collection, ethics approvals and reporting activities of Australian Clinical Quality Registries more efficient.

Principle 9: A secure, future-proof and scalable Australian Clinical Quality Registry design and infrastructure should support and host multiple Registries. Efficiency and best practice are best achieved through the operation of a small number of Australian Clinical Quality Registry systems or centres.

Principle 10: Australian Clinical Quality Registries must meet the requirements of national operating principles.

[14] < http://www.safetyandquality.gov.au/internet/safety/publishing.nsf/Content/PriorityProgram-08_clinical1>

Operating principles for Australian Clinical Quality Registries

Attributes of Australian Clinical Quality Registries15

1. Australian Clinical Quality Registries must be developed with clear and precisely defined purposes aimed at improving the safety and/or quality of health care.

2. For Australian Clinical Quality Registries to provide the maximum value to the health system they must focus their core data collection on the essential elements required to serve their main purposes.

3. Data collected by Australian Clinical Quality Registries should be confined to items which are epidemiologically sound, i.e. simple, objective, and reproducible, valid (including for risk adjustment) and related to a specific case definition;

4. Methods used to collect data in Australian Clinical Quality Registries must be systematic, with identical approaches used at the different institutions contributing information.

5. Outcome determination should be undertaken at a time when the clinical condition has stabilised and the outcome can therefore be reasonably ascertained.

6. In determining the time to outcome assessment, Australian Clinical Quality Registries must consider the burden and cost of data collection together with the likelihood of loss to follow-up.

7. Australian Clinical Quality Registries must ensure that complete registry data are collected from the entire eligible population.

Data collection

8. The collection of data for an Australian Clinical Quality Registry should maintain an appropriate balance between the time and cost of data collection and the impact on patient care, particularly where clinicians are directly involved in data collection. The collection of data must not be an unreasonable burden on consumers, nor should it incur any cost to consumers.

9. Data capture should be performed as close as possible to the time and place of care by appropriately trained data collectors;

10. Data should be uniformly and easily accessible from the primary data source.

11. Standard definitions, terminology and specifications should be used in Australian Clinical Quality Registries wherever possible to enable meaningful comparisons to be made and to allow maximum benefit to be gained from linkage to other registers and other databases (if approved by relevant ethics committees, etc.).

12. Australian Clinical Quality Registries must use data dictionaries when they are established to ensure that a systematic and identical approach is taken to data collection and data entry. They need to publish eligibility criteria, metadata, data dictionaries, etc.

13. To avoid duplicating data capture, Australian Clinical Quality Registries should use data from existing data sources, including administrative data, where they are of a satisfactory quality.

Data elements

14. Australian Clinical Quality Registries should have the capacity to enhance their value through linkage to other disease and procedure registers or other databases.

15. Australian Clinical Quality Registries must collect sufficient patient identifying information to support the registry's stated purpose. Most clinical quality registries would require individually identifiable data, for which use of national Individual Healthcare Identifiers is recommended.

[15] < http://www.safetyandquality.gov.au/internet/safety/publishing.nsf/Content/PriorityProgram-08_clinical1>

16. Where patterns or processes of care have an established link to outcomes and process measures that are simple, reliable and reproducible, they should be considered for collection by Australian Clinical Quality Registries.

17. Where possible, outcomes should be assessed using objective measures. Where this is not possible, outcome should be assessed by an independent person and undertaken using standardised and validated tools.

Risk adjustment

18. Australian Clinical Quality Registries should collect objective, reliable co-variates for risk adjustment to enable factors outside the control of clinicians to be taken into account by the use of appropriate statistical adjustments.

Data security

19. To protect register data, Australian Clinical Quality Registries must utilise secure access controls and secure electronic transfer and electronic messaging systems.

20. The collection, storage and transmission of clinical registry data must be in line with relevant legislation, regulation, standards and guidelines.

Ensuring data quality

21. Australian Clinical Quality Registries must report as a quality measure the percentage of eligible patients recruited to the registry.

22. Australian Clinical Quality Registries must have a robust quality assurance plan which allows ongoing monitoring of the completeness and accuracy of the data collected.

23. Australian Clinical Quality Registry data should be checked in a sample of cases. This usually involves audit against source records. The sample size needs to be sufficient to produce reliable measures of data completeness and accuracy. The frequency of audits needs to be sufficient for data quality lapses to be identified promptly. Incomplete or inaccurate data should be identified by the data centre and remedied as soon as possible.

24. Australian Clinical Quality Registries should incorporate in-built data management processes such as data range and validity checks.

Organisation and governance

25. Australian Clinical Quality Registries must formalise governance structures to ensure accountability, oversee resource application, provide focus and optimise output from the registry.

26. Australian Clinical Quality Registries must establish policies to manage a range of contingencies arising from the analysis of data from the registry, which includes a formal plan ratified by the Registry Steering Committee to address outliers or unexplained variance, to ensure that quality of care issues are effectively addressed and escalated appropriately.

Data custodianship

27. Custodianship of clinical register data must be made explicit in Contracts and/or Funding Agreements. Australian Clinical Quality Registries should make clear statements of data ownership and data custodianship publicly available.

28. Data access and reporting policies for Australian Clinical Quality Registries must be made available to persons wishing to use register data. Australian Clinical Quality Registries should make data access and reporting policies publicly available.

29. Third parties wishing to access data and publish findings must seek approval from the Registry Steering Committee and obtain relevant Institutional Ethics Committee endorsement where identified or re-identifiable data is sought.

Ethics and privacy

With the exception of instances where data collection has been mandated through legislation or enabled through regulation or legislation:

30. Institutional Ethics Committee (IEC) approval must be obtained to establish the Australian Clinical Quality Registry.

31. Registry personnel must be familiar with and abide by the requirements set out in relevant privacy legislation, the National Statement on Ethical Conduct in Human Research and the Australian Code for the Responsible Conduct of Research.

32. Participants or their next of kin must be made aware of the collection of register data. They must be provided with information about the Australian Clinical Quality Registry, the purpose to which their data will be put and provided with the option to not participate. This must be at no cost to the register participant.

33. Where projects are undertaken using registry data, IEC approval must be sought unless the project falls within the scope of an institution’s quality assurance activity.

Information output

34. Data from Australian Clinical Quality Registries must be used to evaluate quality of care by identifying gaps in best practice and benchmarking performance.

35. Australian Clinical Quality Registries must report without delay on risk adjusted outcome analyses to institutions and clinicians.

36. Australian Clinical Quality Registries should verify data collected using a formalised peer review process prior to publishing findings.

37. Clinicians and/or staff at contributing units should have the capacity to undertake ad hoc analyses of their data to enable monitoring of clinical care.

38. Australian Clinical Quality Registries must produce a publicly-accessible aggregated annual report detailing clinical and corporate findings.

39. Australian Clinical Quality Registry reports should be produced according to a strict timeline and should demonstrate funding to enable this to occur.

40. Australian Clinical Quality Registries must have documented procedures, including methods employed, for reporting on quality of care, including addressing outliers or unexplained variance.

Resources and funds

41. Australian Clinical Quality Registries should demonstrate sufficient funding is allocated to allow data collection, reporting and the institution of strong quality assurance procedures.