AUSTRALIAN COMMISSION
ON SAFETY AND QUALITY IN HEALTH CARE

National consultation version

Attachment 2: Australian CQR security compliance guideline Second Edition

December 2022

ISBN: 978-1-922880-06-2

Suggested citation:
Australian Commission on Safety and Quality in Health Care, Framework for Australian clinical quality registries - a quality standard for clinical outcome data collections and reporting. Attachment 2: Australian CQR security compliance guideline Second Edition. Sydney. ACSQHC, December 2022.

Australian Commission on Safety and Quality in Health Care
GPO Box 5480
Sydney NSW 2001
Email: mail@safetyandquality.gov.au.

Contents

List of Tables

List of Figures

1. Introduction

1.1. Purpose

The purpose of the *Security Compliance Guideline for Clinical Quality Registries* (the Guideline) is to provide the security compliance checklist and guidance for Australian clinical quality registries (CQRs).

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 CQR against appropriate security standards and techniques current, as at November 2022.

1.3. About the *Guideline*

The Guideline builds on the work of the Australian Digital Health Agency. *National E-Health Security and Access Framework – v4.0*. and current 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 information security infrastructure using a risk-based approach.

The Guideline has been developed in consultation with the Commission's Clinical Quality Registries Framework Review Advisory Group and a group of CQR experts in health data systems.

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 Framework and ISO/IEC 27002.

2. Considerations in securing Clinical Quality Registries

This section defines the key elements of information security sets out the context for information security for national CQRs including 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. Definitions of key elements of information security

The information held by CQRs is a core health data 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 below[1]:

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 CQRs 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.

[1] Australian Digital Health Agency. *National E-Health Security and Access Framework – v4.0*.

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 (below) identifies the most common threats and associated vulnerabilities that may exist within the CQR environment:

- **Phishing**
  This attack is designed to steal sensitive information, such as username and passwords. Phishing attacks impersonate reputable websites, and personal contacts, which come in the form of immediate phishing e-mails or messages designed to look legitimate. Once the user clicks the URL or reply to the messages, you are prompted to enter your credentials, which then sends your data to the malicious source. The user may have the same credential that they are using to access the CQR system.

- **Virus or Malware or spyware attack**
  Attacks use many methods to get malware into a user's device via SMS or Email by asking user to click link to download. Once malware is installed, it can monitor user activities, send confidential data to the attacker, assist the attacker in penetrating other targets within healthcare provider IT network.

- **Password attacks**
  A hacker can gain access to the password information of an individual by 'sniffing' the connection to the IT network, guessing, or gaining access to the CQR System. An attacker can also guess a password in a random or systematic way.

- **SQL injection attack**
  SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behaviour.

To help fully identify threats that CQRs may encounter, please refer to section 4.4 of NESAF v4 - Business Blueprint v1.0.

Section 6 of this Guideline provides detailed guidance and explanation on each security control, categorised by security domain details the controls that will facilitate secure operation in an environment characterised by such threats.

2.3. Legislation and regulation

In Australia there is Commonwealth, state and territory and private health sector legislation, regulation, principles, and policies relating to privacy of personal health information.

Commonwealth Government agencies and the Australian Capital Territory (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 required to comply with 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. A summary of current legislation and health data custodial arrangements is also available on the Commission's website.

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[3] 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.

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

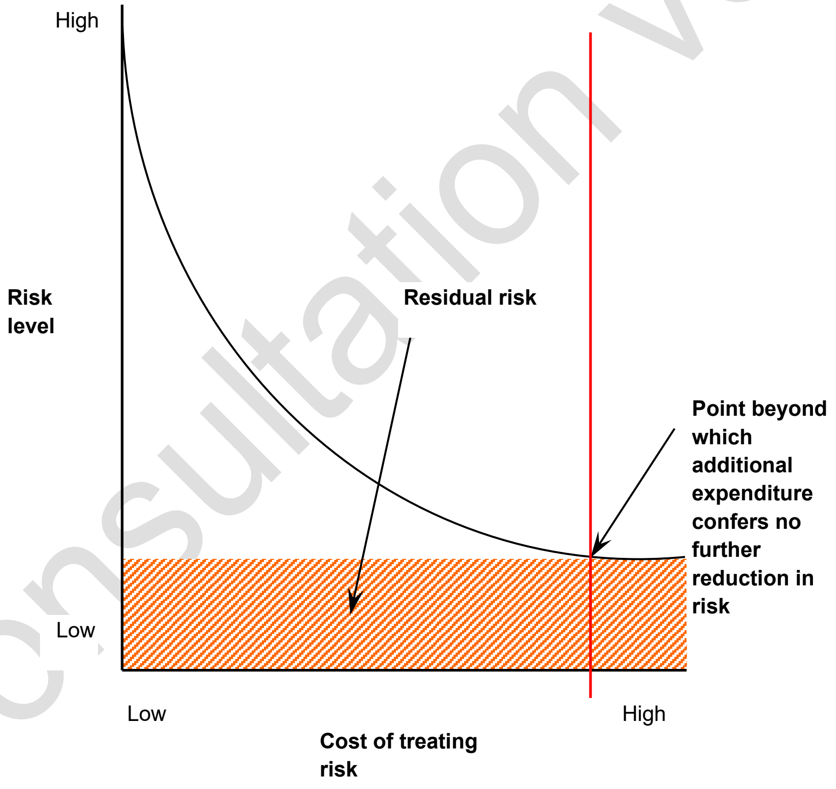
[3] Source: NESAF Business Blueprint, NEHTA 2011

- 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.

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 CQRs, two distinct infrastructure configurations or ‘models’, and risk profiles have been identified.

3.1. Infrastructure Models

This *Guideline* may be used to assess Australian CQRs operating in either of two organisational ‘models’, depending on whether or not they are co-located within a centrally hosted jurisdictional model other standalone model.

Within a centrally hosted jurisdictional model CQRs would benefit from the security infrastructure provided by national system operator and any existing global security certifications, such as ISO27001, and industry specific certifications. Risk profiles can be more readily assessed and ensure compliance to the security guidelines in this document.

3.2. Model 1 - Centrally hosted jurisdictional infrastructure

Model 1 identifies the proposed future state where all CQRs are established and operated in centrally hosted jurisdictional (at the level of the state and territory and Commonwealth) infrastructure.

Under future national arrangements, there would be a standardised approach to the hosting and development of the CQRs.

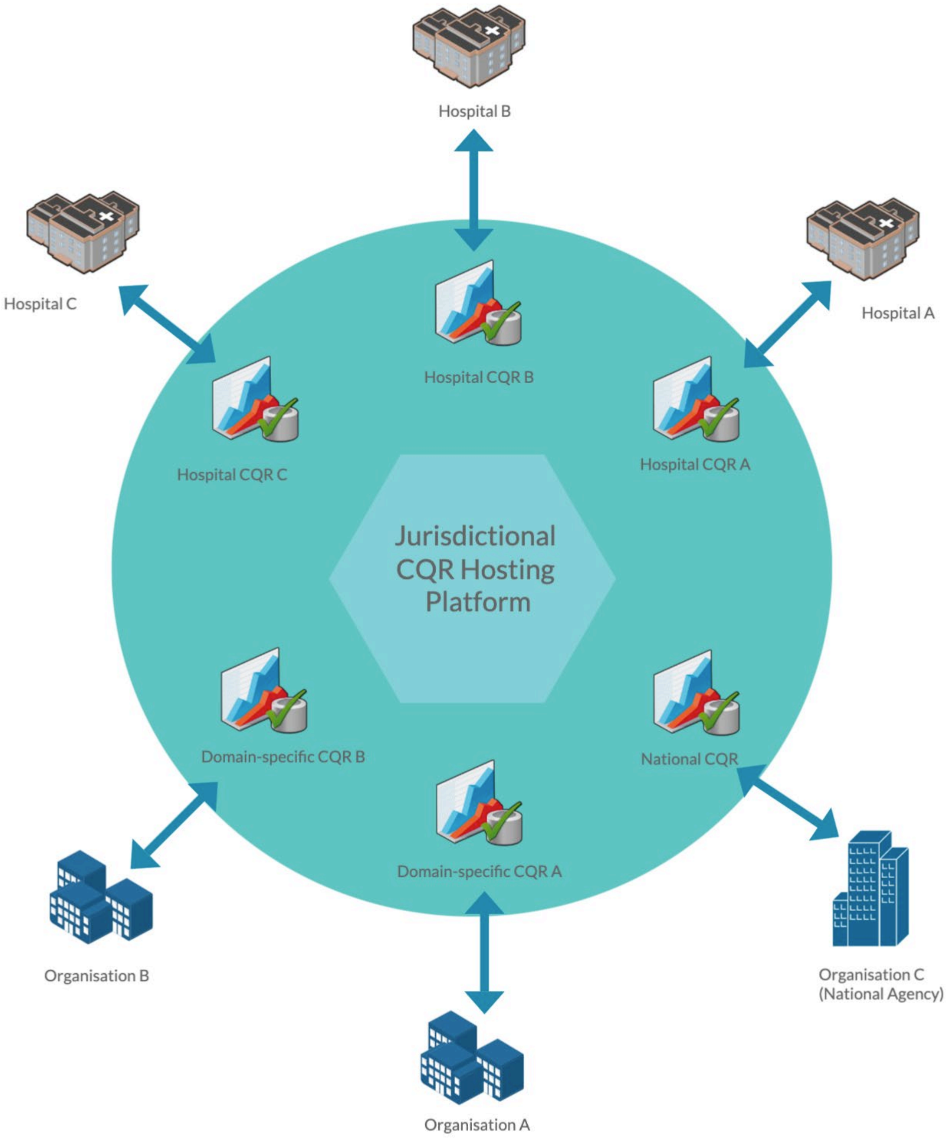
The technical infrastructure for the CQRs in prioritised clinical domains[4] centrally hosted within a jurisdiction[5] is illustrated in Figure 2.

This *Guideline* assumes that CQRs hosted centrally 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).

Figure 2: Centrally hosted jurisdictional CQRs

[4] Prioritised list of clinical domains for clinical quality registry development: Final report https://www.safetyandquality.gov.au/publications-and-resources/resource-library/prioritised-list-clinical-domains-clinical-quality-registry-development-final-report

[5] The Commonwealth of Australia and each state and territory is a jurisdiction.



3.3. Model 2 – Standalone CQRs

Model 2 describes the current situation in which a CQR is developed and operated as a standalone CQR. The CQR may have a technology infrastructure (‘data hosting’) platform that is hosted locally and maintained internally within existing health service organisation information systems (Figure 3) or externally through a third-party service provider, such as a university or another vendor. (Figure 4).

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 3: Standalone CQR with an internal data hosting platform

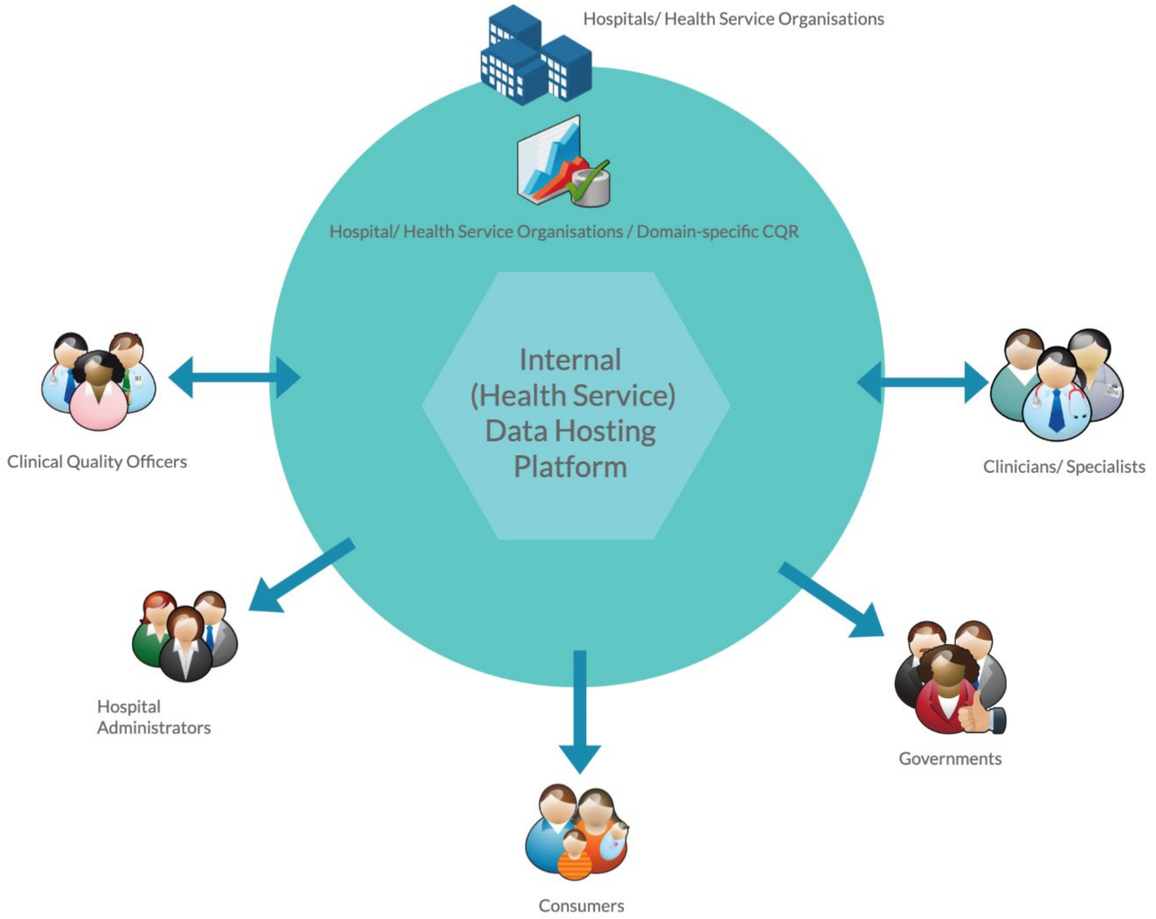
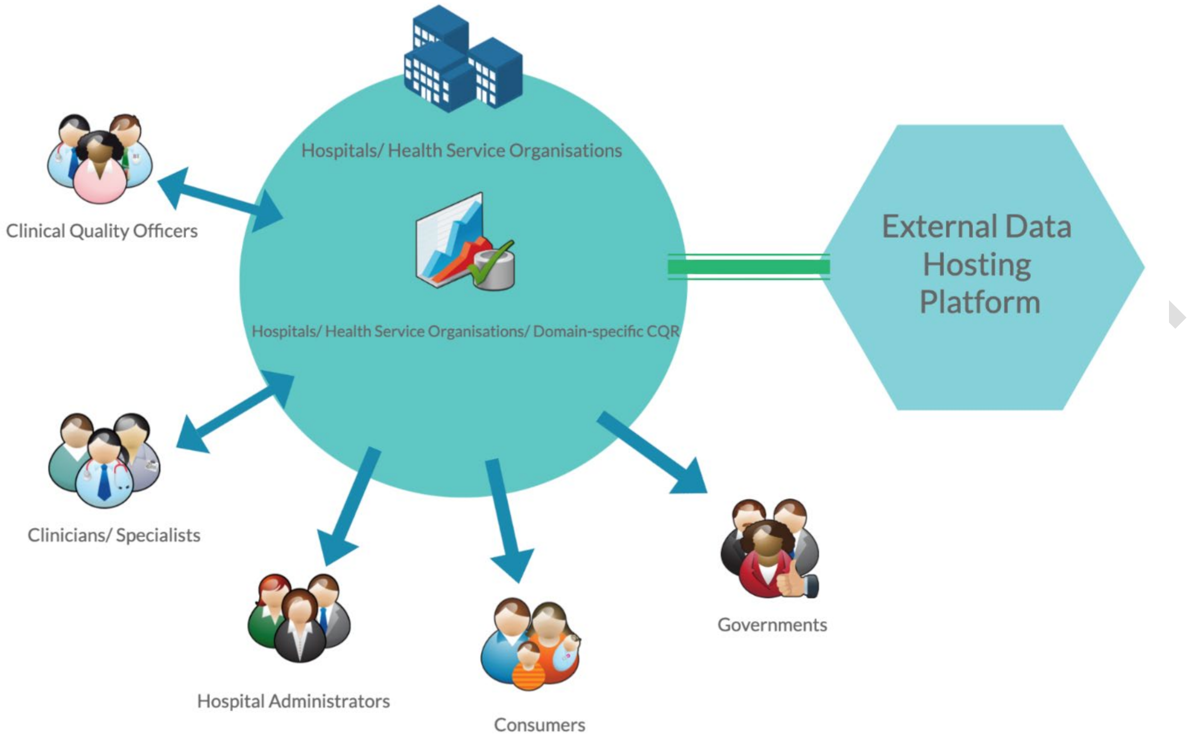

Hospitals/ Health Service Organisations
Hospital/ Health Service Organisations / Domain-specific CQR
Internal (Health Service) Data Hosting Platform
Clinical Quality Officers
Clinicians/ Specialists
Hospital Administrators
Governments
Consumers

Figure 4: Standalone CQR using an external data hosting facility


Hospitals/ Health Service Organisations
Clinical Quality Officers
External Data Hosting Platform
Hospitals/ Health Service Organisations/ Domain-specific CQR
Clinicians/ Specialists
Governments
Hospital Administrators
Consumers

3.4. 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’).

3.4.1 Summary of risk profiles

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

Overall, the greatest risks to CQRs data holdings are security breaches of confidentiality and the 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 1: Risk profiles

Profile	Infrastructure Model Type	Number of CQRs	Inherent Risk		
			Inherent Confidentiality Risk	Inherent Integrity Risk	Inherent Availability Risk
1	Centrally hosted jurisdictional infrastructure	Multiple	High	Medium	Medium
2	Standalone CQR(s)	Single or Multiple	Medium	Medium	Low

3.4.2. Risk profile for centrally hosted jurisdictional model

Table 2 outlines the nature and extent of information security risks associated with the centrally hosted jurisdictional model (future state) (refer to Model 1 in Section 3.1). National infrastructure 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 2 are reflected in the security compliance checklists in Section 5.

Table 2: National infrastructure 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 Central Administration staff) due to Central Administration Staff'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 Central Administration)	Unlikely	Major	High	Information Security Policy; HR Security; Information Security Organisation
4	Confidentiality	Changing to new Central Administration 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

No.	Factor	Risk	Likelihood	Impact	Risk	Security Domain
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 (e.g.: 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
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

No.	Factor	Risk	Likelihood	Impact	Risk	Security Domain
						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 led 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 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 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 cause 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

3.4.3. Risk profile for a standalone CQR

Table 3 outlines the nature and extent of information security risks associated with existing legacy CQRs hosted in a standalone environment (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 3 are reflected in the security compliance checklists in Section 5.

Table 3: 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
4	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

No.	Factor	Risk	Likelihood	Impact	Risk	Security Domain
5	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
6	Confidentiality	Breach of legislation due to Information used not in accordance with the purpose for which it has been collected (e.g.: violation of consent)	Unlikely	Moderate	Medium	Compliance; HR Security
7	Confidentiality	Theft of (non-portable) information systems containing confidential information	Unlikely	Moderate	Medium	Physical Security
8	Confidentiality	Authorised user inadvertently gives information to unauthorised user	Unlikely	Moderate	Medium	HR Security;
9	Integrity	Data integrity errors in bulk upload / external file transfers	Possible	Moderate	High	Information Systems Acquisition, Development and Maintenance
10	Integrity	Data quality errors through data entry from data entry person (transposition)	Unlikely	Insignificant	Low	Information Systems Acquisition, Development and Maintenance; HR Security

No.	Factor	Risk	Likelihood	Impact	Risk	Security Domain
11	Integrity	Malicious staff purposely change multiple records	Unlikely	Moderate	Medium	HR Security; Communications and Operations Management; Access Control
12	Integrity	Untrained/unskilled staff accidentally change multiple records	Unlikely	Moderate	Medium	HR Security; Access Control
13	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
14	Integrity	Message received or sent from unauthorised party	Unlikely	Moderate	Medium	Access Control; Communications and Operations Management
15	Integrity/Availability	Malware/viruses resulting in loss of availability/integrity of multiple records	Unlikely	Major	High	Communications and Operations Management; Incident Management
16	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
17	Integrity	Application errors - e.g. Store dates in US format led to multiple records becoming corrupt	Unlikely	Moderate	Medium	Information Systems Acquisition, Development and Maintenance

No.	Factor	Risk	Likelihood	Impact	Risk	Security Domain
18	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
19	Availability	Denial of service attacks through external services (malicious or accidental)	Unlikely	Minor	Low	Communications and Operations Management; Incident Management
20	Availability	Infrastructure capacity issues - e.g., low server RAM/HDD etc	Unlikely	Minor	Low	Communications and Operations Management;
21	Availability	Unauthorised software/hardware changes cause outages beyond acceptable period	Unlikely	Minor	Low	Communications and Operations Management;
22	Availability	User accidentally causes environmental issues - turns of server; spills liquid etc	Unlikely	Minor	Low	HR Security; Physical Security
23	Availability	Vendor fails to meet SLA	Unlikely	Minor	Low	Information Security Organisation
24	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.

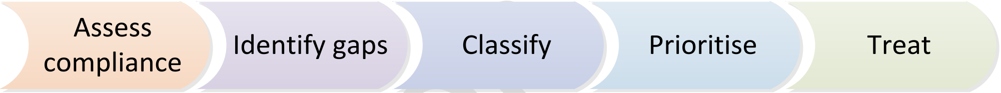
To assess security compliance, assessors should first identify the checklists that are applicable to the organisation being assessed.

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. Centrally Hosted Jurisdictional Checklist
3. Standalone CQR Checklist (local 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 or local data hosting checklist is used by standalone CQRs which operate and maintain their own data hosting infrastructure.

The Centrally Hosted Jurisdictional Checklist is used where ISO 27001 or Australian Signals Directorate (ASD)[6] certification does not exist. It will also be used when considering the centrally hosted national infrastructure.

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 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 Centrally Hosted Jurisdictional Checklist should be used. This checklist involves best practice controls for securing CQR information within jurisdictional infrastructure and requires an annual review.

Once a Standalone CQR becomes accredited, all future CQRs may outsource their data hosting requirements to the accredited 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

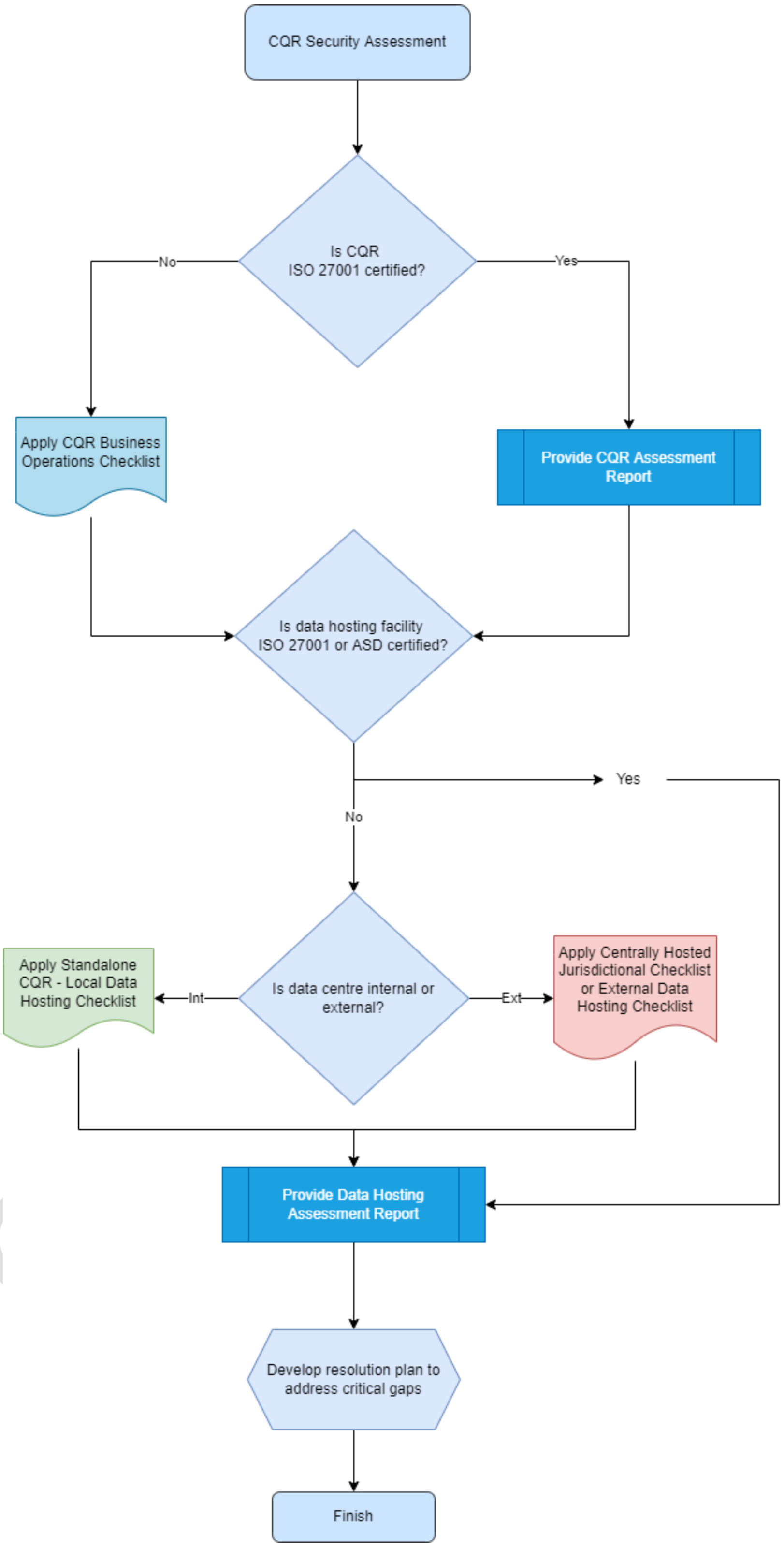
The flowchart (Figure 5) and matrix (Table 4) below should be used to determine the appropriate checklists to be used to assess an organisation’s security control measures based on the two organisational infrastructure models outlined in Section 3.1:

1. Centrally hosted jurisdictional infrastructure CQRs
2. Standalone CQRs

[6] ASD is now cyber.gov.au and the Australian Cyber Security Centre (ACSC)

Figure 5: Flowchart for determining the appropriate assessment checklists

The flowchart complements Table 4: 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
Apply Standalone CQR - Local Data Hosting Checklist
Int
Is data centre internal or external?
Ext
Apply Centrally Hosted Jurisdictional Checklist 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 4: Matrix for determining the appropriate assessment checklists

The matrix complements Figure 5: Flowchart for determining the appropriate assessment checklists .

	The certification checklist(s) that the organisation needs to complete is (are)…			
The organisation being assessed is a …	**CQR Business Operations Checklist**	**Existing CQR Local Data Hosting Checklist**	**Existing CQR using External Data Hosting or National Infrastructure** **Checklist**	**Other**
Existing CQR with an internal data hosting platform (all data and applications are hosted and maintained by CQR staff). (Refer to Figure 3).	✓	✓		
National infrastructure that hosts information for multiple CQRs. (Refer to Figure 2).	✓ (per CQR)		✓	
National Infrastructure CQR using an external data hosting provider (e.g. Cloud provider) that DOES NOT have ISO 27001 certification. (Refer to Figure 4).	✓		✓ CQR is responsible for ensuring the external provider complies.	
Existing CQR using an external data hosting provider (e.g. Cloud provider) that DOES have ISO 27001 certification. (Refer to Figure 4).	✓			✓ Proof of certification to be sighted by CQR
Standalone or national infrastructure that uses an external data hosting provider who does not have ISO 27001 certification.	✓ (per CQR)		✓ CQR is responsible for ensuring the external provider complies.	
Standalone or national infrastructure that uses an external data hosting provider that does have ISO 27001 certification.	✓			✓ Proof of certification
Central jurisdictional infrastructure that has previously attained certification using the Centrally Hosted Jurisdictional Infrastructure or Standalone Data Hosting Checklist, and another CQR wishes to join	✓ (per CQR)		Not required - already accredited once.	

The organisation being assessed is a …	The certification checklist(s) that the organisation needs to complete is (are)…			
	CQR Business Operations Checklist	Existing CQR Local Data Hosting Checklist	Existing CQR using External Data Hosting or National Infrastructure Checklist	Other
the existing central jurisdictional infrastructure services).				

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

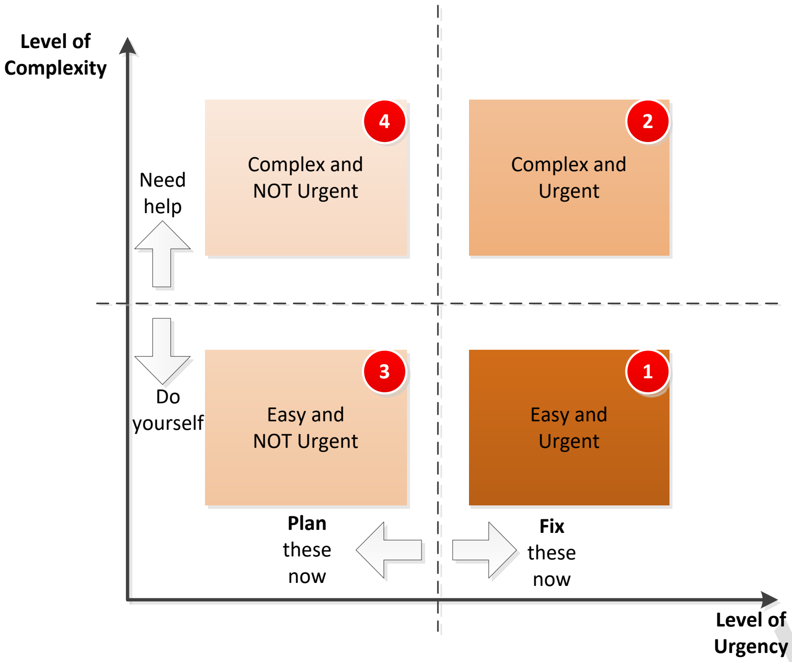
Once a security control gap has been identified, the next stage is to classify the importance of the gap in terms of urgency and complexity. Classification of security gaps provides a logical hierarchy of prioritisation for gap remediation work.

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 6 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 6: 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.

The checklist can be accessed in Excel[7]:

CQR Business
Operations Complia

5.2. Compliance Checklist: Standalone CQR – Local Data Hosting

To be completed by CQRs implementing and managing local infrastructure

The checklist can be accessed in Excel[8]:

Standalone CQR –
Local Data Hosting (

5.3. Compliance Checklist: National Infrastructure or External Data Hosting Providers

To be completed by data hosting providers prior to hosting CQR infrastructure or applications

The checklist can be accessed in Excel[9]:

[7] Source: Section 2.1 of NESAF v4 - Framework Model and Controls v1.0
[8] Source: Section 6.1 of NESAF v4 - Framework Model and Controls v1.0
[9] Source: Section 2.1 of NESAF v4 - Framework Model and Controls v1.0

CoE CQR – Local
Data Hosting Compl

6. Detailed Guidance on Controls

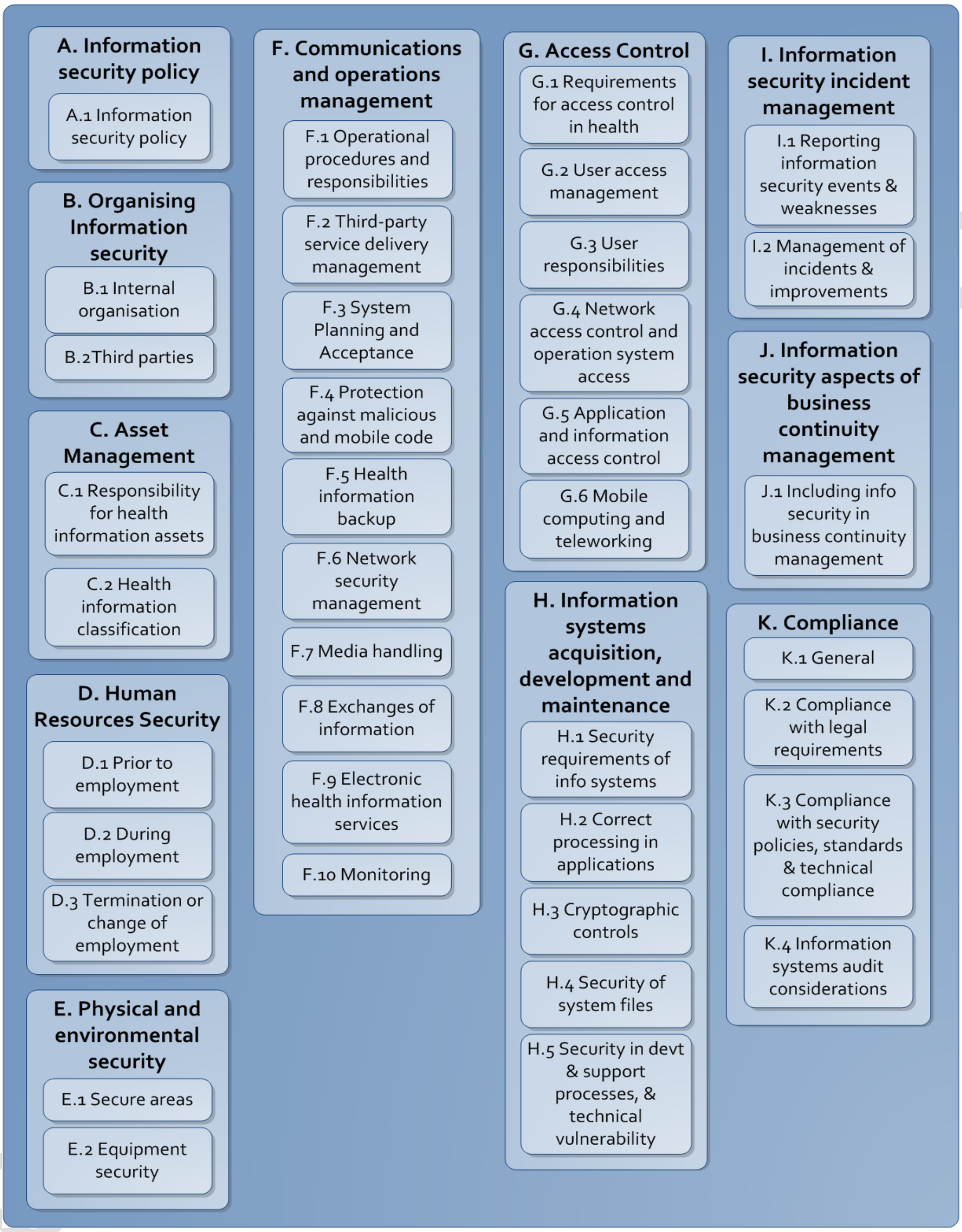
Each security control is explained in more detail in this section, categorised by security domains. The guidance provided is a blend of detail from relevant security guidelines and specific detail to suit CQR environments. The guidance provided borrows heavily from the National eHealth Security and Access Guideline and ISO/IEC 27002 [10].

The following diagram[11] represents the domains of information security.

[10] Refer to: Section 2 of NESAF v4 - Framework Model and Controls v1.0

[11] Source: National eHealth Security and Access Framework v4.0 and ISO/IEC 27002.

Figure 7: 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

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[12], and the RACGP Computer Security Standards.

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

6.2. Organising information security

6.2.1. Internal and/or external organisation

Objective: To manage information security within the CQR and its internal and/or 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 internal and/or external data hosting infrastructure providers may assign a role for managing information security to one of the positions within their organisation. Internal and/or 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[13].

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.

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 Royal Australian College General Practitioners Computer and Information Security Standards[14] 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

[12] NESAF v4 Business Blueprint, NEHTA 2011

[13] NESAF v4 Business Blueprint, NEHTA 2011

[14] https://www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Practice%20standards/Computer-and-information-security.pdf

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 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, researchers, data recipients – clinicians, clinical colleges, government agencies and funders, 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.

A number of organisations with data custodianship responsibilities have adopted the "Five Safes Framework". The Fives Safe Framework is an internationally recognised approach to considering strategic, privacy, security, ethical and operational risks as part of a holistic assessment of the risks associated with data sharing or release. The *Data Availability and Transparency Act 2022* references the Data Sharing Principles based on the Five Safes Framework[15].

The Five Safes Framework considers five dimensions:

- Project – is the use of data appropriate?
- People – can the users be trusted to use it in an appropriate manner?
- Data – is there a disclosure risk in the data itself?
- Settings – does the access facility prevent unauthorised use?
- Output – are the statistical results non-disclosive.

The Five Safes Framework should be used in conjunction with the detailed guidance provided in Attachment 2 *Security Compliance Guideline.*

[15] The Five Safes framework - Australian Institute of Health and Welfare (aihw.gov.au)

Table 5 List of national and state/territory data governance guidance

Document	Author	Reference
National guidance		
Australian Government Public Data Policy Statement - data held by the Australian Government is a strategic national resource that holds considerable value for growing the economy, improving service delivery and transforming policy outcomes for the Nation.	Australian Government	Australian Government. Australian government public data policy statement [Internet]. Canberra: Australian Government; [2015 Dec 12; cited 2022 May 30]. Available from: https://www.pmc.gov.au/sites/default/files/publications/aust_govt_public_data_policy_statement_1.pdf
***The Data Availability and Transparency Act 2022 (DATA)* Scheme** - commended on 1 April 2022	Australian Government Prime Minister and Cabinet	Australian Government. *Data Availability and Transparency Act 2022* [Internet]. Canberra: Australian Government; [2022 Apr 11; cited 2022 May 30]. Available from: https://www.legislation.gov.au/Details/C2022A00011
The Foundational Four - To get the most out of the data they hold, government agencies need to look after and manage their data assets in the same way they look after their people,	Australian Government Office of the National Data Commissioner	Australian Government. The foundational four [Internet]. Canberra: Office of the National Data Commissioner; [2022; cited 2022 May 30]. Available from: https://www.datacommissioner.gov.au/sites/default/files/2020-06/foundational-four.pdf

Document	Author	Reference
physical property and IT systems. - The Foundational Four provides guidance for agencies on how they can start improving their data practices and address the technical and cultural challenges that can limit their ability to get the most out of their data.		
Data Governance Framework 2021 (Public edition) - This Framework lists the elements that comprise the AIHW approach to data governance, and describes in detail how they work together to support the legal, ethical and safe management of our data holdings. - It recognises that a combination of supporting legislation, roles, policies, practices, standards, tools and technologies is required to deliver effective data governance arrangements at AIHW.	Australian Institute of Health and Welfare	Australian Institute of Health and Welfare. Data governance framework 2021 [Internet]. Canberra: Australian Institute of Health and Welfare; [2021 Apr 6; cited 2022 May 30]. Available from: https://www.aihw.gov.au/getmedia/c3e00f60-c40d-4989-ad22-de1be3ab5380/Data-Governance-Framework-2021.pdf.aspx
The Five Safes framework - an internationally recognised approach to considering	Australian Institute of Health and Welfare	Australian Institute of Health and Welfare. The five safes framework [Internet]. Canberra: Australian Institute of Health and Welfare; [updated 2021 Sep 1; cited 2022 May 30].

Document	Author	Reference
strategic, privacy, security, ethical and operational risks as part of a holistic assessment of the risks associated with data sharing or release.		Available from: https://www.aihw.gov.au/about-our-data/data-governance/the-five-safes-framework
Data.gov.au - is the central source of Australian open government data. Anyone can access the anonymised public data published by federal, state and local government agencies	Australian Government; supported by the Australian Bureau of Statistics	Australian Government. Data.gov.au [Internet]. Canberra: Australian Bureau of Statistics; [cited 2022 May 30]. Available from: https://data.gov.au/page/about
Establishing an information governance framework - includes a link to a Data Interoperability Maturity Model https://www.naa.gov.au/sites/default/files/2019-12/IM-Infographic-interoperatability-maturity-model-V2.pdf	National Archives of Australia	National Archives of Australia. Establishing an information governance framework [Internet]. Canberra: National Archives of Australia; [cited 2022 May 30]. Available from: https://www.naa.gov.au/information-management/information-governance/establishing-information-governance-framework
State and territory guidance (add other jurisdictional frameworks)		
NSW Health Data Governance Framework	NSW Ministry of Health	NSW Health. Health Data Governance Framework 2019. [Internet]. Sydney: NSW Health; [cited 2022 May 30].

Document	Author	Reference
- applies to state wide data assets that support the delivery of high quality safe patient care, enable timely response to population health issues, and promote the prevention and control of disease.		Available from: https://www1.health.nsw.gov.au/pds/ActivePDSDocuments/GL2019_002.pdf

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.[16]

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 are 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.

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

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.

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

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

CQRs 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 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 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 centrally hosted jurisdictional CQR 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 assess 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 publicly. 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 tamFiper 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 monitor 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 timeclock, 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 user's 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 are 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[17])
- 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.

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

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

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 accredited 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 timescales; 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[18]

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. AS ISO 27799-2011
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; 27799-2011]
Centrally hosted	Centrally hosted jurisdictional (Commonwealth, state and territory infrastructure model) national infrastructure
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, 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.
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 standalone CQRs through a third-party service provider arrangement.

[18] Reference: Glossary in NESAF v4 - Framework Model and Controls v1.0

Term	Definition
Encryption	Data are 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-process-able form, stored and transmitted securely, and accessible by multiple authorised users. AS ISO 27799-2011
Healthcare	Any type of service provided by professionals or paraprofessionals with an impact on health status. AS ISO 27799-2011
Healthcare organisation	Generic term used to describe many types of organisations that provide healthcare services. AS ISO 27799-2011
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. AS ISO 27799-2011
NEHTA	National eHealth Transition Authority.
NESAF	National E-Health Security and Access Guideline.
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. AS ISO 27799-2011
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.

Term	Definition
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 **Error! Reference source not found.** in **Error! Reference source not found.** 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. [HB174-2003]
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. [HB 174-2003]
Vulnerability	A weakness that can be exploited that may cause damage to a system or information assets. [HB 174-2003]

8. References

Tag	Name	Version
[RACGP1]	RACGP Computer and Information Security Standard https://www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Practice%20standards/Computer-and-information-security.pdf	2nd Edition
[HB174-2003]	Information Security Handbook for Healthcare https://www.saiglobal.com/PDFTemp/Previews/OSH/as/misc/handbook/HB174.pdf	174-2003
[NESAF; 27799-2011]	Information security management in health using ISO/IEC 27002	2011

AUSTRALIAN COMMISSION
ON SAFETY AND QUALITY IN HEALTH CARE

Level 5, 255 Elizabeth Street, Sydney NSW 2000
GPO Box 5480, Sydney NSW 2001
PHONE: (02) 9126 3600

@ACSQHC

safetyandquality.gov.au