nehta

NESAF Release 3.1

Business Blueprint (S1131)

Version 3.1

Approved for release

National E-Health Transition Authority

National E-Health Transition Authority Ltd
Level 25
56 Pitt Street
Sydney, NSW, 2000
Australia.
www.nehta.gov.au

Document control

Name of document:	NESAF R3.1 – Business Blueprint
Document owner:	National E-Health Security and Access Framework
Document coordinator:	NESAF Configuration Librarian
Author(s):	NESAF Development Team
Document approver:	Project Executive

Document authoring and review

Version	Date	Author	Status and nature of amendments
2.0	20110729	NESAF Team	Version 2.0 Approved for release
3.0	20111130	NESAF Team	Version 3.0 Approved for release
3.1	20120330	NESAF Team	Version 3.1 Approved for release

Document publication

Publication:	✓ Internal ✓ External ✓ Public
Published version and date:	The March 2012 publication of the NESAF has been released for adoption and implementation trials. The NESAF will continue to be developed through application learning's, community feedback and changes to eHealth technologies, International and Australian Standards, as well as changes to the Australian Health working practices.

This page is intentionally left blank

Table of contents

Table of Figures

This page is intentionally left blank

1 Introduction

1.1 Purpose

The purpose of this document is to provide a further release of the Business Blueprint within the National E-Health Security and Access Framework (NESAF) suite of documents.

1.2 Intended audience

This document is written in a style that should be affable to a range of individuals actively working in eHealth, including health executives, managers, healthcare professionals, consumer representatives, policy officers, security practitioners and privacy experts. The document audience will also include interested government agencies and information security practitioners outside the health sector.

1.3 Scope

The scope of business for the NESAF is all public and private sector healthcare provider organisations that have information or connectivity traceability to national systems.

1.4 Overview

This document describes the purpose, structure and benefits of the Framework as well as providing detailed implementation advice for healthcare business owners, managers or practice team leads responsible for information security within healthcare organisations. The document will be further developed and refined as feedback is received through consultation.

1.5 Questions and feedback

The NESAF Programme values your feedback about the usefulness of this document. We also encourage your comments or suggestions about the content of the document to inform its further development. Please direct your questions or feedback to feedback.saf@nehta.gov.au.

2 Business Blueprint

2.1 Introduction

In Australia we have enjoyed the benefits of a world class healthcare service that has ensured that all Australians have access to quality healthcare when it is needed. To meet increasing demand for healthcare and to maintain our status in healthcare delivery, Australian Governments are looking to the potential of advances in electronic health (eHealth) to maximise the use of critical health information and drive efficiencies across the sector. eHealth offers a range of improvements for shared care and care planning including medication management, handover of care through electronic discharge summaries and referrals, complete access to test results through electronic pathology reporting and access to comprehensive medical records for every patient through a national system of electronic health records. Today, our eHealth systems already facilitate the sharing and transferring of sensitive health data and are subject to existing controls and governance relating to the management of health information.

Increasing investment in eHealth in Australia will result in larger quantities of information being transferred, and increasing volumes of information being exchanged in novel ways to support emerging clinical models. Improved management of healthcare information through eHealth offers significant safety and quality benefits for all Australians. Governments across Australia have committed to a national approach to eHealth that will enable a safer, higher quality, more equitable and sustainable health system for Australians. The application of the National E-Health Security and Access Framework (NESAF) within healthcare organisations will assist in ensuring that this commitment is met.

There are not enough security professionals nor is there always financial capacity to access to specialist security resources to provide the necessary advice and or strategies for organisations for approaching security within health. This business blueprint aims is to assist in providing a greater understanding of security responsibilities and a path for organisations at a holistic level rather than the current practice which is organisation inward centric.

Importance of assuring privacy within eHealth

Australian society recognises that a person's healthcare records contain some of their most sensitive and private information. Increasing use of eHealth will result in the ability of healthcare providers to collaborate and share personal health information. The ability to support this move of healthcare information throughout the national eHealth system, while respecting patient privacy and rigorously protecting the confidentiality of the information, presents some of the biggest challenges to the development, adoption and acceptance eHealth in Australia.

Increasing exposure of personal healthcare information to a larger number of individuals, organisations and the internet means that proactive information security approaches are essential in the national eHealth environment. High-quality information underpins the delivery of high-quality, evidence based healthcare. Healthcare information has greatest value when it is accurate, up to date and is accessible where and when it is needed. Without effective security, information assets may become unreliable and untrustworthy, may not be accessible where or when needed, or may be compromised by unauthorised third parties. All organisations, and those who supply or make use of eHealth information, therefore have an obligation to ensure that there is adequate provision for the security management of the information resources that they own, control or use.

Importance of security to businesses/organisations involved in eHealth

Successful eHealth initiatives around the world rely on patients and healthcare professionals having trust in their information systems and solutions. Trust stems from people having confidence in the system's content, in their ability to appropriately collect access, use and disclose data held by these systems and solutions, and the knowledge that the data is held privately, in line with patient wishes and clinical needs. Breaches and failures of security and access control will diminish trust within the national eHealth system, seriously compromising adoption and uptake of these systems and the expected benefits derived from investments in them. Being able to manage local security and access measures will be an important pre-requisite for a business to be able work effectively in the national eHealth environment.

2.2 Purpose of the NESAF

This document describes the goals and principles of NESAF. Many healthcare organisations do not have access to specialist security resources to provide them with advice and assist with strategies for approach security within eHealth environments. This is often due to lack of availability of security professionals or insufficient financial resources within organisations to secure their services. This blueprint aims to provide organisations with a greater understanding of their security responsibilities, and provides guidance to businesses engaged in health about how to establish an information security infrastructure using a risk-based approach within their organisation.

The content of the Blueprint is standards-based. As such it provides a consistent interpretation of relevant standards in relation to their application in the Australian eHealth environment.

Goals of the NESAF include ensuring that:

- Access to consumer health information is consistently controlled and monitored as it transitions through independent organisations, business processes and systems in the Australian health sector.
- The provenance of all electronic health information can be traceable from its creation at a verifiable trusted source through its transition and possible augmentation on route to its destination.

Security is not a single solution. It is a pervasive, cyclical process in which risks are assessed and controls implemented and reviewed based on changes in the business and eHealth environment. Building an effective security infrastructure within an organisation requires analysis and planning, along with the development of policies, procedures and technology.

2.3 Target audience for the Business Blueprint

The NESAF recognises that the complexities of security in eHealth cannot be solved by information technology professionals alone. It requires a co-ordinated approach of people working within the management/business, clinical and information technology domains within an organisation. Accordingly, the NESAF document suite contains documents specifically for business, clinical, technical and consumer audiences and NESAF information is presented accordingly (refer also to Section 2.5).

The target audience for this Blueprint is business owners, managers and team leaders responsible for information security within healthcare organisations e.g. primary care practice owners/managers, private hospital owners/managers, public hospitals managers, practice/clinical team leads and owners/managers of other healthcare organisations.

2.4 Benefits

Key benefits of security and access control within an organisation include the ability to:

- Ensure the confidentiality, integrity, and availability of personal health information held in electronic form.
- Specify the requirements for establishing and implementing security and access control over eHealth systems within the context of the business's or organisation's overall business risks.
- Protect the organisation's information and the healthcare information of its patients.
- Enable the organisation to meet current legal requirements, relevant standards and professional better practice in relation to the use of eHealth systems.
- Assist organisations to meet their privacy obligations.
- Support patient safety through the protection of the integrity of health information.
- Engender trust within the national eHealth system, thus increasing adoption and uptake of these systems and maximising the expected benefits from these investments.

Value proposition of the NESAF

Healthcare organisations today continue to face many, and often increasing challenges when managing health risks across the enterprise and between organisations. Healthcare organisations are increasingly reliant on electronic information systems, which are becoming more complex, integrated and interoperable. Connected healthcare systems provide a rich breeding ground for risks to individual privacy, confidential information, data integrity, and service availability. In order to manage health information risks across the enterprise, and between organisations, organisations look at ways to help address those challenges when making information security and security arrangements.

The NESAF consists of a comprehensive set of information security and access-specific principles, controls and guidance reflecting the findings from a wide range of Australian Health projects, such as the PCEHR (Personally Controlled Electronic Health Record), the NASH (National Authentication Service for Health), SMD (Secure Messaging Delivery), HI (Health Identifiers) Service, and CCA (Conformance, Criteria and Accreditation). In addition it draws on main security controls and better practice guidance contained in other security related standards including; HL7PASS, OASIS, ISO/IEC 27002 (27799), COBIT and industry guidelines.

2.5 NESAF document framework

This *Business Blueprint* is a document within the suite of NESAF documents. Figure 1 provides a view of the elements of the core framework, and specific artefacts, or documents within the NESAF suite targeted to specific audiences.

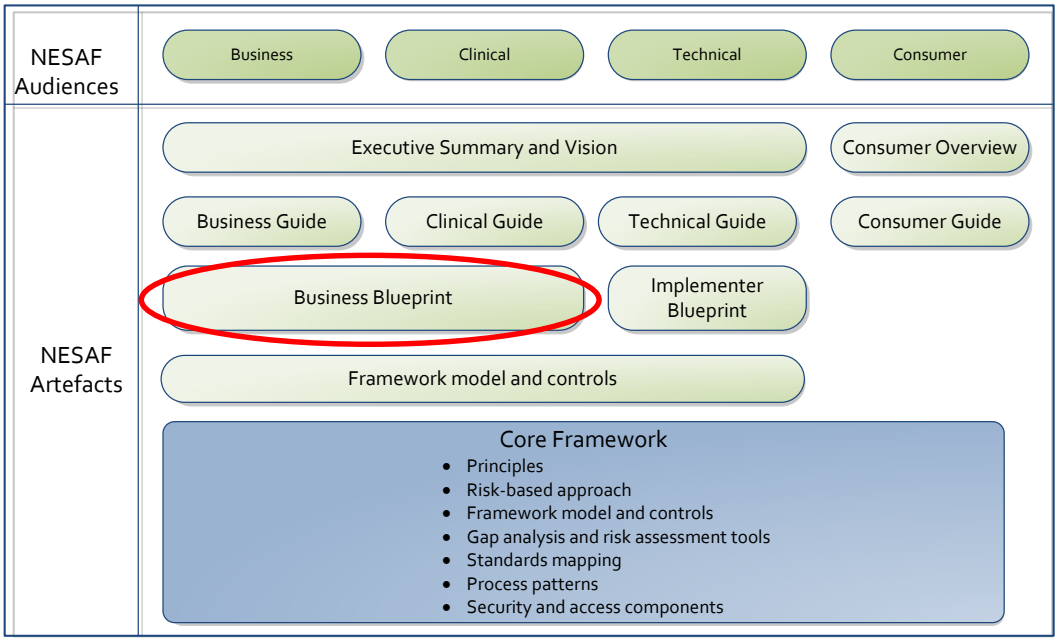


Figure 1: Suite of NESAF 3 documents

3 Structure of the NESAF

Figure 2 illustrates the structure of the core framework and identifies the focus of each of the key documents in the NESAF document suite.

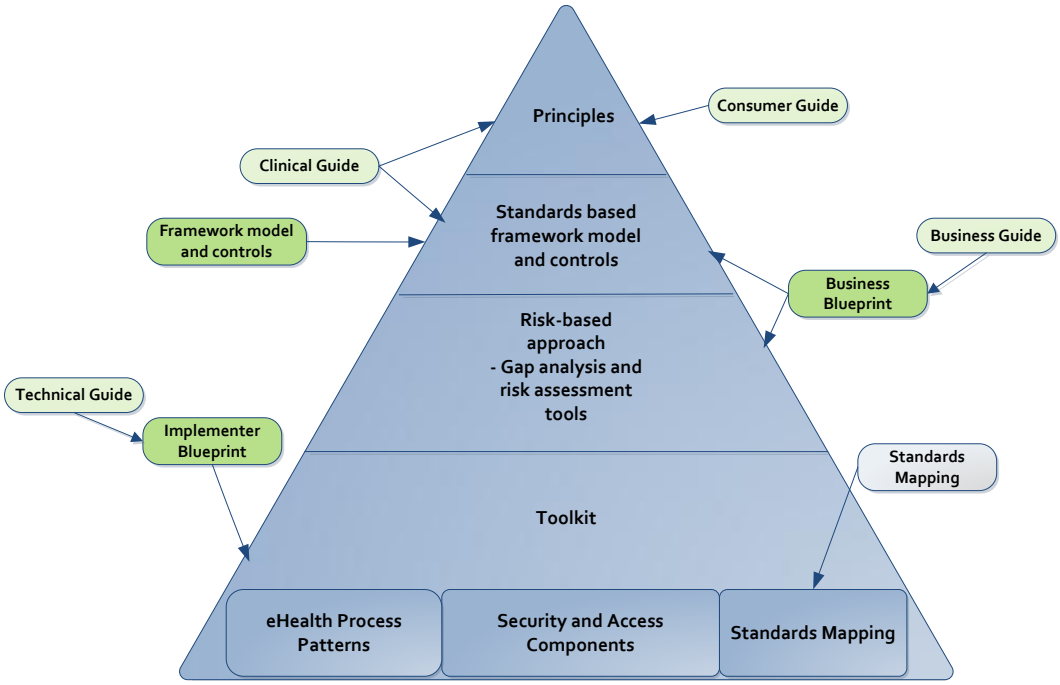


Figure 2: Structure of the NESAF core framework

The core framework includes:

- A set of **principles** that are intended to guide the design and implementation of secure eHealth systems.
- The framework **model** that identifies key security and access control areas, control objectives and **controls**.
- A **risk-based approach** to support implementation of the framework, including:
  - **Gap analysis and risk assessment tools** that organisations can use to assess their level of risk and compliance with each of the security and access control areas within the framework model.
- A **toolkit** that provides a comprehensive library of information relevant to specific eHealth processes (e.g. authenticate authorised user) and security and access functions (e.g. authentication). Key components of the toolkit include:
  - **eHealth process patterns** that assist businesses to identify core security and access functions in the context of their business.
  - **Security and access components** that include relevant standards, controls, better practice examples, compliance, services, policy and issues associated with each security and access function.
  - **Standards mapping** which identifies a suite of standards and relevant documents that relate to security and access in eHealth in Australia.

3.1 Goals and Principles of the NESAF

The goals and principles of the NESAF are intended to guide the application of the framework in the design and implementation of secure eHealth systems to manage and protect healthcare information.

Figure 3: Goals and Principles of the NESAF

Confidentiality, availability and integrity of healthcare information are the goals of information security. Specifically:

Confidentiality refers to ensuring that information is only accessible and available to those authorised to have access.

Availability ensures that information is accessible to authorised individuals when and where it is required and contributes to patient safety where treatment is often time-critical.

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.

The goals of information security are manifested in the following expectations:

Patient expectations: Patients have the right to expect that their privacy is respected and their information is treated confidentially over the lifecycle of their health records. This includes the general right to obtain access to their health information and to understand when and by whom their health information has been collected, accessed, used and disclosed by others.

Provider expectations: Healthcare providers expect to have timely access to healthcare information and be able to rely upon the integrity of the information as the basis of providing high quality health care.

The following NESAF principles provide qualification to the information security goals and expectations of patients and providers:

Patient control: Patients can be aware of what is happening with their healthcare information and what options they have for exercising a degree of control over who can access their healthcare information, and how their healthcare information is used are available to them. They have the right to professional advice concerning the consequences and impacts of choices relating to control of their health information and are able to express their preferences (which may change over time).

Authorised access: Any individual collecting, accessing, using or disclosing personal health information must have an authenticated right and authorised reason for those activities. Persons accessing healthcare information must respect the confidential nature of that information.

Accountability: All access to personal health information must be accounted for through audit and audit review procedures.

Usability and safety: Security as an integral part of healthcare information systems should support the purpose of the organisation by ensuring users find the secure way is the easy way. The effectiveness of health information systems in terms of clinical safety is paramount.

Governance and continuous improvement: Organisations must provide commitment and support to healthcare information security and access within and outside the boundaries of the organisation and ensure that statutory, regulatory and contractual security requirements are met. Governance mechanisms should be used to regularly measure, reassess and improve information security and access control.

3.2 Standards-based framework model

The framework model identifies eleven key security and access control areas (e.g. G. Access Control) relating to eHealth, each of which contains one or more control categories (e.g. G.1 Requirements for access control in health, G.2 User access management). Each control category contains a control objective stating what is to be achieved, and one or more controls that can be applied to achieve the control objective. The model is based on Australian Standards for information security management, and information security management in health (AS ISO 27002 and AS ISO 27799), and has been tailored to address the specific health information security and access requirements in the Australian eHealth environment.

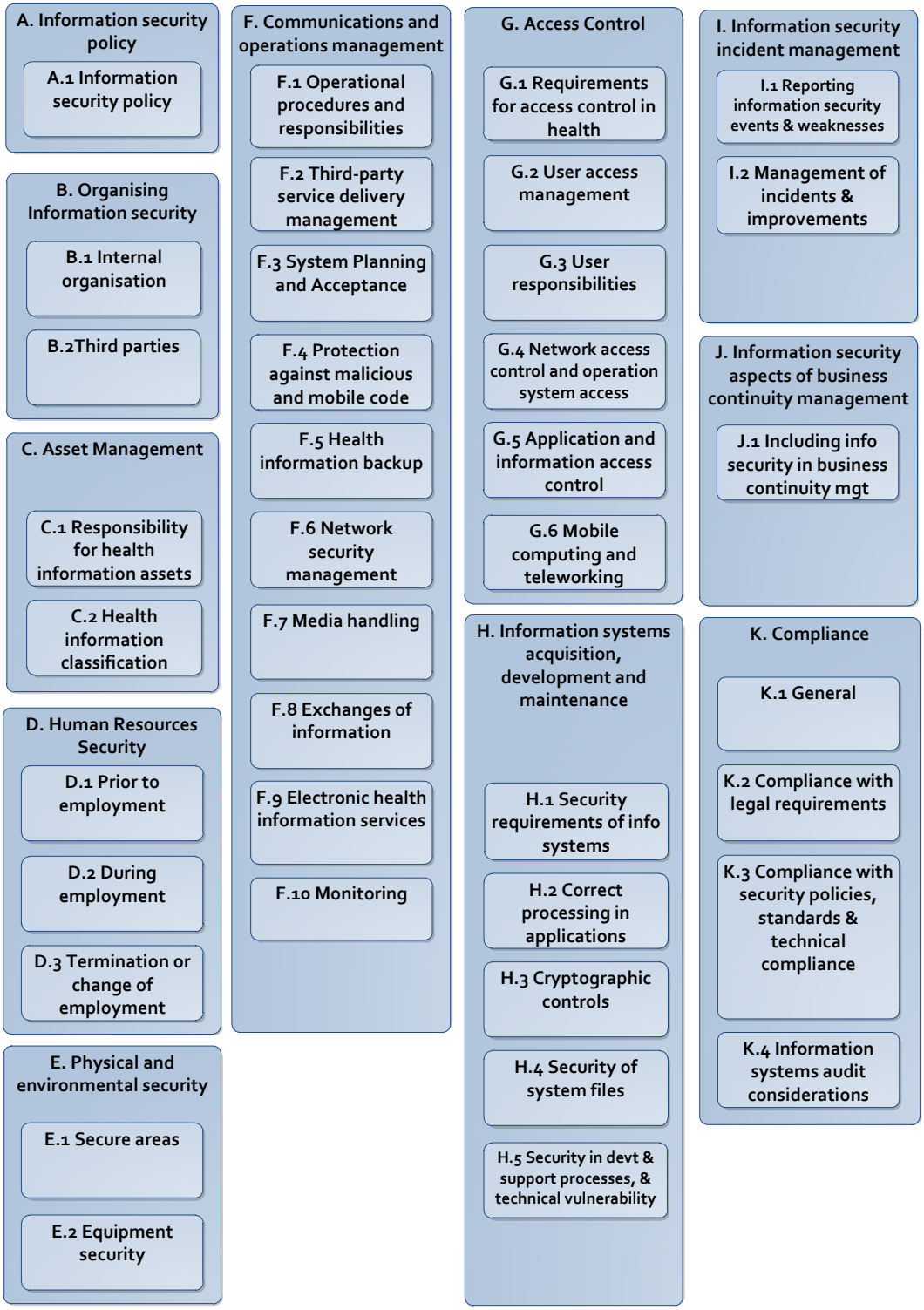


Figure 4: Standards-based framework model

A list of the control objectives and controls within the model is included in Appendix A: and further information in relation to each control is contained in the *Framework Model and Controls* document [NEHTA2011b].

Within each control area, a range of controls is identified that businesses may select, based on the outcome of risk assessment processes, to address the security and access requirements for their organisation.

Security of eHealth information requires the use of a layered approach to information security that incorporates control within the business, healthcare services, IT services and specific eHealth services which include technical and non-technical controls. The NESAF framework model includes a range of controls that are applicable to each of the domains identified in Figure 5. The framework focuses in greater depth on the controls used to secure eHealth services, with better practice guidance provided in relation to those in the *Implementer Blueprint*. [NEHTA2011a]

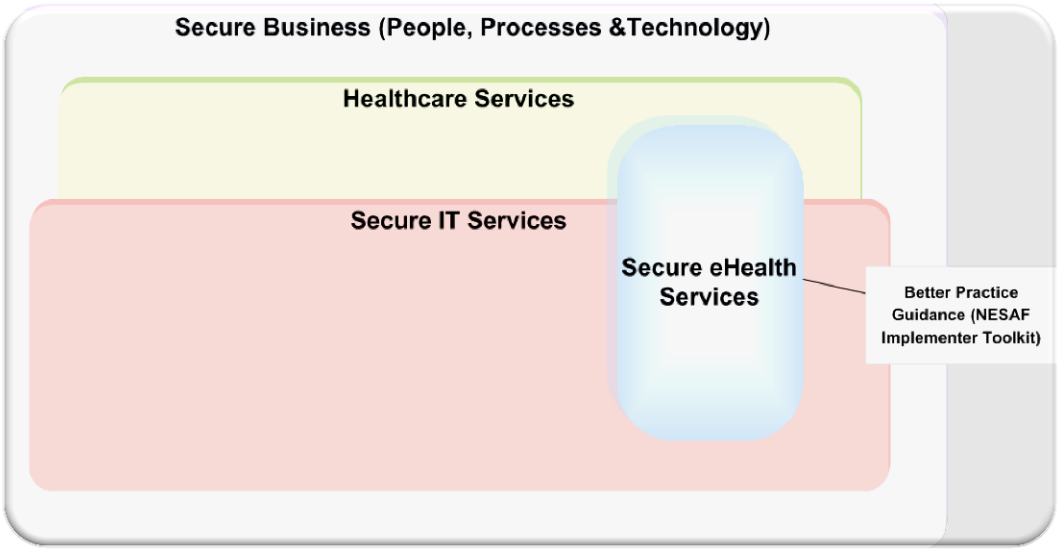


Figure 5: Coverage of NESAF controls

4 Risk-based approach

The NESAF sets out a risk-based approach and process to assist businesses and organisations to analyse their risk in relation to participation in the Australian eHealth environment, and to identify appropriate security and access controls. The process assists businesses to identify appropriate methods – that may include policies, practices, procedures or software and other technical solutions – for protecting their health information, and the information that they may access and share with other healthcare organisations in the national eHealth environment.

The application of the framework can be scaled to different organisational sizes and types and the nature of their interaction with national eHealth systems. The amount of effort and investment in information security depends on the size of the organisation and the perceived value of its information assets. In the context of national eHealth, however, the value of the information assets and threats and risk associated with those assets needs to be assessed in the context of participation within the national eHealth system. The manner in which a business/organisation interacts with eHealth systems will influence the options and potential actions a business/organisation may take to align with the NESAF's principles and controls.

The national eHealth environment comprises a range of organisations and services that will have differing levels of interaction with eHealth systems, and different types of data, complexity, usage and access:

- **National Infrastructure –** organisations that deliver core elements of national eHealth system infrastructure, for example the core services required to support the Personally Controlled Electronic Health Record (PCEHR) such as the Participation and Authorisation Service, Index Service, and Template Service and NEHTA Foundation Services such as the National Healthcare Identifiers (HI) Service, the National Authentication Service for Health (NASH), and the Clinical Terminologies Information Service.
- **Hosts –** businesses/organisations that operate and maintain repositories of clinical documents such as Medicare-operated repositories holding Medicare history, PBS history, organ donor information, childhood immunisation information, diagnostic service repositories holding Pathology Result Reports and Diagnostic Imaging reports, and regional or State/Territory operated repositories.
- **Connected users –** businesses that contribute and receive information to and from healthcare records/repositories/systems external to their organisation – e.g. hospitals, general practices, community health, and medical specialists.

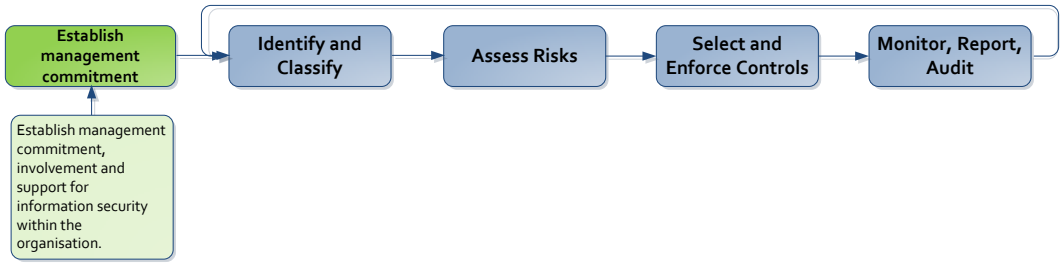
4.1 Implementation process steps

Figure 6 outlines key steps that a business should undertake in order to implement suitable information security and access control within their organisation.

Figure 6: NESAF process flow

Each of the steps is explained in further detail in the following sub-sections.

4.1.1 Establish management commitment



Health information security should involve all aspects of a healthcare organisation. Information security is the responsibility of every staff member within an organisation and cannot be delivered purely through technical solutions. Consequently, management support and the buy-in of staff to the information security measures adopted by an organisation are critical to their success and ensure that everyone in the organisation is working together towards a common goal. Coordination of information security can only be maintained over the long term if the organisation has an explicit commitment to information security.

Why is this important?

A health organisation's management is responsible for the security of personal health information, even if the organisation relies upon managed services provided by third party organisations. Security is one of the key enablers for ensuring that a health organisation's privacy obligations are being met.

The process of assessing information security risk, and selecting and enforcing controls may require financial investment in the short-term. In a healthcare organisation, tension commonly exists in relation to trade-offs between expenditure on healthcare service provision and other business-related expenditure. The willingness of management to dedicate resources and adopt changes in policy and procedures that support information security as an integral part of the operation of the business signals the importance of information security within the organisation.

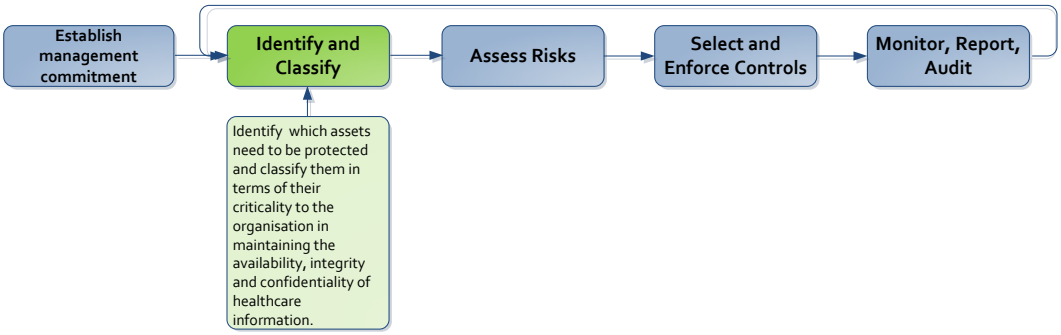
Key activities for establishing management commitment to information security and access:

- Have a written information security policy or (for smaller organisations) a Statement of Management Intent that is approved by management, published, and then communicated to all employees and relevant external parties.
- Ensure that the organisation's information security policy is subject to ongoing, staged review at least annually and following the occurrence of a serious security incident.
- Require that people who have access to healthcare information sign a confidentiality and non-disclosure agreement and understand the penalties associate with a breach of confidentiality.
- Clearly define and assign responsibilities for security and access control.
- Have an information security management forum in place that meets regularly to ensure there is clear direction and visible management support for security initiatives involving the security of health information.
- Ensure that at least one individual is responsible for health information security within the organisation.
- Ensure that appropriate contractual arrangements reflecting the organisation's security requirements are put in place in relation to any third parties who access, process, communicate or manage the organisation's information.

Useful references:

- *Australian Standard AS ISO 27799 – 2011 Information security management in health using ISO-IEC 27002*. [AS27799]
- *HB174-2003 Handbook. Information security management – Implementation guide for the health sector*. [HB174]
- *ISO 31000:2009 Risk Management – Principles and guidelines. [ISO31000]*
- *The Royal Australian College of General Practitioners. Computer security guidelines: A self-assessment guide and checklist for general practice*. [RACGP1]
- Appendix A: contains information on NESAF control areas and controls relating to A. Information Security Policy and B. Organising Information Security.
- Appendix B: contains guidance for the development of an organisation's information security policy.
- Appendix C: contains guidance on key issues and responsibilities in relation to information security and access that could be included in role descriptions within a healthcare organisation.

4.1.2 Identify and classify



At the heart of information security is a set of assets to be protected. Assets can include data (e.g. patient healthcare information, personnel information), software (e.g. medical software, operating systems), hardware (e.g. laptops, mobile devices, network equipment) supporting services (e.g. telecommunications services, cloud computing) and human assets (e.g. patients, providers). A key stage in information security planning is the identification and classification of information assets to be protected. This stage addresses the fundamental questions of:

- What are the health information related assets we need to protect?
- How important are these assets?

Prior to conducting a risk assessment, an organisation needs to define the scope of assets that need to be protected and classified in terms of their value, legal requirements, sensitivity and criticality to the organisation. The scope of these assets will form the basis of the risk assessment and lead to the selection and implementation of appropriate security and access controls.

4.1.2.1 Approaches to asset identification

In theory, the scope of the risk assessment can apply to whole organisations, however experience shows that large organisations find this difficult to implement in practice. An alternative approach is to use an incremental and iterative process covering particular sites or business processes progressively over time to achieve total coverage of the organisation. [AS27799]

Common healthcare information assets are identified in Figure 7.

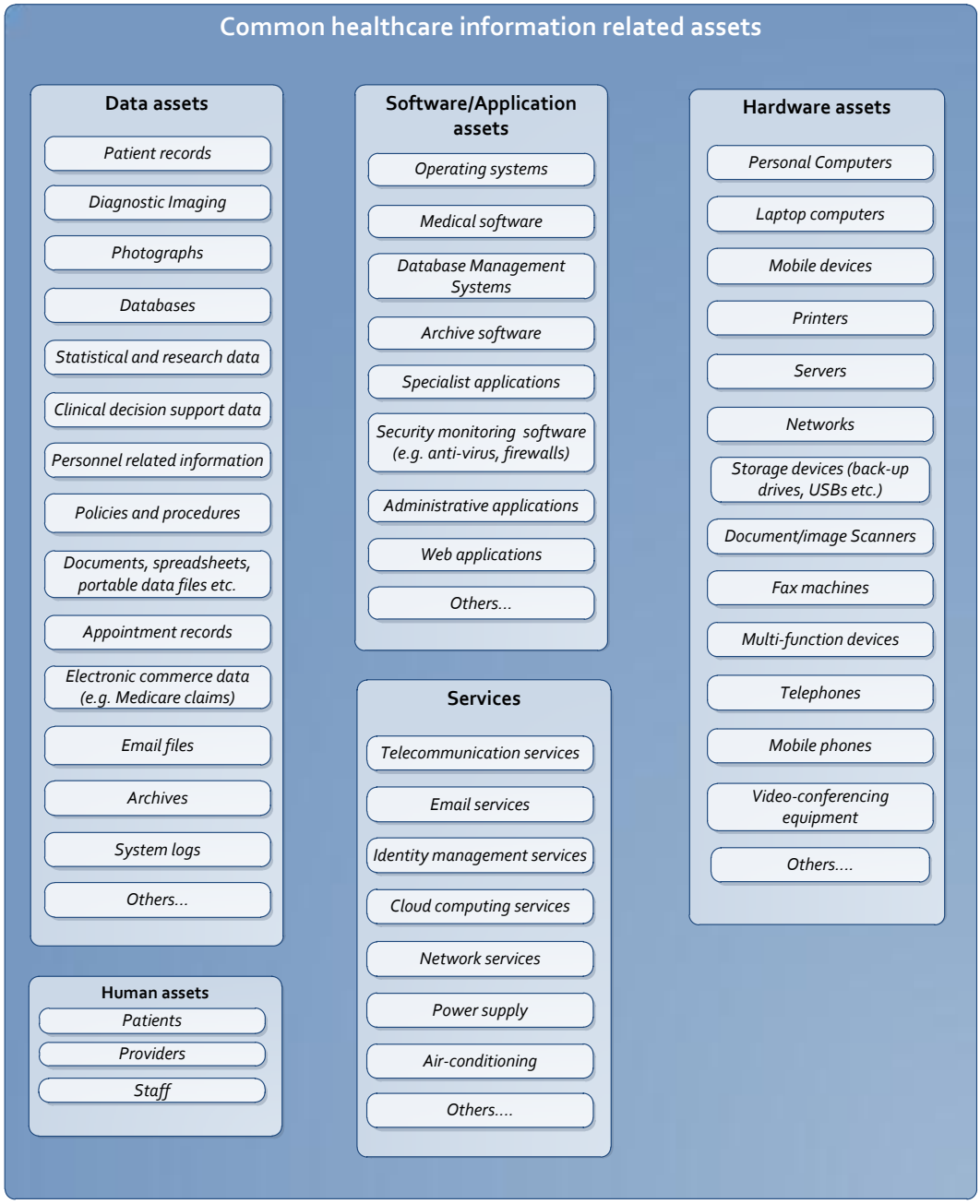


Figure 7: Common healthcare information related assets

These are intended as a useful prompt for the identification of assets, rather than as an exhaustive list. Each organisation will have a unique set of assets.

Organisations may choose to apply the NESAF to all, or to a subset of its information assets; or to apply the framework incrementally to particular eHealth projects such as use of the National Healthcare Identifier Service or participation in the PCEHR.

Using the latter approach, organisations may choose to base their risk assessment on key processes relevant to a specific project or implementation of the NESAF and use these as the basis of identifying a related set of assets. To assist businesses in identifying the scope of assets to be addressed within a risk assessment, the NESAF contains a library of common eHealth process patterns. Organisations can use these as reference business processes, or determine their own set of business processes upon which their asset identification and classification will be based. Figure 8 below shows the set of eHealth process patterns contained in NESAF.

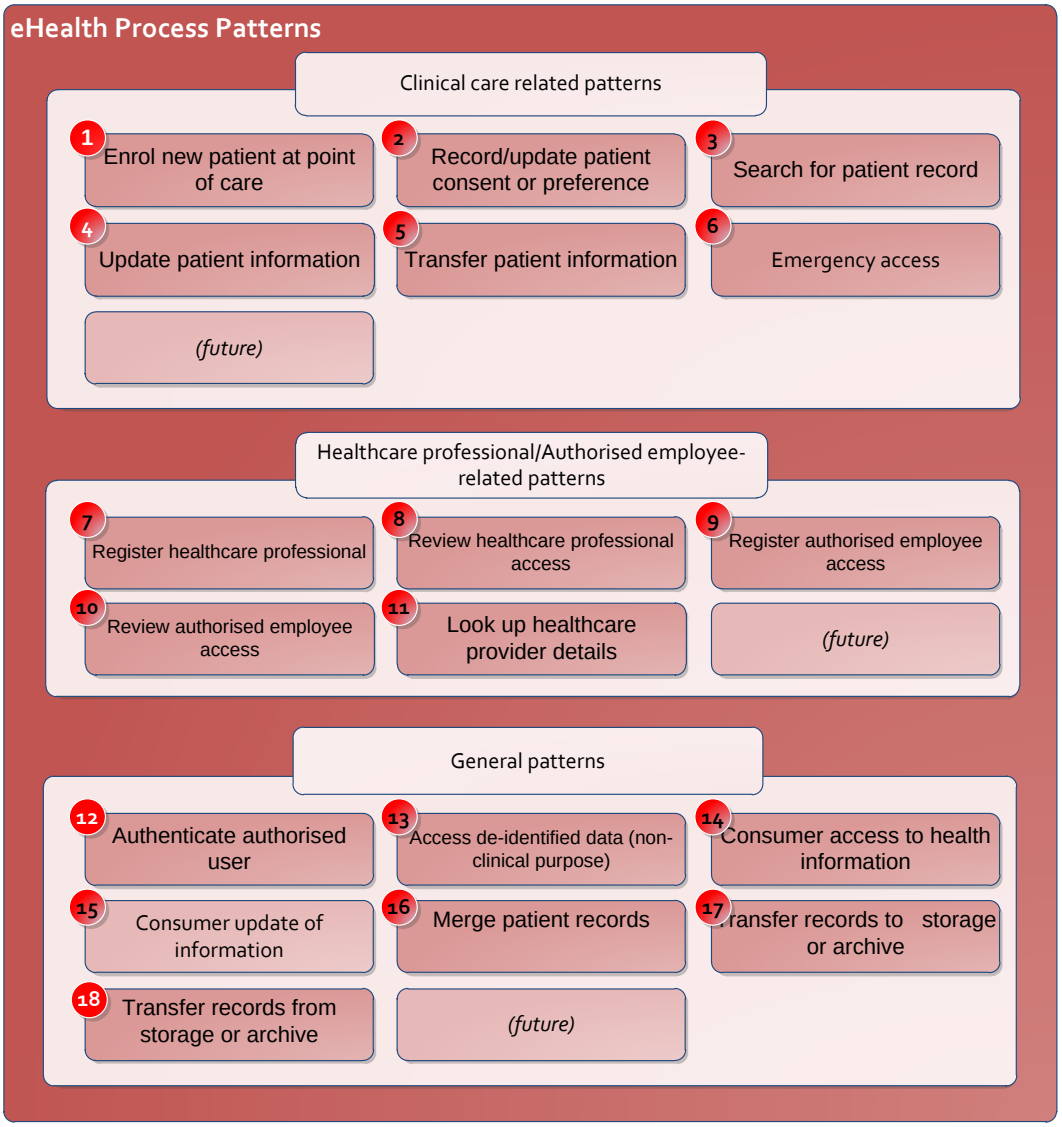


Figure 8: NESAF eHealth process patterns

Once the relevant processes and services have been identified, the information assets associated with those elements can be identified and classified. Figure 9 provides an example of this approach.

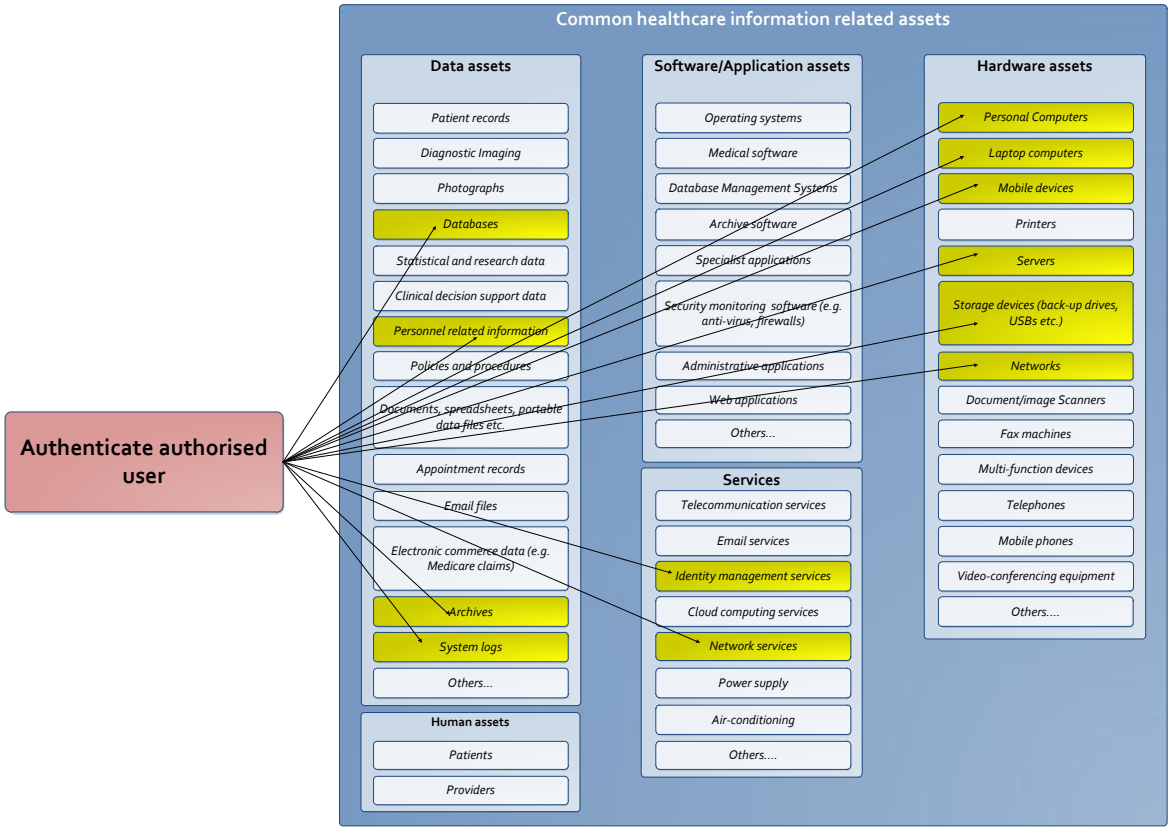


Figure 9: Example of using eHealth process patterns to identify related information assets

As organisations increase their eHealth activity, further projects within the organisation can be assessed and appropriate NESAF controls adopted, until ultimately all eHealth activity within the organisation is covered.

4.1.2.2 Asset description

In relation to identified assets, it is useful for the organisation to describe or characterise, the use of the assets within the organisation to inform the risk assessment process. Characterisation involves a description of the operational environment in which the assets are used that can include (but is not limited to):

- Relevant policies, laws, industry practices.
- Processes performed (including inter organisation exchanges).
- Users of the assets.
- Persons/organisations that support the assets (e.g. third party service providers).
- Information flows and interfaces.
- Security architecture:
  - Technical, people and process controls in use.
  - Network design.
  - Physical and environmental security (e.g. facility security, controls for temperature, power etc.).

A range of techniques can be used to compile the information above, including document reviews, interviews and questionnaires.

Why is this important?

The purpose of asset characterisation is to establish the scope and boundaries of the risk assessment and provide contextual information (e.g. existing and/or planned controls, applicability of relevant laws, regulation and policies) that is important in assessing risk.

4.1.2.3 Asset classification

Classification of assets seeks to 'label' assets to increase awareness of their importance to the business and to determine appropriate responses (controls) for handling and protecting those assets. Assets can be classified individually, however in practice it is more efficient to group assets that have similar roles – for example all data assets relating to individual patients (appointments, patient records, diagnostic imaging) could be classified as a group.

For each asset (or asset group) a classification is assigned that indicates the severity of the impact on the organisation that loss of availability, integrity or confidentiality would have on the organisation. Under The Federal Privacy Act, and various other State and Territory Privacy and Health Acts, health information is deemed to be sensitive information and there are special provisions that need to be made for the appropriate safeguarding of this information. Understanding the assets that impact the protection of health information is important to recognise.

NESAF provides an indicative data security classification for guidance (refer to Appendix C:). The classification provides the following benefits:

- Provision of an efficient and consistent scheme for identifying the different sensitivities of various information assets, in particular information subject to Privacy Act provisions (federal, state and territory), across the eHealth domain.
- Ensures that more sensitive health information assets are identified to facilitate the application of appropriate protection from unauthorised disclosure or modification within the healthcare setting.
- Enables resources to be focused on protecting the most sensitive information assets within organisation undertaking eHealth activities.
- Guides further analysis of risks and controls for information assets.

The security classification should consider the confidentiality, integrity and availability requirements of the data.

Why is this important?

Security classification of information is important for all organisations in the management of risk and the implementation of appropriate controls, both process and technical, to protect information based on its classification. Information should be handled and controlled appropriately based on its classification during every phase of its lifecycle:

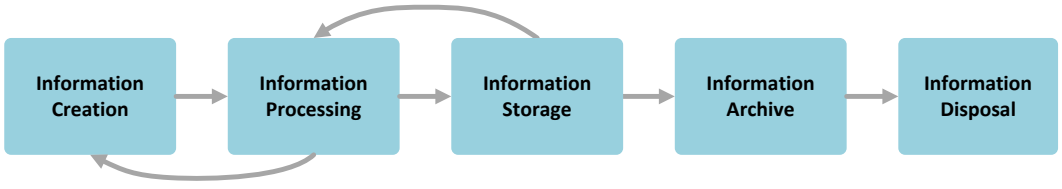
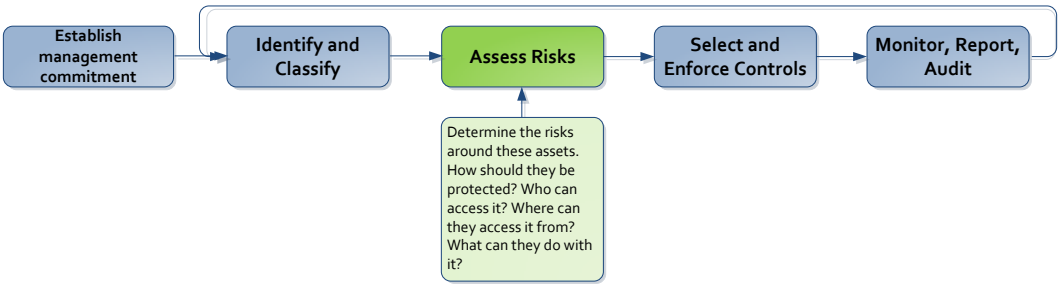


Figure 10: Information lifecycle

Useful references

- *Australian Standard AS ISO 27799 – 2011 Information security management in health using ISO-IEC 27002*. [AS27799]
- *Australian Standard AS/NZS 4360*:*1999 Risk Management.* [AS/NZS4360]
- *ISO 31000:2009 Risk management – Principles and guidelines*
- *HB174-2003 Handbook. Information security management – Implementation guide for the health sector*. [HB174]
- *Australian Government Information security management guidelines.* [AGISMG]
- *Queensland Government Information Security Classification Framework.* [QGISCF]
- *Data classification and management implementation guideline.* [GSDVIC]
- National Institute of Standards and Technology. *Risk Management Guide for Information Technology Systems*. [NIST1]
- *MEHARI Security Stakes Analysis and Classification Guide.* [MEHARI2010]
- *NESAF Implementer Blueprint – eHealth Process Patterns*. [NEHTA2011a]
- Appendix A: contains information on NESAF control areas and controls relating to C. Asset Management.
- Appendix C: Contains information for the classifying of information assets.

4.1.3 Assess risks



The concept of risk relates to the possibility of harm or loss and combines the probability of an event occurring and its consequence. Risk assessment is a standard information security process that identifies threats to and vulnerabilities of information systems and the associated risk that they present to the business.

A threat is an action or event that may result in a detrimental outcome to a system or information asset. A vulnerability is a weakness that can be exploited that may cause damage to a system or information asset. Risk is a function of the likelihood of a given threat triggering or exploiting a particular vulnerability and the resulting impact on the organisation. A threat does not present a risk when there is no vulnerability that can be exploited.

Risk is inherent in all businesses, but the investment being made in eHealth in Australia will result in increasingly larger quantities of information being transferred and exchanged in novel ways, across increasing numbers of organisations, to support emerging clinical models. The sensitive nature of health information, and the interconnectedness of national eHealth systems require additional oversight and vigilance in managing risks to healthcare information privacy and confidentiality in order to reap the benefits that eHealth offers the Australian healthcare system. As healthcare organisations increase the volume of eHealth transactions undertaken with external organisations, and the number of external organisations with which they exchange information, their risk profile will increase substantially.

Based on the scope defined in the identification and classification step, an organisation needs to identify potential threats to and vulnerabilities associated with their eHealth information assets. An important consideration in conducting a NESAF risk assessment is to consider the impact of threats and vulnerabilities at a local level on risks to national eHealth. For example, poor practice in relation to allowing multiple people to access the same user account may not appear to be a significant risk in a small organisation where users and consumers are perceived to be well-known to each other, however in the national eHealth environment such practice results in a risk that a user will be able to obtain unauthorised access (by accessing another users' account) to the healthcare information of a much greater number of individuals and avoid detection.

Following identification of threats and vulnerabilities, organisations should assess their current security measures in order to understand the likelihood that a potential vulnerability may be exploited. Finally, a risk level for a particular threat and associated vulnerabilities can be determined based on the likelihood and impact of a threat occurring and the adequacy of current security controls for reducing or eliminating the risk.

Why is this important?

A risk assessment will identify potential threats to and vulnerabilities of eHealth information assets and enable your organisation to determine what measures will be necessary to address/reduce those risks to an acceptable level.

How do organisations conduct a risk assessment?

The risk assessment should be undertaken in relation to the scope and set of information assets identified in Section 4.1.2 Identify and classify.

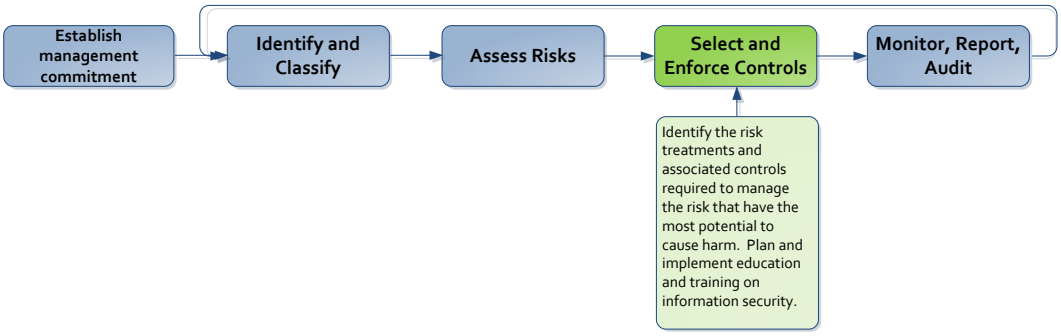
1. Threats should be identified and documented. Common threats to health information security are provided in the NESAF Risk Assessment tools (refer to Appendix E: Common threats to health information and associated vulnerabilities). Nevertheless, organisations should consider any relevant threats that exist in the context of their organisation to ensure completeness of the assessment. Information sources such as the organisation's own history of system break-ins, security violation reports, national eHealth user communities and information security advisers can be valuable resources in assisting organisations to comprehensively identify threats to information security. Common threat categories include natural threats (floods, electrical storms etc.), human threats (accidental/unintentional, deliberate) and environmental threats (power failure, liquid leakage etc.).
2. Vulnerabilities that could be exploited by potential threats should be identified. This process is similar to the process used for identifying threats. An additional way to identify technical vulnerabilities in information systems is through information systems security testing using security testing tools that can scan computers or networks for known technical vulnerabilities. (Refer to Appendix E: Common threats to health information and associated vulnerabilities).

3. Assess current security controls in order to understand the likelihood that a potential vulnerability may be exploited. The NESAF Gap Assessment Tool (refer to Appendix F: Sample Gap assessment tool) can assist organisations to determine their current compliance with NESAF controls.
4. Determine the level of risk associated with each identified threat and related vulnerabilities. Risk level is determined by assessing the likelihood of a given threat and impact of the threat occurrence. Likelihood relates to the probability that a threat will trigger or exploit a specific vulnerability. The impact of a threat occurring in an organisation (including the impact on national eHealth systems more broadly) relates to the potential outcomes that would arise. (Refer to Appendix H: Risk assessment tools).

Useful references

- *ISO 31000:2009 Risk management – Principles and guidelines*
- Appendix E: Common threats to health information and associated vulnerabilities – to assist in identifying threats and vulnerabilities.
- Appendix F: Sample Gap assessment tool – to assist in assessing current compliance with NESAF controls.
- Appendix G: Sample Gap assessment scorecard – to provide a summary of the outcomes of the gap assessment process.
- Appendix H: Risk assessment tools – to assist in determining probability, impact and overall risk level for each threat and related vulnerabilities.

4.1.4 Select and enforce controls



Once the risks to information security and access have been identified and assigned a risk level, the organisation should begin to identify the risk treatments (controls) required to manage the risks that have the most potential to cause harm. It may not be practical for an organisation to address all identified risks, so priority should be given to threats and associated vulnerabilities that have the greatest potential to compromise the confidentiality, availability and integrity of healthcare information.

Risk treatment options 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 and corrective actions such as business continuity management, disaster recovery, back-up, emergency procedures, to reduce the consequences of the risk occurring.
- Risk transfer – sharing the risk with another party or parties e.g. through the use of contracts, insurance, outsourcing arrangements.

Potential controls that could be implemented to treat risks should be prioritised and evaluated. Evaluation of controls should include considerations in relation to usability and clinical safety.

The definition of what level of risk is acceptable is dependent on many factors within an organisation, including the organisation's appetite for risk, costs associated with reducing, availability of effective protection methods, controls already in place, patient expectation, legislation and regulations and consideration of the additional benefits to the organisation of reducing particular risks. Risks are also dependent on the number of exchanges of information that take place with difference types of organisations, as well as the volume of these changes.

Figure 11 illustrates the trade-off that organisations should consider in relation to selecting and implementing appropriate controls. The costs of implementing controls should be justified by the reduction in the risk level and assessed against the risks associated with not implementing the control. Almost no information system is risk free and not all implemented controls can 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.

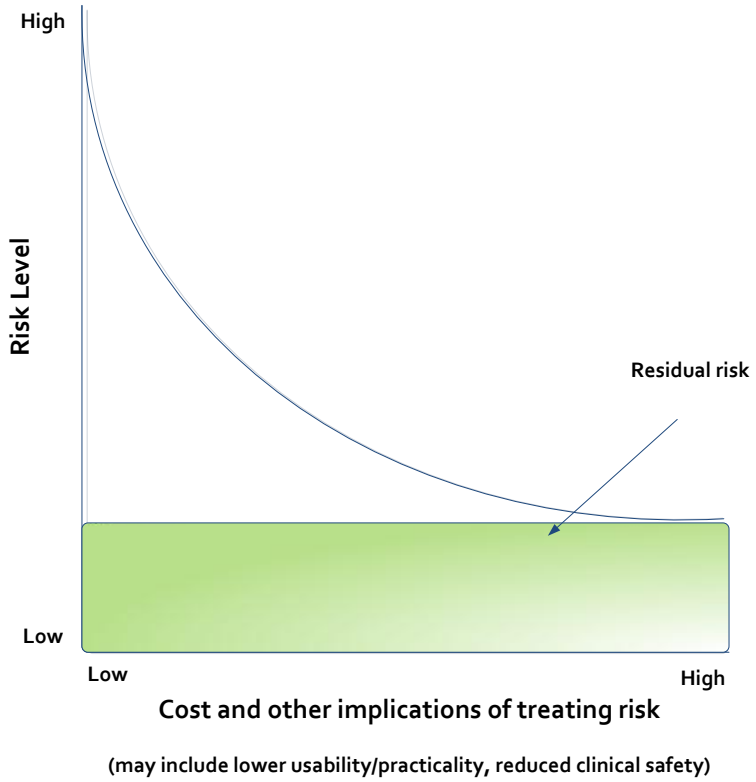


Figure 11: Cost-benefit trade-off – risk treatment options

Strong, effective information security infrastructure should comprise a mix of people, process and technology components, as the best available technical controls cannot mitigate all risks.

4.1.4.1 Risk Management action plan

Once appropriate controls have been selected, a Risk Management Action plan for implementing managing the identified information security risks should be developed. The plan should identify:

- Risks to be treated.
- Prioritisation of risks.
- Current controls.
- Additional/enhanced controls to be implemented.
- Responsibilities for implementing controls.
- Allocation of resources.
- Timeframes for implementation.
- Revised risk levels.

A template for use in security risk management action planning is included in Appendix I:

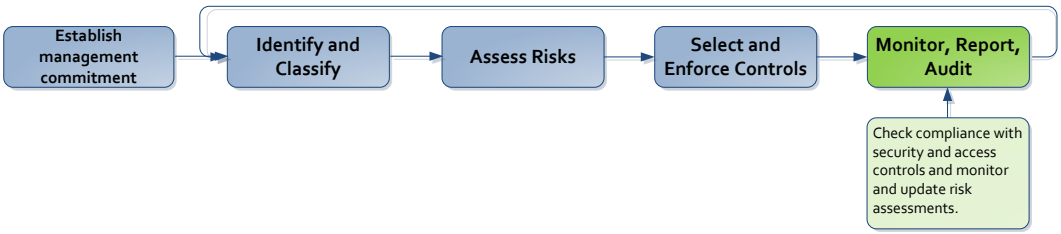
4.1.4.2 Training and awareness

A critical component of success of implementation of a comprehensive information security infrastructure relies on the awareness and cooperation of staff, contractors, health professionals and others within the organisation that must follow information security policies and procedures, and comply with implemented controls in order for them to be effective. Awareness training should begin at staff induction to familiarise new staff with the organisation's information security policies and expectation and continue on an ongoing basis.

Useful references

- Appendix A: contains information on NESAF Controls that may be useful to organisations in developing training and awareness information for staff.
- Appendix I: contains a template for use in the development of an action plan.

4.1.5 Monitor, report, audit



The final step in the NESAF implementation process is to continue monitoring, evaluating and reporting on the risk mitigation measures (controls) that have been implemented.

Why is this important?

As organisations change and the information assets within them change (e.g. network expansions, introduction of new software/hardware), threats also change. Consequently risk analysis and management are ongoing and dynamic processes that require periodic review and updates.

Monitoring and reviewing implementation of controls is also valuable for learning lessons that lead to continuous improvement in information security management.

How do organisations check, monitor and review information security risk?

- Check compliance with security and access controls.
- Establish processes to identify actual and potential information security incidents or systems weaknesses.
- Monitor and update information security risk assessments as required.
- Monitor the effectiveness of the risk-based approach to managing information through internal reviews and independent audit.
- Review and update policies and processes on a regular basis.

5 References

[AGISMG]	Australian Government. *Information security management guidelines: Australian Government security classification system.* Version 1.0. Approved 19 July 2011 Accessed at: http://www.ag.gov.au
[Andress2004]	Amanda Andress *Surviving security: how to integrate people, process and technology*. 2nd Edition. CRC Press. 2004.
[AS27799]	Standards Australia AS ISO 27799-2011 *Information security management in health using ISO/IEC 27002.*
[AS/NZS4360]	Standards Australia AS/NZS 4360:1999 *Risk Management.*
[GSDVIC]	Government Services Division, Department of Treasury and Finance. Victorian Government. *Data classification and management implementation guideline. Version 1.0. February 2011.* Accessed at: https://www.dtf.vic.gov.au
[HB174]	Standards Australia HB174 – 2003 *Information security management: Implementation guide for the health sector*.
[Infoway2006]	Canada Health Infoway. *An overview of the Electronic Health Record Privacy and Security: Conceptual Architecture*. 2006.
[ISO/IEC27002]	*ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management*. 2005.
[ISO/TS25237]	*ISO/TS 25237 Technical specification: Health Informatics – Pseudonymization*. 2008.
[ISO31000]	*ISO 31000:2009 Risk management – principles and guidelines.*

[MEHARI2010]	MEHARI 2010 *Security Stakes Analysis and Classification Guide. August 2010*. Accessed at: https://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Stakes-Analysis-and-Classification-Guide.pdf
[NEAF2009]	Department of Finance and Deregulation *National e-Authentication Framework*. January 2009. Accessed at: http://www.finance.gov.au/e-government/security-and-authentication/docs/NeAFFramework.pdf
[NEHTA1]	National E-Health Transition Authority *Healthcare Today: E-Health: an information revolution*. http://www.nehta.gov.au/publications/nehta-publications Accessed 15 April 2011.
[NEHTA2009]	National E-Health Transition Authority. *HI Service Security and Access Framework*. 13 November 2009.
[NEHTA2010a]	National E-Health Transition Authority *NEHTA Blueprint* Version 1.0. Draft for consultation. 13 August 2010. https://vendors.nehta.gov.au
[NEHTA2010b]	National E-Health Transition Authority *National E-Health Security and Access Framework – Release 1*. 17 December 2010.
[NEHTA2011a]	National E-Health Transition Authority *National E-Health Security and Access Framework Release 3 – Implementer Blueprint*. *v*.1.0, 20111125 https://vendors.nehta.gov.au
[NEHTA2011b]	National E-Health Transition Authority National e-Health Security and Access Framework – Release 3 -Framework Model and Controls. V1.0, 20111125 https://vendors.nehta.gov.au

[NHS1]	National Health Service (UK) *Information Security Management. NHS Code of Practice*.
[NHS2]	National Health Service (UK) *Information Governance Toolkit* Requirement No. 8-300. Acute Trust. v.8.0
[NIST1]	National Institute of Standards and Technology Special Publication 800-30. *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*. October 2001.
[QGISCF]	*Queensland Government Information Security Classification Framework. Final. November 2010.* Accessed at: http://www.qgcio.qld.gov.au/SiteCollectionDocuments/Architecture%20and%20Standards/QGISCF.pdf
[RACGP1]	Royal Australian College of General Practitioners. *Frequently asked questions: RACGP Computer security guidelines* (3rd edition) Accessed at: http://www.racgp.org.au/Content/NavigationMenu/ClinicalResources/ehealth/ComputerSecurityGuidelines/ComputerSecurityGuidelinesFAQs.pdf
[RACGP2010]	Royal Australian College of General Practitioners *Computer security guidelines: A self-assessment guide and checklist for general practice*. 3rd edition. October 2010.

6 Terms and abbreviations

Access Control	A means of controlling access by users to computer systems or to data on a computer system.
Asset	Anything that has value to an organisation. [AS27799]
Authentication	Means that one can verify whether the sender is who they say they are. [RACGP1]
Availability	Refers to the property of being accessing and usable on demand by an authorised entity. [AS27799]
Clinical Safety	Clinical safety is concerned with identification and reduction of harm to patients to acceptable levels
Confidentiality	Refers to the property that information is not made available or disclosed to unauthorised individuals, entities or processes.
Control	A means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature. Also used as a synonym for safeguard or countermeasure.[ISO/IEC27002]
Denial of service	An attack that results in preventing authorised access and availability of organisational information/services/resources.
Encryption	Data is electronically 'scrambled' so that it cannot be read unless the information is decrypted. [RACGP1]
Health information system	Repository of information regarding the health of a subject of care in computer-processable form, stored and transmitted securely, and accessible by multiple authorised users. [AS27799]
Healthcare	Any type of service provided by professionals or paraprofessionals with an impact on health status. [AS27799]
Healthcare organisation	Generic term used to describe many types of organisations that provide healthcare services.[AS27799)
Health professional	A person who is authorised buys a recognised body to be qualified to perform certain health duties. [AS27799]

Information security	Preservation of confidentiality, integrity and availability of information.
Integrity	Refers to the property that data has when it has not been altered or destroyed, or a system has when it can perform its intended function in an unimpaired manner, free from deliberate or accidental unauthorised manipulation of the system. [AS27799]
ISMS	Information Security Management System.
ISMF	Information Security Management Forum.
NeAF	National eAuthentication Framework.
NESAF	National E-Health Security and Access Framework.
Malicious code	Programs such as viruses and worms designed to exploit weaknesses in computer software and replicate and/or attach themselves to other software programs on a computer or a network.
Personal health information	Information about an identifiable person which relates to the physical or mental health of the individual or to provision of health services to the individual. [AS27799]
Privacy	Privacy refers to the protection and appropriate handling of information which identifies (or could be used to reasonably ascertain the identity of) an individual.
Provenance	Provenance is a method to enforce security requirements by means of protecting the traces of historical data or information from its creation and transition to its current state. An electronic "chain of custody".
Risk	The probability that a given threat will exploit a given vulnerability. [HB174]
Risk assessment	The process of identifying risks to a business and determining the probability of occurrence, the resulting impact, and identifying actions that would treat the risk.
Threat	An action or event that may result in a detrimental outcome to a system or information asset. [HB174]
Vulnerability	A weakness that can be exploited that may cause damage to a system or information assets.[HB174]

Appendix A: NESAF controls

The Control Categories, Control Objectives and Controls contained in the following table have been derived directly from AS 27799 and ISO 27002, with some additional controls identified during the development of NESAF Release 1. A more extensive description of each control, and identification of the source from which it was derived, is included within the *NESAF Framework Model and Controls* Document [NEHTA2011b].

Table 1: Control Area A. Information security policy

NESAF R3 Ref	Control Category	Control
A.1	Information security policy	**Objective:** To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
A.1.1	Information security policy document	Organisations processing health information, including personal health information, should have a written information security policy that is approved by management, published, and then communicated to all employees and relevant external parties.
A.1.2	Review of the information security policy document	The health organisation's information security policy should be subject to ongoing, staged review such that the totality of the policy is addressed at least annually. The policy should be reviewed after the occurrence of a serious security incident.

Table 2: Control Area B. Organising information security

NESAF R3 Ref	Control Category	Control
B.1	Internal organisation	**Objective:** To manage information security within the organisation.

NESAF R3 Ref	Control Category	Control
B.1.1	Management commitment to information security, information security coordination and allocation of information security responsibilities	Organisations should: 1. Clearly define and assign information security responsibilities. 2. Have an ISMF in place to ensure that there is clear direction and visible management support for security initiatives involving the security of health information. At a minimum, organisations should have at least one individual responsible for health information security within the organisation. The health information security forum should meet regularly, on a monthly or near-to-monthly basis. A formal scope statement should be produced that defines the boundary of compliance activity in terms of people, processes, places, platforms and applications.
B.1.2	Authorisation process for information processing facilities	A management authorisation process for new information processing facilities should be defined and implemented.
B.1.3	Confidentiality agreements	Organisations should have a confidentiality agreement in place that specifies the confidential nature of health information. The agreement should be applicable to all personnel accessing health information.
B.1.4	Contact with authorities, contact with special interest groups	Appropriate contacts with relevant authorities should be maintained. Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained, for example RACGP.
B.1.5	Independent review of information security	The organisation's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.
B.2	Third parties	**Objective:** To maintain the security of the organisation's information and information processing facilities that are accessed processed, communicated to, or managed by third parties.

NESAF R3 Ref	Control Category	Control
B.2.1	Identification of risks related to external parties	Organisations processing health information should assess the risks associated with access by external parties to these systems or the data they contain, and then implement security controls that are appropriate to the identified level of risk and to the technologies employed.
B.2.2	Addressing security when dealing with customers	All identified security requirements should be addressed before giving third parties access to the organisation’s information or assets.
B.2.3	Addressing security in third-party agreements	Health organisations using the services of third parties, where the services of those parties process personal health information, should employ formal contracts that specify: 1. The confidential nature and value of the personal health information; 2. The security measures to be implemented and/or complied with; 3. Limitations to access to these services by third parties; 4. The service levels to be achieved in the services provided; 5. The format and frequency of reporting to the health organisation's ISMF; 6. The arrangement for representation of the third party in appropriate health organisation meetings and working groups; 7. The arrangements for compliance auditing of the third parties; and 8. The penalties exacted in the event of any failure in respect of the above.

Table 3: Control Area C. Asset Management

NESAF R3 Ref	Control Category	Control
C.1	Responsibility for health information assets	**Objective:** To achieve and maintain appropriate protection of organisational assets.
C.1.1	Responsibility for health information assets	Organisations processing personal health information should: 1. Account for health information assets (inventory); 2. Have a designated custodian of these health information assets; and 3. Have rules for acceptable use of these assets that are identified, documented, and implemented.
C.2	Health information classification	**Objective:** To ensure that information receives an appropriate level of protection.
C.2.1	Classification guidelines	Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organisation. Organisations processing personal health information should uniformly classify such data as confidential.
C.2.2	Information labelling and handling	All health information systems processing personal health information should inform users of the confidentiality of personal health information accessible from the system and should label hardcopy output as confidential when it contains personal health information.
C.2.3	De-identification of health information output	Health information systems should enable the de-identification of healthcare information output where such data are used for purposes other than the clinical care of patients.

Table 4: Control Area D. Human resources security

NESAF R3 Ref	Control Category	Control
D.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.
D.1.1	Roles and responsibilities	Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organisation's information security policy.
D.1.2	Screening	Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks. All organisations whose staff, contractors or volunteers process (or are expected to process) personal health information should, as a minimum, verify the identity, current address and previous employment of such staff, contractors and volunteers at the time of job applications.
D.1.3	Terms and conditions of employment	As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organisation's responsibilities for information security.
D.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, and are equipped to support organisational security policy in the course of their normal work, and to reduce the risk of human error.
D.2.1	Management responsibilities	Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organisation.
D.2.2	Information security awareness, education and training	All employees of the organisation and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organisation policies and procedures, as relevant for their job function. All organisations processing personal health information should ensure that information security education and training are provided on induction and, that regular updates in organisational security policies and procedures are provided to all employees, contractors, researchers, students and volunteers who process personal health information.
D.2.3	Disciplinary process	There should be a formal disciplinary process for employees who have committed a security breach.

NESAF R3 Ref	Control Category	Control
D.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.
D.3.1	Termination responsibilities and return of assets	Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.
D.3.2	Removal of access rights	All organisations that process health information should, as soon as possible, terminate the user access privileges with respect to such information for any departing permanent or temporary employee, third-party contractor or volunteer upon termination of employment, contracting or volunteer activities.

Table 5: Control Area E. Physical and environmental security

NESAF R3 Ref	Control Category	Control
E.1	Secure areas	**Objective:** To prevent unauthorised physical access, damage, and interference to the organisation's premises and information.
E.1.2	Physical security perimeter	Organisations processing personal health information should use security perimeters (e.g. walls, card entry gates or manned reception desks) to protect areas that contain information processing facilities supporting such health applications. These should be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.
E.1.3	Physical entry controls; securing offices, rooms and facilities; protecting against external and environmental threat; working in secure areas	Secure areas should be protected by appropriate entry controls to ensure that only authorised personnel are allowed access. Physical security for offices, rooms, and facilities should be designed and applied. Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied. Physical protection and guidelines for working in secure areas should be designed and applied.

NESAF R3 Ref	Control Category	Control
E.1.4	Public access, delivery and loading areas	Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises should be controlled, and, if possible, isolated from information processing facilities to avoid unauthorised access.
E.2	Equipment security	**Objective:** To prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.
E.2.1	Equipment siting and protection	Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.
E.2.2	Supporting utilities, cabling security and equipment maintenance	Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities. Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage. Equipment should be correctly maintained to ensure its continued availability and integrity.
E.2.3	Security of equipment off-premises	Security should be applied to off-site equipment taking into account the different risks of working outside the organisation's premises. Organisations processing personal health information should ensure that any use, outside its premises, of medical devices that record or report data has been authorized. This should include equipment used by remote workers, even where usage is perpetual (i.e. where it forms a core feature of the employee's role, such as for ambulance personnel, therapists, etc.).
E.2.4	Secure disposal or re-use of equipment	All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. Organisations processing health information applications should securely overwrite or else destroy all media containing health information application software or personal health information when the media are no longer required for use.
E.2.5	Removal of property	Equipment, information or software should not be taken off-site without prior authorisation. Organisations providing or using equipment, data or software to support a healthcare applications containing personal health information should not allow such equipment, data or software to be removed from the site or relocated within it without authorisation by the organisation.

Table 6: Control Area F. Communications and operations management

NESAF R3 Ref	Control Category	Control
F.1	Operational procedures and responsibilities	**Objective:** To ensure the correct and secure operation of information processing facilities.
F.1.1	Documented operating procedures	Operating procedures (including processing and handling of information, backup, scheduling requirements, handling errors, support contracts, output and media handling instructions, system restart and recovery, management of audit-trail and system log info) should be documented, maintained, and made available to all users who need them.
F.1.2	Change management	Changes to information processing facilities and systems should be controlled. Organisations processing personal health information should, by means of a formal and structured change control process, control changes to information processing facilities and systems that process personal health information to ensure the appropriate control of host applications and systems and continuity of patient care.
F.1.3	Segregation of duties	Duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.
F.1.4	Separation of development, test and operational facilities	Development, test, and operational facilities should be separated to reduce the risks of unauthorised access or changes to the operational system. Organisations processing personal health information should separate (physically or virtually) development and testing environments for health information systems processing such information from operational environments hosting those health information systems. Rules for the migration of software from development to operational status should be defined and documented by the organisations hosting the affected applications.
F.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.
F.2.1	Service delivery	It should be ensured that the security controls, service definitions and delivery levels included in the third-party service delivery agreements are implemented, operated, and maintained by the third party.

NESAF R3 Ref	Control Category	Control
F.2.2	Monitoring and review of third party services	The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.
F.2.3	Managing changes to third party services	Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.
F.3	System Planning and Acceptance	**Objective:** To minimise the risk of systems failures.
F.3.1	Capacity management	The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.
F.3.2	System acceptance	Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance. Organisations processing personal health information should establish acceptance criteria for planned new information systems, upgrades and new versions. They should carry out suitable tests of the system prior to acceptance.
F.4	Protection against malicious and mobile code	**Objective:** To protect the integrity of software and information.
F.4.1	Controls against malicious code	Detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented. Organisations processing personal health information should implement appropriate prevention, detection and response controls to protect against malicious software and should implement appropriate user awareness training.
F.4.2	Controls against mobile code	Where the use of mobile code is authorised, the configurations should ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code should be prevented from executing.
F.5	Health information backup	**Objective**: To maintain the integrity and availability of information and information processing facilities.

NESAF R3 Ref	Control Category	Control
F.5.1	Health information backup	Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy. Organisations processing personal health information should backup all personal health information and store it in a physically secure environment to ensure its future availability. To protect its confidentiality, personal health information should be backed up in an encrypted format.
F.6	Network security management	**Objective**: To ensure the protection of information in networks and the protection of the supporting infrastructure.
F.6.1	Network controls	Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.
F.6.2	Security of network services	Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced. Organisations processing personal health information should carefully consider what impact the loss of network service availability will have upon clinical practice.
F.7	Media handling	**Objective:** To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities.
F.7.1	Management of removable computer media	There should be procedures in place for the management of removable media. (Organisations should ensure that all personal health information stored on removable media is: 1. Encrypted while its media are in transit or, 2. Protected from theft while its media are in transit.
F.7.2	Disposal of media	Media should be disposed of securely and safely when no longer required, using formal procedures. All personal health information should be securely overwritten or else the media destroyed when no longer required for use.
F.7.3	Information handling procedures	Procedures for the handling and storage of information should be established to protect this information from unauthorised disclosure of misuse. Media containing personal health information should be either physically protected or else have their data encrypted. The status and location of media containing unencrypted personal health information should be monitored.

NESAF R3 Ref	Control Category	Control
F.7.4	Security of system documentation	System documentation should be protected against unauthorised access.
F.8	Exchanges of information	**Objective:** To maintain the security of information and software exchanged within an organisation and with any external entity.
F.8.1	Health information exchange policies and procedures and exchange agreements	Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities. Agreements should be established for the exchange of information and software between the organisation and external parties.
F.8.2	Physical media in transit	Media containing information should be protected against unauthorised access, misuse or corruption during transportation beyond an organisation's physical boundaries.
F.8.3	Electronic messaging	Information involved in electronic messaging should be appropriately protected. (Organisations transmitting personal health information should take steps to ensure its confidentiality and integrity.)
F.8.4	Health information systems	Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.
F.9	Electronic health information services	**Objective:** To ensure the security of electronic commerce services, and their secure use.
F.9.1	Electronic commerce and online transactions	Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorised disclosure and modification. Information involved in on-line transactions should be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.
F.9.2	Publicly available health information	Publicly available health information (as distinct from personal health information) should be archived. The integrity of publicly available health information should be protected to prevent unauthorised modification. The source (authorship) of publicly available health information should be stated and its integrity should be protected.

NESAF R3 Ref	Control Category	Control
F.10	Monitoring	**Objective:** To detect unauthorised information processing activities.
F.10.1	Audit logging	Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.
F.10.2	Audit review	A patient can ask to see a record showing when and by whom their healthcare information was accessed. In the absence of any prohibition on doing so, any information that may be relevant (irrespective of how it is stored within an application) should be provided.
F.10.3	Monitoring system use	Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly. Audit logging facility should be operational at all times while the health information system being audited is available for use.
F.10.4	Protection of log information	Audit records should be secure and tamper-proof. Access to system audit tools and audit trails should be safeguarded to prevent misuse or compromise.
F.10.5	Administrator and operator logs	System administrator and system operator activities should be logged.
F.10.6	Fault logging	Faults should be logged, analysed and appropriate action taken.
F.10.7	Clock synchronisation	Health information systems supporting time-critical-shared care activities should provide time synchronisation services to support tracing and reconstitution of activity timelines where required.

Table 7: Control Area G. Access control

NESAF R3 Ref	Control Category	Control
G.1	Requirements for access control in health	**Objective:** To control access to information.

NESAF R3 Ref	Control Category	Control
G.1.1	General	Organisations processing personal health information should control access to such information. In general, users of health information systems should only access personal health information when a health care relationship exists between the users and the data subject; when the user is carrying out an activity on behalf of the data subject; and when there is a need for specific data to support this activity.
G.1.2	Access control policy	Organisations processing personal health information should have an access control policy governing access to this data. The organisation's policy on access control should be established on the basis of predefined roles with associated authorities which are consistent with, but limited to, the needs of that role. The access control policy, as a component of the information security policy framework described in A.1.1, should reflect professional, ethical, legal and subject-of-care-related requirements and should take account of the tasks performed by health professionals and the task's workflow.
G.2	User access management	**Objective:** To ensure authorised user access and to prevent unauthorised access to information systems.
G.2.1	User registration	Access to health information systems that process personal health information should be subject to a formal user registration process. User registration procedures should ensure that the level of authentication required of claimed user identity is consistent with the levels of access that will become available to the user. User registration details should be periodically reviewed to ensure that they are complete, accurate and that access is still required.
G.2.2	Patient Registration (anonymous/pseudonymous)	Healthcare information systems should support the ability of patients to receive anonymous or pseudonymous care wherever it is lawful and practicable.

NESAF R3 Ref	Control Category	Control
G.2.3	Privilege management	The allocation and use of privileges should be restricted and controlled. Several access control strategies can help significantly to ensure the confidentiality and integrity of personal health information: 1. Role-based access control, which relies upon the professional credentials and job titles of users established during registration to restrict users' access privileges to just those required to fulfil one or more well-defined roles. 2. Workgroup-based access control, which relies upon the assignment of users to workgroups (such as clinical teams) to determine which records they can access. 3. Discretionary access control, which enables users of health information systems who have a legitimate relationship to a subject of care's personal health information (e.g. a family physician) to grant access to other users who have no previously established relationship to that subject of care's personal health information (e.g. a specialist).
G.2.4	User password management	The allocation of passwords should be controlled through a formal management process.
G.2.5	Review of user access rights	Management should review users' access rights at regular intervals using a formal process. Special consideration needs to be given to users who will reasonably be expected to provide emergency care, as they may need access to personal health information in emergency situations where a subject of care may be unable to communicate consent.
G.3	User responsibilities	**Objective:** To prevent unauthorised user access, and compromise or theft of information and information processing facilities.
G.3.1	Password use	Users should be required to follow good security practices in the selection and use of passwords.
G.3.2	Unattended user equipment	Users should ensure that unattended equipment has appropriate protection.
G.3.3	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

NESAF R3 Ref	Control Category	Control
G.4	Network access control and operation system access control	**Objective:** To prevent unauthorised access to networked services.
G.4.1	Policy on use of network services	Users should only be provided with access to the services that they have been specifically authorised to use.
G.4.2	User authentication for external connections	Appropriate authentication methods should be used to control access by remote users.
G.4.3	Equipment identification in networks	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.
G.4.4	Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports should be controlled.
G.4.5	Segregation in networks	Groups of information services, users and information systems should be segregated on networks.
G.4.6	Network connection control	For shared networks, especially those extending across the organisation's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications.
G.4.7	Network routing control	Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.
G.4.8	Secure log-on procedures	Access to operating systems should be controlled by a secure log-on procedure.
G.4.9	User identification and authentication	All users should have a unique identifier for the personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.
G.4.10	Password management system	Systems for managing passwords should be interactive and should ensure quality passwords.

NESAF R3 Ref	Control Category	Control
G.4.11	Use of system utilities	The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.
G.4.12	Session time-out	Inactive sessions should shut down after a defined period of inactivity.
G.4.13	Limitation of connection time	Restrictions on connection times should be used to provide additional security for high-risk applications.
G.5	Application and information access control	**Objective:** To prevent unauthorised access to information held in application systems.
G.5.1	Information access restriction	Health information systems processing personal health information should authenticate users and should do so by means of authentication involving at least two factors.
G.5.2	Sensitive system isolation	Sensitive systems should have a dedicated (isolated) computing environment.
G.6	Mobile computing and teleworking	**Objective:** To ensure information security when using mobile computing and teleworking facilities
G.6.1	Mobile computing and communications	A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.
G.6.2	Teleworking	A policy, operational plans and procedures should be developed and implemented for teleworking activities.

Table 8: Control Area H. Information systems acquisition, development and maintenance

NESAF R3 Ref	Control Category	Control
H.1	Security requirements of information systems	**Objective:** To ensure that security is an integral part of information systems.
H.1.1	Security requirements analysis and specification	Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.
H.2	Correct processing in applications	**Objective:** To prevent errors, loss, unauthorised modification or misuse of information in applications.
H.2.1	Uniquely identifying subjects of care	Health information systems processing personal health information should: 1. Ensure that each subject of care can be uniquely identified within the system; 2. Be capable of merging duplicate or multiple records if it is determined that multiple records for the same subject of care have been created unintentionally or during a medical emergency.
H.2.2	Input data validation	Data input to applications should be validated to ensure that this data is correct and appropriate.
H.2.3	Error correction	Where errors in a healthcare information record are identified, it should be possible to annotate information to indicate the nature of the error. Evidence of the original form of the record should be maintained and the time and date of entries, including those correcting errors, should be recorded.
H.2.4	Control of internal processing	Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.
H.2.5	Message integrity	Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.

NESAF R3 Ref	Control Category	Control
H.2.6	Output data validation	Health information systems processing personal health information should provide personally identifying information to assist health professionals in confirming that the electronic health record retrieved matches the subject of care under treatment.
H.2.7	Data output for the purposes of non-clinical care	When data is sent, exported or printed from healthcare information systems for purposes other than the clinical care of patients, systems should enable a record to be made of the reason and purpose for which data is being provided.
H.3	Cryptographic controls	**Objective:** To protect the confidentiality, authenticity or integrity of information by cryptographic means.
H.3.1	Policy on the use of cryptographic controls and key management	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.
H.3.2	Key management	Key management should be in place to support the organisation's use of cryptographic techniques.
H.4	Security of system files	**Objective:** To ensure the security of system files.
H.4.1	Control of operational software	There should be procedures in place to control the installation of software on operational systems.
H.4.2	Protection of system test data	Test data should be selected carefully, and protected and controlled. Health or personal information should not be used for testing purposes.
H.4.3	Access control to program source code	Access to program source code should be restricted.
H.5	Security in development and support processes, and technical vulnerability management	**Objectives:** To maintain the security of application system software and information and to reduce risks resulting from exploitation of published technical vulnerabilities.

NESAF R3 Ref	Control Category	Control
H.5.1.	Change control procedures	The implementation of changes should be controlled by the use of formal change control procedures.
H.5.2	Technical review of applications after operating system changes	When operating systems are changed, business-critical applications should be reviewed and tested to ensure there is no adverse impact on organisational operations or security.
H.5.3	Restrictions on changes to software packages	Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.
H.5.4	Information leakage	Opportunities for information leakage should be prevented.
H.5.5	Outsourced software development	Outsourced software development should be supervised and monitored by the organisation.
H.5.6	Control of technical vulnerabilities	Timely information about technical vulnerabilities of information systems being used should be obtained, the organisation's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

Table 9: Control Area I. Information security incident management

NESAF R3 Ref	Control Category	Control
I.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.
I.1.1	Reporting information security events and weaknesses	Information security events should be reported through appropriate management channels as quickly as possible. Health organisations should establish security incident management responsibilities and procedures.

NESAF R3 Ref	Control Category	Control
I.2	Management of incidents and improvements	**Objective:** To ensure a consistent and effective approach is applied to the management of information security incidents.
I.2.1	Responsibilities and procedures	Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.
I.2.2	Learning from incidents	There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.
I.2.3	Collection of evidence	Where a follow-up action against a person or organisation after an information security incident involves legal action(either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Table 10: Control Area J. Information security aspects of business continuity management

NESAF R3 Ref	Control Category	Control
J.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.
J.1.1	Including information security in the business continuity management process	A managed process should be developed and maintained for business continuity throughout the organisation that addresses the information security requirements needed for the organisation's business continuity.
J.1.2	Business continuity and risk assessment	Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security.
J.1.3	Developing and implementing continuity plans including information security	Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

NESAF R3 Ref	Control Category	Control
J.1.4	Business continuity planning framework	A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.
J.1.5	Testing, maintaining and re-assessing business continuity plans	Business continuity plans should be tested and updated regularly to ensure that they are up-to-date and effective.

Table 11: Control Area K. Compliance

NESAF R3 Ref	Control Category	Control
K.1	General	**Objective:** Establish a graduated compliance auditing framework.
K.1.1	General	Health organisations should put a compliance auditing programme in place that addresses the full life cycle of operations, i.e. not just of those processes that identify issues, but also of those that review outcomes and that decide on updates to the Information Security Management System (ISMS). Health organisations' audit programmes should be formally structured to cover all elements of this framework, all areas of risk and all implemented controls, within a 12 to 18 month cycle.
K.2	Compliance with legal requirements	**Objective:** To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

NESAF R3 Ref	Control Category	Control
K.2.1	Identification of applicable legislation, intellectual property rights and protection of organisational records	All relevant statutory, regulatory and contractual requirements and the organisation's approach to meet these requirements should be explicitly defined, documented and kept up to date for each information system and the organisation. Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products. Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual and business requirements.
K.2.2	Data protection and privacy of personal information	Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses. Organisations processing personal health information should manage informational consent of subjects of care. Where possible, informational consent of subjects of care should be obtained before personal health information is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the healthcare organisation.
K.2.3	Prevention of misuse of information-processing activities and regulation of cryptographic controls	Users should be deterred from using information processing facilities for unauthorised purposes. Cryptographic controls should be used in compliance with the relevant agreements, laws and regulations.
K.3	Compliance with security policies and standards and technical compliance	**Objective:** To ensure compliance of systems with organisational security policies and standards.
K.3.1	Compliance with security policies and standards	Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.
K.3.2	Technical compliance checking	Information systems should be regularly checked for compliance with security implementation standards.
K.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.

NESAF R3 Ref	Control Category	Control
K.4.1	Information systems audit controls	Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimise the risk of disruptions to business processes.

Appendix B: Key elements of an information security and access policy

Security policies provide direction and support for health information security; identify the security and access control principles that will be implemented in the organisation at a high level, and serve as a point of reference for all staff in relation to their information security responsibilities.

Guidance for developing an Information Security and Access policy:

Policies should be:

- Consistent with the organisation's culture and business practices
- Realistic and explicitly endorsed by management
- Communicated effectively within the organisation
- Complied with through the implementation of controls
- Supported by compliance monitoring procedures and audit and include sanctions for non-compliance
- Consistent with the NESAF principles and control objectives
- Reviewed on a regular (e.g. annual) basis.

The policy should contain:

- A definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing. This should include statements about:
  - The need for health information security.
  - The goals of health information security.
- A statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives.
- A framework for setting control objectives and controls, including the structure of risk assessment and risk management (these may be based on the NESAF model and risk-based approach).
- A brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organisation including:

  - Legislative, regulatory and contractual requirements, including those for the protection of personal health information and the legal and ethical responsibilities of health professionals to protect this information. (Legislative and regulatory requirements may be State/Territory specific).
  - Security education, training and awareness requirements.
  - Business continuity management.
  - Consequences of information security policy violations.
- A definition of general and specific responsibilities for information security management. This should include arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentiality, without fear of blame or recrimination.
- References to documentation that may support the policy such as more detailed organisational security policies and procedures for specific information systems or security rules that staff members should comply with.

Specific considerations

In creating an information security policy, health organisations should consider:

- The rights and ethical responsibilities of staff, as agreed in law, and as accepted by members of professional bodies.
- The rights of subjects of care, where applicable, to privacy and to access to their records.
- The obligations of clinicians with respect to obtaining informational consent from subjects of care and maintaining the confidentiality of personal health information.
- The legitimate needs of clinicians and health organisations to be able to overcome normal security protocols in certain circumstances (often due to the incapacity of consumers/patients to express their preferences), and the procedures required to overcome this.
- The obligations of respective health organisations, and of consumers/patients, where healthcare is delivered on a ‘shared care’ or ‘extended care’ basis.
- The laws, protocols and procedures to be applied to the sharing of information for the purposes of research and clinical trials.
- The arrangements for, and authority limits of, temporary staff, such as locums, students and 'on-call' staff.
- The arrangements for, a limitations placed upon, access to personal health information by volunteers and support staff such as clergy and charity personnel.

Communication of the policy

The organisation's Information Security Policy should be communicated throughout the organisation in a form that is relevant, accessible and understandable. This may include making the document available electronically via email or on the organisation's intranet site. All staff should be required to read, understand and acknowledge the content, and all new employees should be made aware of the policy as part of employee induction.

Appendix C: Asset Classification

This appendix describes the roles common to eHealth information security management, to provide guidance on key issues and responsibilities that could be included in role descriptions within a healthcare organisation. Individual organisations may describe roles differently and/or combine some of the roles within their organisation. The list is intended to provide useful guidance, rather than prescriptive information.

Role	Responsibilities
Business Owner/Director of Business	• Overall responsibility for information security within the organisation.
Senior Management	• Ensure that the necessary resources are applied effectively to implement appropriate security and access control needed to accomplish the NESAF goals and principles. • Endorse and communicate the organisation's Information Security Policy. • Ensure that the Information Security Policy and associated policies and procedures are reviewed at least annually. • Identify how to address non-compliance with information security policy.
Chief Information Officer/IT Manager	• Responsible for the organisation's IT planning, budgeting and performance, including its information security components. • Ensure that decisions, made in relation to information security and access, are founded on a risk-based approach. • Ensure that compliance with the organisation's information security policy is monitored and reviewed. • Evaluate information received from the monitoring and reviewing of information security incidents, and recommend appropriate actions.

Role	Responsibilities
System and information owners	• Responsible for ensuring that proper controls are implemented to address confidentiality, availability and integrity of the systems and healthcare information they own. • Be fully involved in the risk management approach to information security. • Identify significant threat changes and exposure of information and information processing facilities to threats. • Liaise with external providers to inform them of and enforce security requirements. • Report technical vulnerabilities and incidents to senior management. • Evaluate information received from the monitoring and reviewing of information security incidents, and recommend appropriate actions.
Business and functional managers	• Take an active role in the risk management approach. • Contribute to decision making in relation to selection of controls. • Make staff aware of their responsibilities regarding physical and information security. • Ensure that staff are trained in relation to information security policies and procedures. • Ensure that staff and third parties sign the organisation's information security policy and confidentiality agreement. • Evaluate information received from the monitoring and reviewing of information security incidents, and recommend appropriate actions.
Health Professionals	• Understand their Professional Code of conduct in relation to the privacy and security of healthcare information.
Everybody	• Act in accordance with the organisation's information security policy and make security an inbuilt part of conducting their everyday business.

Appendix D: Security and access role descriptions

Security classifications commonly used in government within Australia, the *Australian Government Information security management guidelines - Australian Government security classification system* support the Australian Government Information Security Management Protocol and applies to all agencies identified in Section 5.4 of the *Australian Government Protective Security Policy Framework (PSPF)*.

The ISO/TS 14265 Health Informatics - Classification of Purposes for processing health information is a contemporary framework for classifying the purposes for which health information is used. Each purpose within the publication defines a context that then allows an organisation to consider appropriate collection, access and processing activities surrounding health information in that context. Organisations should consider in each context relevant to them at least the following aspects:

- What information is appropriate to collect?
- How should the information be used?
- To whom should the information be disclosed?
- For how long should the information be retained?

ISO/TS 14265 should be consulted a fuller treatment of the considerations and the purpose definitions.

The following table summarises the classification of purposes defined in ISO/TS 14265.

Table: 12: ISO/TS 14265 Classification of Purposes

Purpose code	Classification	Description
1	Clinical care provision to an individual subject of care	To inform persons or processes responsible for providing healthcare services to the subject of care.
2	Emergency care provision to an individual subject of care	To inform persons who need to provide health care services to the subject of care urgently, possibly requiring consent and override policies distinct from those pertaining to purpose 1.

Purpose code	Classification	Description
3	Support of care activities within the provider organisation for an individual subject of care	To inform persons or processes that enable others to provide health care services to the subject of care, by coordinating activities and/or facilities.
4	Enabling the payment of care provision to an individual subject of care	To inform persons or processes responsible for enabling the availability of funds and/or permissions from a paying party for providing health care services to the subject of care.
5	Health service management and quality assurance	To inform persons or processes responsible for determining the availability, quality, safety, equity and cost-effectiveness of healthcare services.
6	Education	To support the learning and professional development of health care professionals.
7	Public health surveillance, disease control	To inform persons or processes that have responsibility to monitor populations or sub-populations for significant health events and then intervene to provide health care or preventive care services to relevant individuals.
8	Public safety emergency	To inform persons with responsibility for the protection of the public in a situation in which there is considered to be a significant risk to members of the public, possibly requiring consent and override policies distinct from those pertaining to purpose 7.
9	Population health management	To inform persons or processes that have responsibility to monitor populations or sub-populations for health events, trends or outcomes in order to inform relevant strategy and policy.
10	Research	To support the discovery of generalise-able knowledge.
11	Market studies	To support the discovery of product or organisation-specific knowledge.
12	Legal procedure	To inform persons or processes responsible for enforcing legislation, or undertaking legally authorised criminal, civil or regulatory investigation.
13	Subject of care uses	To inform the subject of care, or his or her legally authorised agent, in support of the subject of care's own interests or in the case of a deceased person in order to support the care of a family member.

Purpose code	Classification	Description
14	Unspecified	Disclosure on the basis of authorisations not requiring a purpose to be declared or purposes for which the other categories in this clause do not apply.

Health organisations should make their own assessments based on their local conditions.

Appendix E: Common threats to health information and associated vulnerabilities

The tables in this appendix summarise an example list of common threats to health information with respect to the following categories:

- Deliberate
- Environmental
- Accidental

Threats specific to the organisation should be assessed. Note that that where vulnerabilities may exist for a threat the appropriate control may be to address the vulnerability, either through people, process or technical controls.

Table 13: Threat Categories

Threat Category	Threat	Example Vulnerabilities	Example Potential Consequences
Deliberate	Denial of Service	• Lack of Perimeter Security mechanisms • Inadequate network management • Lack of OS update management, leading to exploitation • Lack of alerting and incident response processes	Loss of availability
	Eavesdropping	• Unencrypted communications over public networks • Lack of physical security over data communications equipment • Inappropriate network configuration, i.e. shared Ethernet broadcast traffic to any machine	Loss of confidentiality
	Fire	• Lack of physical security • Lack of fire detection devices • Lack of fire suppression devices	Loss of availability

Threat Category	Threat	Example Vulnerabilities	Example Potential Consequences
	Malicious Code	• Lack of anti-virus software • Lack of anti-virus software update processes • Inadequate staff awareness and education on virus issues • Lack of Security policy • Uncontrolled downloading and use of files off the Internet	Loss of integrity Loss of availability
	Malicious destruction of data and facilities	• Lack of physical security • Lack of logical access control leading to damage to / deletion of data • Lack of processes to ensure terminated employees accounts are disabled from system access	Loss of availability Loss of integrity
	Masquerade	• Lack of identification and authentication mechanisms • Unprotected passwords • Lack of identification of sender and receiver	Loss of confidentiality Loss of integrity
	Social Engineering	• Lack of security policy • Lack of awareness of staff allowing unauthorised people into QIC premises or giving information over the phone	Loss of integrity Loss of availability Loss of confidentiality
	Repudiation	• Lack of proof of sending or receiving a message • Lack of digital signatures	Loss of integrity
	Sabotage	• Lack of physical security • Lack of logical access controls • Lack of change management • Inappropriate access controls	Loss of integrity Loss of availability

Threat Category	Threat	Example Vulnerabilities	Example Potential Consequences
	Theft & Fraud	• Lack of physical security • Lack of application integrity controls • Lack of authentication • Lack of access controls • Lack of change management	Loss of integrity Loss of confidentiality
	Unauthorised Physical Access	• Lack of physical security controls • Poor awareness of 'shoulder surfing' risk • Lack of monitoring	Loss of integrity Loss of availability Loss of confidentiality
	Unauthorised Data Access	• Lack of logical access controls • Inability to authenticate requests for information • Transmission of unencrypted confidential data • Lack of physical security over communications equipment	Loss of integrity Loss of confidentiality
	Unauthorised Software changes	• Lack of change management policy and procedures • Lack of appropriate change control system • Inadequate segregation of duties between developer and operations staff • Inadequate reporting and handling of software malfunctions • Lack of backups	Loss of integrity Loss of availability

Threat Category	Threat	Example Vulnerabilities	Example Potential Consequences
	Website Intrusion	• Lack of Perimeter network defences • Inappropriate firewall rules / access controls • Lack of system hardening • Lack of processes to install OS and application security fixes • Inadequate software development standards	Loss of integrity Loss of availability
Environmental	Natural Disaster • Earthquake • Fire • Flood • Storm	• Location in an area susceptible to threat • Lack of back-up processes • Back-up media not available • Lack of BCP or procedures for recovery of data and IT • Lack of detection devices and monitoring • Lack of appropriate fire suppression mechanism	Loss of availability
	Environmental Conditions • Contamination • Electronic interference • Extremes of Temperature & humidity • Failure of Power Supply • Power Fluctuations	• Location in an area susceptible to threat • Lack of maintenance of equipment and facilities • Lack of detection devices and monitoring • Lack of back-up processes • Back-up media not available • Lack of BCP or procedures for recovery of data and IT • Lack of UPS • Lack of Power Conditioning equipment	Loss of availability

Threat Category	Threat	Example Vulnerabilities	Example Potential Consequences
Accidental	Fire	• Location in an area susceptible to fire • Inadequate physical access control to buildings • Lack of fire detection systems • Lack of fire suppression systems • Lack of BCP and DRP • Lack of backup	Loss of availability
	Failure of communications services	• Lack of redundancy and backup • Inadequate network management • Lack of planning and implementation of communications cabling • Inadequate incident handling • Lack of service levels with external communications providers	Loss of availability
	Failure of outsourced operations	• Unclear obligations in outsource agreements • Lack of BCP and DRP • Lack of backup	Loss of availability
	Loss or absence of key personnel	• No backup staff • Lack of cross-training • Undocumented procedures • Lack of succession planning	Loss of availability
	Misrouting / re-routing of messages	• Sensitive data not encrypted • Lack of verification of message receipt • Misconfigured networks	Loss of availability Loss of confidentiality Loss of integrity

Threat Category	Threat	Example Vulnerabilities	Example Potential Consequences
	User Error	• Lack of user awareness • Lack of user training • Lack of documentation • Lack of change management • Complicated user interface	Loss of availability Loss of integrity
	Software / Programming Error	• Inadequate system development lifecycle process and procedures • Unclear or incomplete system specification • Lack of change management • Lack of policy • Unskilled staff	Loss of availability Loss of confidentiality Loss of integrity
	Technical Failure	• Lack of Environmental controls • Lack of user awareness • Inadequate maintenance of hardware • Lack of backup facilities or processes • Lack of network capacity through improper planning or maintenance • Failure of change management processes • Lack of BCP or DRP	Loss of availability
	Transmission Error	• Inappropriate cabling • Inadequate incident handling • Lack of backup facilities or processes • Lack of BCP or DRP	Loss of availability

A number of other threat classification schemes are available that can be leveraged for risk assessment purposes, for example the STRIDE (**S**poofing identity, **T**ampering with data, **R**epudiation, **I**nformation disclosure, **D**enial of service and **E**levation of privilege) threat classification scheme provides a useful baseline list of six common threat categories that can be used for the basis of a risk assessment focussing on information security related risks.

Appendix F: Sample Gap assessment tool

Organisations could use this tool to assess the applicability of the NESAF controls, and their current compliance with these controls. This tool could also be used as the basis for a local tool that might incorporate additional considerations around assessment.

Table 14: Gap assessment tool

Access Control To control access to information.			Compliance
G.1.2	Organisations processing personal health information should have an access control policy governing access to this data. The organisation's policy on access control should be established on the basis of predefined roles with associated authorities which are consistent with, but limited to, the needs of that role. The access control policy, as a component of the information security policy framework described in A.1.1, should reflect professional, ethical, legal and subject-of-care-related requirements and should take account of the tasks performed by health professionals and the task's workflow.	Applicable	Met
G.2.1	Access to health information systems that process personal health information should be subject to a formal user registration process. User registration procedures shall ensure that the level of authentication required of claimed user identity is consistent with the levels of access that will become available to the user. User registration details shall be periodically reviewed to ensure that they are complete, accurate and that access is still required.	Applicable	Partially Met
Physical and environmental security To prevent unauthorised physical access, damage, and interference to the organisation's premises and information.			
E.1.2	Organisations processing personal health information should use security perimeters (e.g. walls, card entry gates or manned reception desks) to protect areas that contain information processing facilities supporting such health applications. These should be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	Applicable	Not Met

Appendix G: Sample Gap assessment scorecard

Based on the responses entered by an organisation in the gap assessment tool (refer to Appendix G:), the Gap assessment tool can generate a scorecard for the organisation in relation to each control category. An average compliance score for each control category is calculated based on the extent to which the organisation has indicated that it meets each applicable control (met = 100%; partially met = 50%; not met = 0%) within the category. The higher the compliance score, the lower the risk associated with the control category.

Table 15: Legend for compliance score

0	17	33	50	67	83	100
Needs Improvement	Below Average	Average			Above Average	Excellent

Table 16: Compliance scores

	Compliance Score (%)
Information Security Policy	73.33
Organising Information Security	52.35
Asset Management	40.67
Human Resources Security	54.00
Physical and environmental security	66.36
Vulnerability Management	57.50
Access Control	86.67
Acquisition, development and maintenance	60.00
Incident management	62.50
Business continuity	65.71
Compliance	62.56

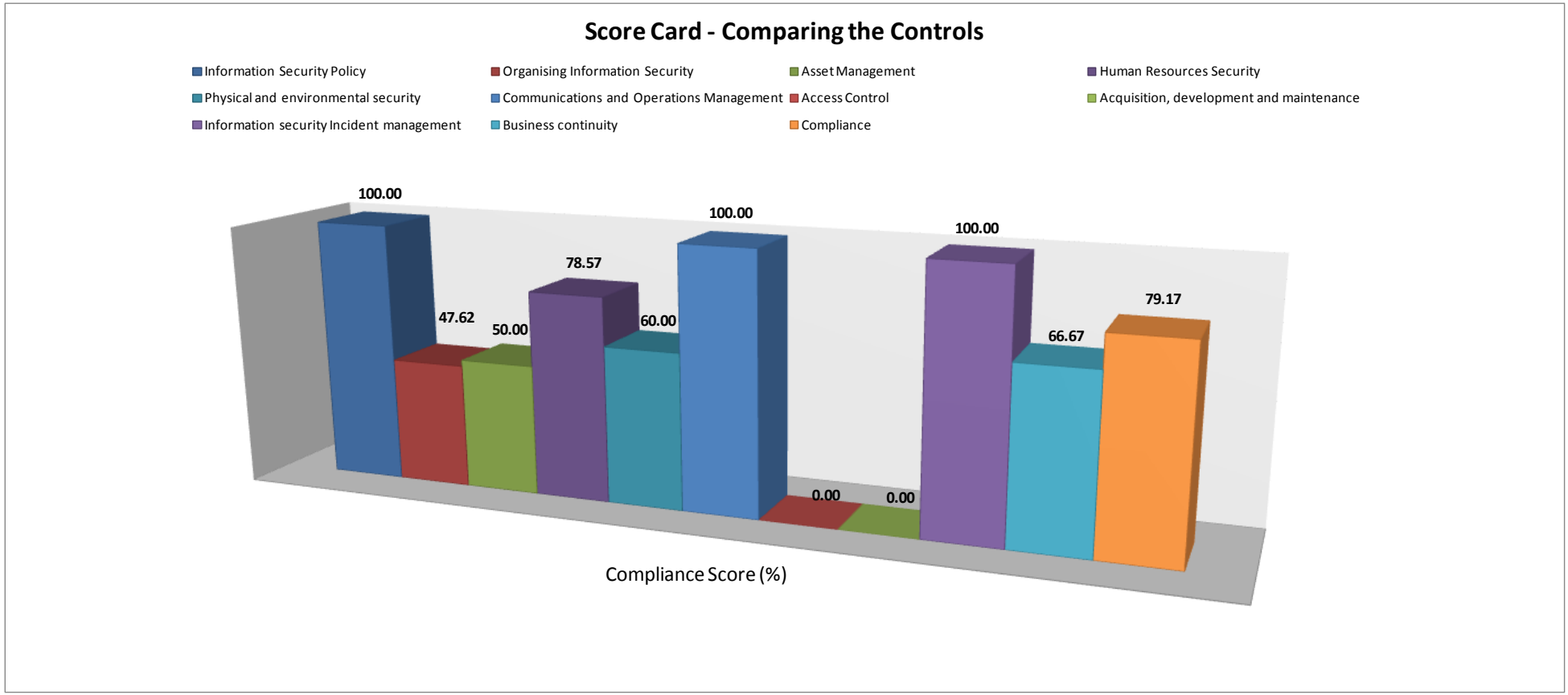


Figure 12: Compliance score card

A graphical compliance score card illustrates comparative scores across each of the NESAF control categories.

Appendix H: Risk assessment tools

Table 17: Table for determining impact severity

	Insignificant	Minor	Moderate	Major	Catastrophic
Risk to Individual safety	No injury/minimal risk to personal safety, no lost time.	Single injury/low risk to personal safety of client or employee, minimal impact on workload.	Multiple injuries/moderate risk to safety of client/employee, some workload pressure.	Death/disabling injury, high risk to safety of client/employee, high workload pressure.	Multiple deaths of disabling injuries/very high risk to safety of client/employee.
Distress caused to any party	None/negligible.	Minor distress.	Substantial short term distress.	Substantial long term distress.	Substantial long term distress to multiple parties.
Damage to any party's standing or reputation	Negligible, no public concern – attention from minor stakeholder with no publicity, only routine internal reporting.	Minor damage, visible dissatisfaction from public, limited/localised media interest, specific internal reporting.	Significant short term damage, public embarrassment of Provider, restricted negative publicity from local media, internal inquiry.	Mainstream media reports, new oversight required, persistent questions in Parliament, external inquiry e.g. Inquest.	Broad public concern, media event, senior resignations/removals, Parliamentary Inquiry or Royal Commission.
Legal Non-compliance, incl. Inappropriate release of legally protected data to third parties	Minor compliance issues. No or negligible impact. Offence punishable by small fine.	Short to medium term action required to achieve compliance. Minor impact. Offence punishable by moderate fine.	Immediate action needed to achieve compliance. Measureable impact. Offence punishable by major fine.	Shutdown of service for non-compliance. Significant impact. Offence punishable by imprisonment.	Shutdown of multiple services for non-compliance. Major consequences to a person, agency.

Threat to Provider, Provider partner, or third party systems, capacity to deliver Provider-related services	No or Negligible threat to, or disruption of, business or systems or service delivery.	Minimal threat to, or disruption of, localised business or systems or service delivery.	Moderate threat to or cessation of a service for a week, and subsequent disruption.	Multiple essential, critical services impaired or disrupted over several months.	Total business halted cessation of multiple essential/critical services for several months.

Table 18: Likelihood assessment table

[redacted]					
[redacted]	< 1%	1% – 10%	11% – 50%	51% – 99%	>= 99%
[redacted]	Conceivable but only in exceptional circumstances. Exceptionally unlikely even in the long-term future.	Has not happened yet, but could, or could occur after several years.	Could happen, has occurred before, or could occur within a year or so.	Could easily happen or could occur within weeks to months.	Happens often, or could occur within days to weeks.
[redacted]	No sharing	Sharing between trusted parties with a history of being trustworthy.	Sharing with new parties, but with effective protection in place (e.g. legalisation, audit trails, access controls etc.)	Sharing with new parties, but with limited to weak protections in place.	Public Access or sharing with parties that cannot be trusted.
[redacted]	Two or less	Small to Medium sized business (3–10 people).	Large business (e.g. hospital).	Multiple large businesses collaborating using shared records.	Multi-jurisdictional system (e.g. national or international).

Table 19: Matrix for determining risk levels

Likelihood (probability)	Potential Consequence (Impact)				
	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	High	High	Extreme	Extreme	Extreme
Likely	Medium	High	High	Extreme	Extreme
Possible	Low	Medium	High	Extreme	Extreme
Unlikely	Low	Low	Medium	High	Extreme
Rare	Low	Low	Medium	High	High

Source: AS/NZS 4360:1999 *Risk Management* [AS/NZS4360]

Table 20: Sample risk assessment tool

			Likelihood	Impact	Risk Level
1	Unauthorised data access	• Lack of logical access controls • Inability to authenticate requests for information • Transmission of unencrypted confidential data • Lack of physical security over communications equipment	Likely	Major	Extreme
2	Theft & Fraud	• Lack of physical security • Lack of application integrity controls • Lack of authentication • Lack of access controls • Lack of change management	Unlikely	Catastrophic	Extreme

Appendix I: Security Risk Action Plan template

	Risk Description	Level of Risk	Priority	Current Controls/ Treatments	Mitigation/ Controls and Measures	Responsibility	Timeframe	Resources	Mitigated Level of Risk
Risk ID	Brief outline of main components of the risk	Calculated risk level from risk assessment matrix	Priority assigned by organisation to the need to address this risk	List of current policy, process and technical controls	List new/additional controls required to manage the risk	Staff member(s) responsible for implementing the mitigation/control measure	Timeframe in which implementation of the control measure is to occur	Resources to be allocated to implementation of the control measure	Revised level of risk following implementation of control measure
1 (Example only)	Unauthorised change to Health information.	High	High	Access control services are managed by access control regimes.	Implement adequate logging of user activities. Ensure responsibilities are clearly defined. Implement acceptable and or complimentary access control services and constraints part of the Service. Conduct security education and awareness training.	IT Manager	By April 2012	Infrastructure team	Low