nehta

National eHealth Security & Access Framework (NESAF) v4.0

Business Blueprint v1.0

6 June 2014

Approved for external use

Document ID: NEHTA-1546:2014

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 information

Key information

Owner	Lead Security Architect	
Date of next review	2 June 2015	
Contact for enquiries	e:	help@nehta.gov.au

Product version history

NESAF version	Product version	Date	Release comments
2.0		20110729	Version 2.0 Approved for release
3.0		20111130	Version 3.0 Approved for release
3.1		20120330	Version 3.1 Approved for release
4.0	1.0	06 Jun 2014	See NESAF v4.0 release note for details

Table of contents

Table of figures

1 Introduction

1.1 Purpose

This document provides a good understanding of the NESAF methodology and appropriate tools to conduct a risk assessment to secure information.

1.2 Target audience

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.

This document is written in a style that should be suitable for 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 may also include interested government agencies and information security practitioners outside the health sector.

People unfamiliar with the NESAF should read the *NESAF v4.0 Overview* [1] first.

1.3 Document map

This document is a part of a suite of documents designed to provide specific views of the NESAF for different audiences, i.e. general, business, and technical, as illustrated below.

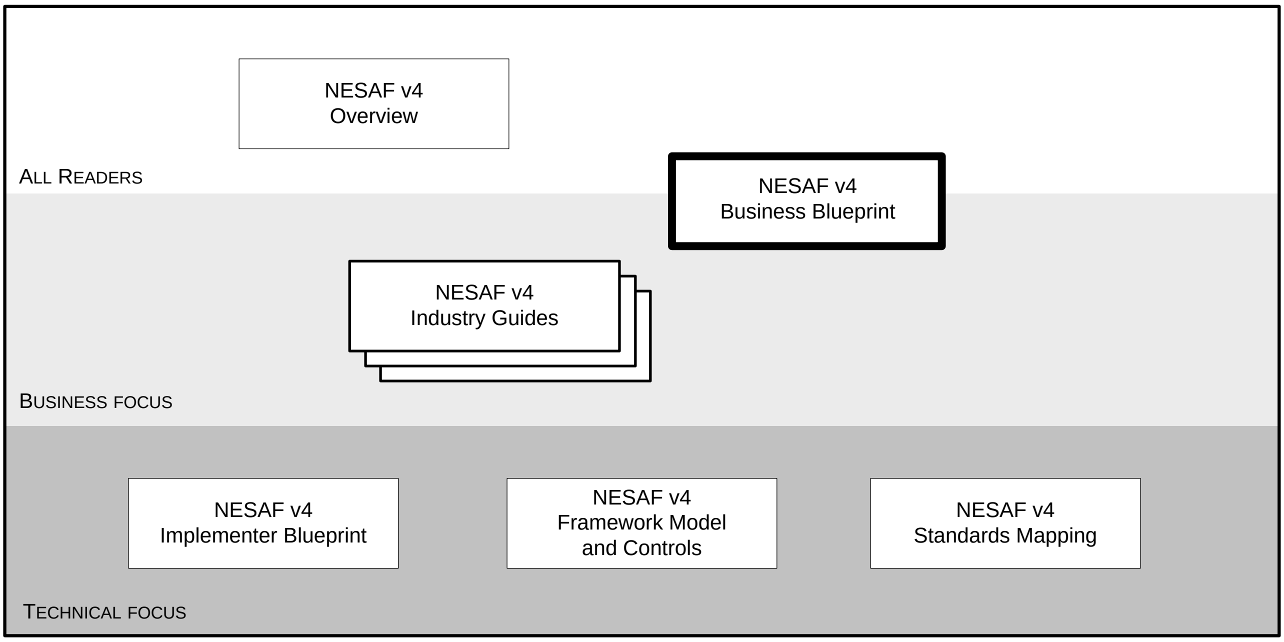


Figure 1: NESAF document framework

As this map would suggest, all readers with an interest in the NESAF should read both the *NESAF v4.0 Overview* [2] and the *NESAF v4.0 Business Blueprint* [3]. Once these two documents have been absorbed, readers should be well placed to judge which of the other NESAF documents are most relevant to their needs. See Section 2.1 for additional details.

1.4 Scope

The NESAF is applicable to all public and private sector healthcare provider organisations that have information or connectivity traceability to national systems.

1.5 Overview

This document describes the purpose, structure and benefits of the NESAF 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.

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, as well as 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, compromising adoption and uptake of eHealth and the expected benefits derived from investments in it. Being able to manage local security and access measures will be an important pre-requisite for a business to be able to work effectively in the national eHealth environment.

1.6 Background

In Australia we have enjoyed the benefits of a world class healthcare service that has ensured that most Australians have access to quality healthcare when it is needed. To meet increasing demand for healthcare the Australian Government is deploying 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 and more accurate 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 NESAF within healthcare organisations will assist in ensuring that this commitment is met.

A health organisation's management is legally responsible for the security of personal health information, even if the organisation relies upon managed services provided by third party organisations.

This business blueprint provides an understanding of the security responsibilities that are required within your organisation and any other health provider organisations you may connect to or communicate with.

Importance of assuring privacy within eHealth

The ability to move 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 of eHealth in Australia. Once a patient's health details have been exposed to an unauthorised third party, the damage cannot be undone.

Increasing exposure of personal healthcare information to a larger number of individuals, organisations and the internet means that proactive information security approaches are essential. High-quality information underpins the delivery of high-quality, evidence-based healthcare.

All organisations that supply or make use of eHealth information have an obligation to ensure that there is adequate provision for the security management of the information resources that they own, control or use.

1.7 Benefits

Value proposition of the NESAF	Healthcare organisations, with increasing reliance on interconnected electronic information systems need assistance to reduce the risks to patient data, provide privacy, and ensure integrity and availability of information.
For clinicians	Clinicians are able to trust the integrity and provenance of clinical information systems and be assured that the clinical data they need to provide patient care is available when they need it, secured and reliable.
For consumers	Consumers can trust that their personal health information is secure and that their confidentiality and privacy are maintained when interacting with eHealth and that only those that are involved in their care can access their personal health information.
For vendors	Improved security and access in clinical information systems offers improved product maturity and reduces ongoing development costs, patches and bug fixes.
For providers	Providers are able to meet legislative requirements, save implementation and ongoing development costs and ensure that data assets are protected.

1.8 Questions and feedback

The NESAF programme values your feedback about the NESAF and this document itself. Please direct your questions, comments and feedback to help@nehta.gov.au.

2 Structure of the NESAF

2.1 The NESAF document pyramid

The pyramid diagram below depicts the major themes and relationships of the NESAF, also noting the documents that address those themes. Introductory documents are closer to the apex, and the technical foundations are closer to the base. At the core of the NESAF is its risk-based approach, with the ultimate goal of creating systems that can be trusted by clinicians and users alike.

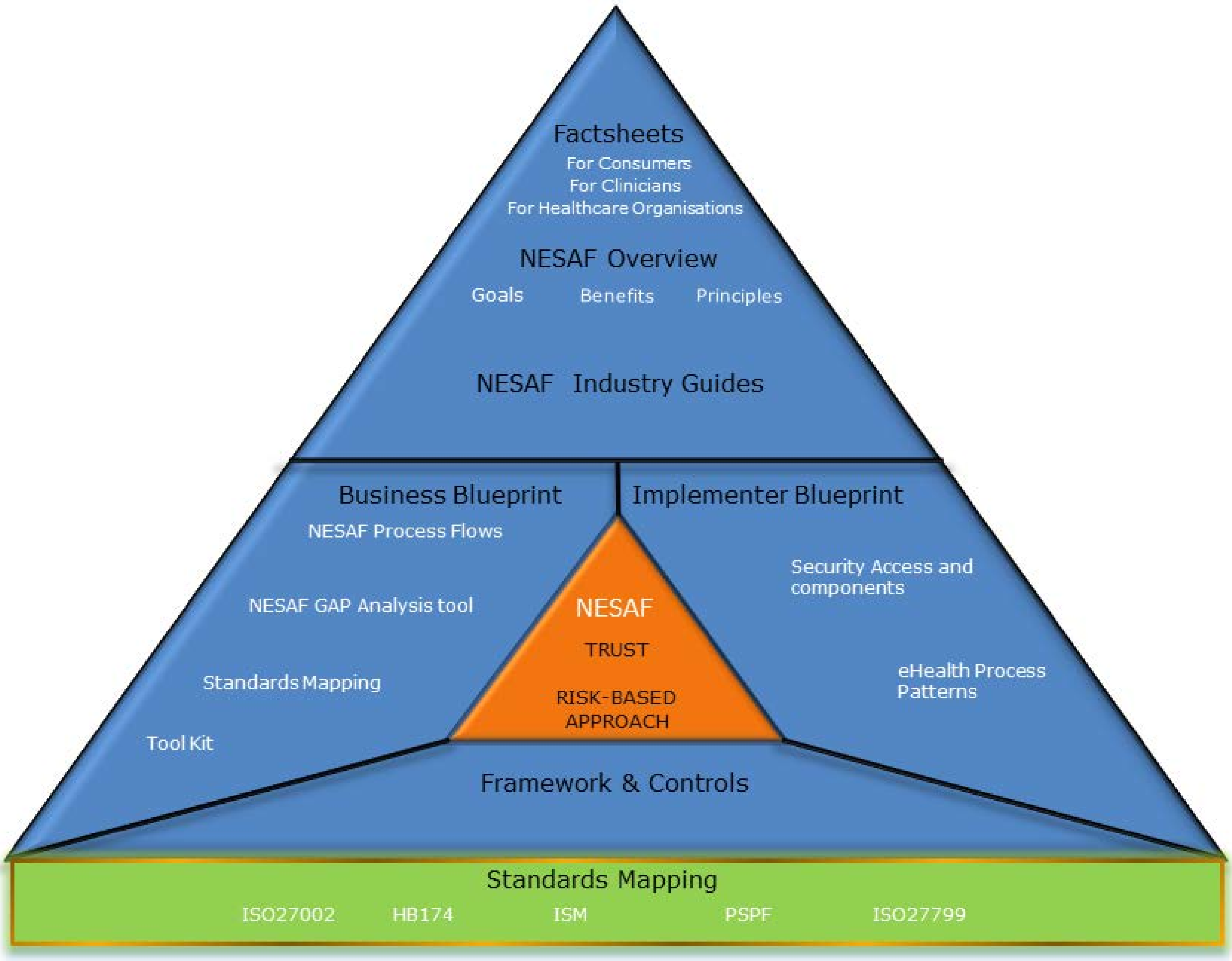


Figure 2: NESAF themes and documents

The following table elaborates on the documentation depicted above.

Table 1: NESAF documentation details

Document	Intended Audience	Description
NESAF v4.0 Consumer Factsheet [4]	General public	An introduction to the NESAF 4.0, targeted at the general public.
NESAF v4.0 Clinician Factsheet [5]	Clinicians	An introduction to the NESAF 4.0, targeted at clinicians.

Document	Intended Audience	Description
NESAF v4.0 Healthcare Organisation Factsheet [6]	Healthcare organisations	An introduction to the NESAF 4.0, targeted at healthcare organisations.
NESAF v4.0 Overview [2]	Business oriented document, suitable for the following: • Business executives • System owners • Healthcare organisation management teams	Provides a holistic view of the NESAF and its goals, benefits and principles.
NESAF Industry Guides (in development)	• Administrators • Clinicians • Health information managers • Implementers • Security Practitioners • Users	Security guidance for healthcare organisations, focussing on particular strategies or technologies.
NESAF v4.0 Business Blueprint [3] (this document)	• Business executives • System owners • Healthcare organisation management teams	This document aids the business to analyse the risk and identify appropriate security methods. Provides details of NESAF process flows and access to tool kits that can be utilised in implementing the NESAF.
NESAF v4.0 Implementer Blueprint [7]	Technically-oriented document aimed at ICT professionals.	Provides technical information on how ICT professionals can implement the NESAF. It introduces the eHealth process patterns and the security and access components to assist in the completion of a risk-based approach to information security.
NESAF v4.0 Framework Model and Controls [8]	ICT professionals	Describes a standards-based model and relevant industry standards, including ISO27799 and ISO27001. This document identifies 11 key security and access control areas. Within each area a range of controls are identified that businesses may select, based on the outcome of risk assessment processes to address the security and access requirements for their organisation.
NESAF v4.0 Standards Mapping [9]	• Business executives • ICT professionals	A suite of standards that have been referenced or mapped in the development of NESAF v4.0, which may provide useful references for readers seeking a deeper understanding of the areas covered within NESAF v4.0.

2.2 Standards-based framework model

The framework model is based on Australian Standards for information security management, and information security management in health (see Figure 3 below). It has been tailored to address the specific eHealth information security and access requirements.

The framework model identifies 11 key security and access control areas (for example, *G. Access Control*) relating to eHealth, each of which contains one or more control categories (for example, *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.

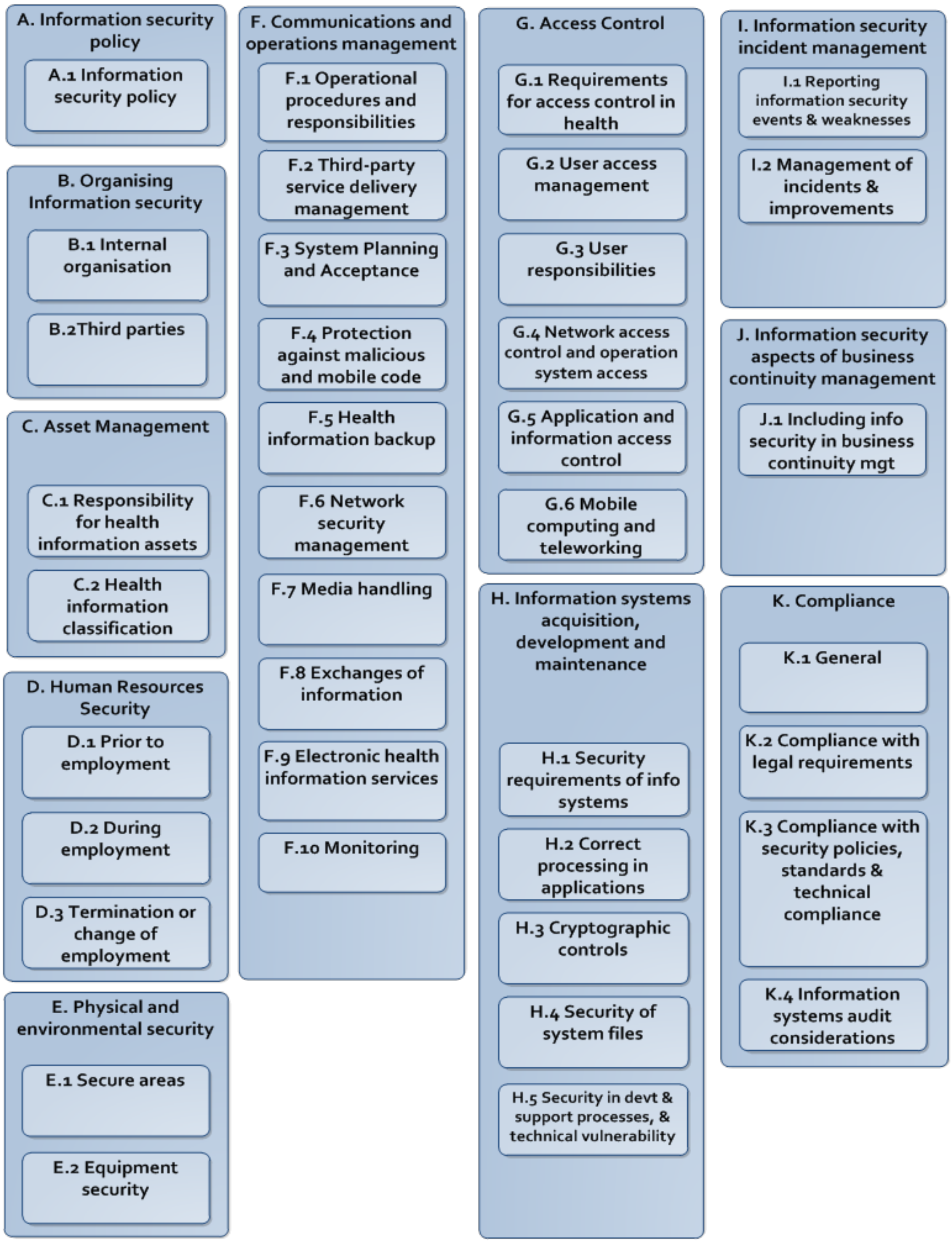


Figure 3: Standards-based framework model

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

A list of the control objectives and controls within the model is contained in *NESAF v4.0 Framework Model and Controls* [10].

2.3 Standards and frameworks map

The NESAF leverages content from recognised frameworks, particularly national standards by the Australian Government. Frameworks such as the *Protective Security Policy Framework* [11] and the *Information Security Manual* [12] and other legislation such as the *Privacy Act 1988 (Cth)* [13] and the *Australian Privacy Principles* [14][1] are supported.

Figure 4 provides an illustrative map of primary and secondary standards and other standards that are relevant to the NESAF.

There are three types of standards incorporated into the NESAF.

1. **Primary standards** – the NESAF is closely aligned to the elements and approach used in these standards.
2. **Secondary standards** – the NESAF's primary standards may reference these standards, or these standards may provide support to the broader security and access domain covered by the NESAF.
3. **Relevant frameworks** – these are relevant technical and policy documents, typically from governments in Australia and overseas.

Note: For further information please refer to *NESAF v4.0 Standards Mapping* [15].

[1] The *Australian Privacy Principles* [14] (APPs) commenced in March 2014, replacing the Information Privacy Principles that apply to Australian Government agencies and the National Privacy Principles that apply to businesses.

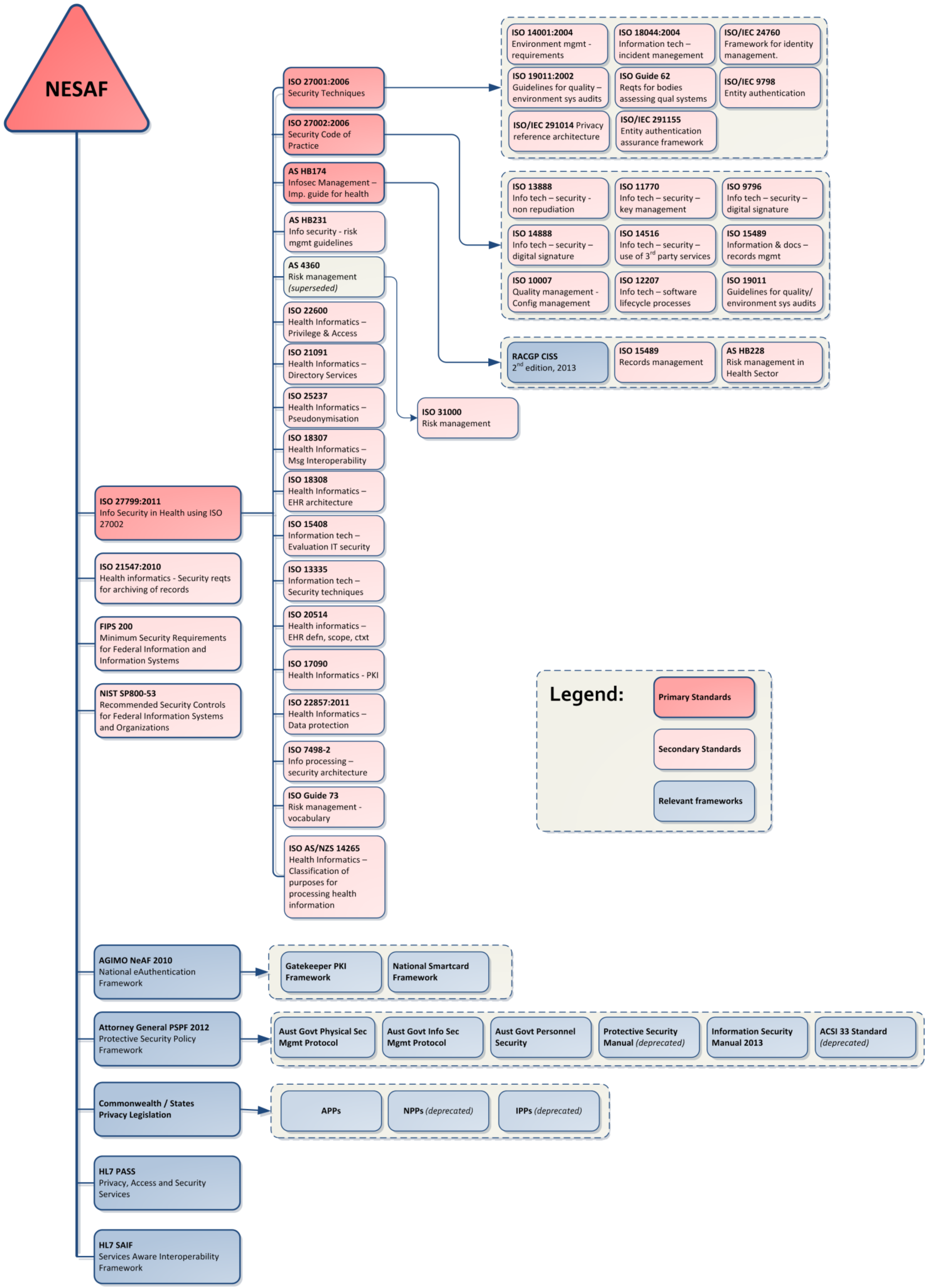


Figure 4: Standards and frameworks map

3 Risk-based approach

The NESAF uses a risk-based approach that organisations can use to identify risks to their operating environment and as well as the selection of appropriate security and access controls. The process assists businesses to identify appropriate controls – that may include policies, practices, procedures or software and 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. The manner in which a business/organisation interacts with eHealth systems will influence the options and potential actions it may take to align with the NESAF's principles and controls.

The following figure illustrates the NESAF's principles.

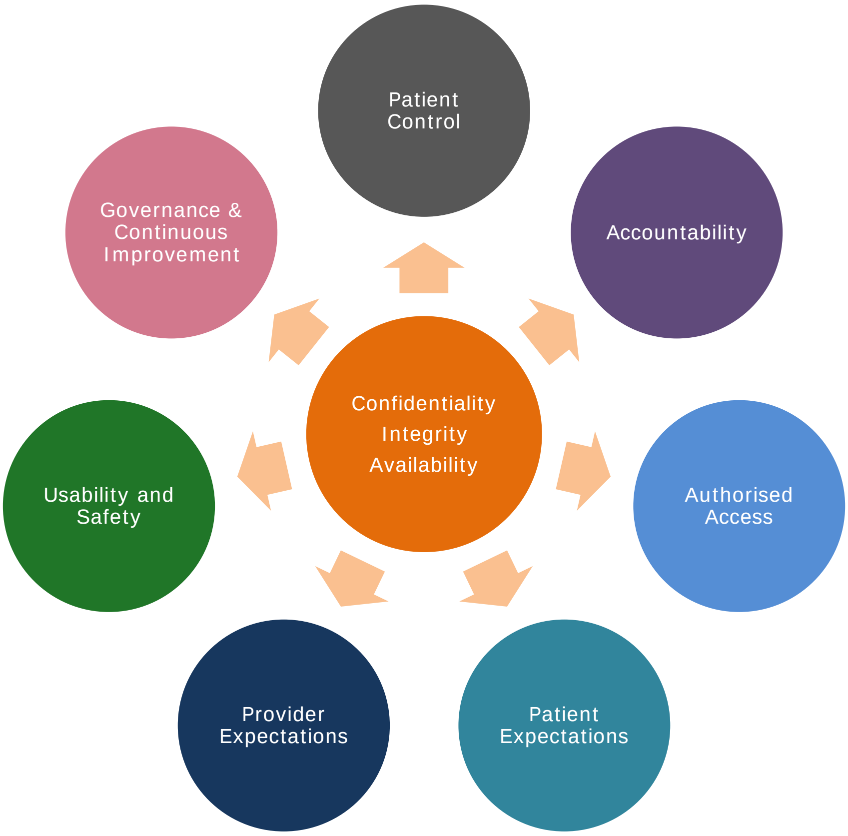


Figure 5: NESAF principles

Note: Refer to *NESAF v4.0 Overview* [1] for further details on the NESAF's principles.

The national eHealth environment comprises a range of organisations and services that will have differing levels of 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 – for example, hospitals, general practices, community health, and medical specialists.

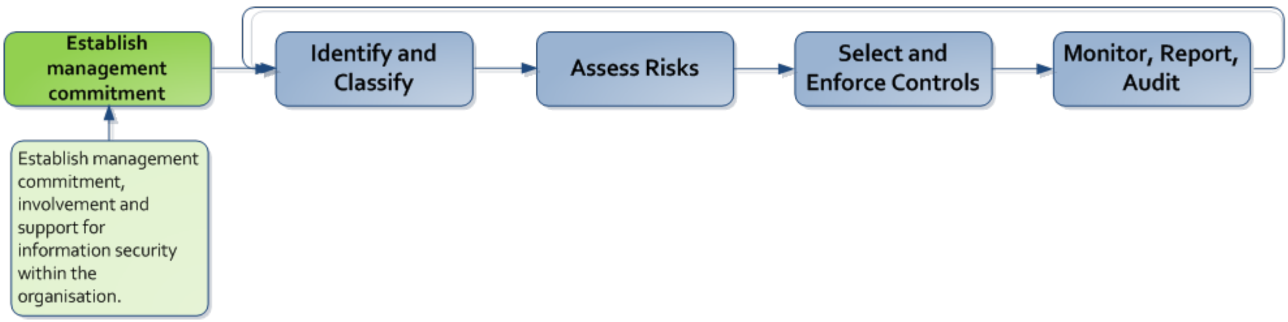
3.1 Implementation process steps

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

Figure 6: NESAF process flow

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

3.1.1 Establish management commitment



Security of health information 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. Information security can only be maintained over the long term if the organisation's management is explicitly committed.

Why is this important?

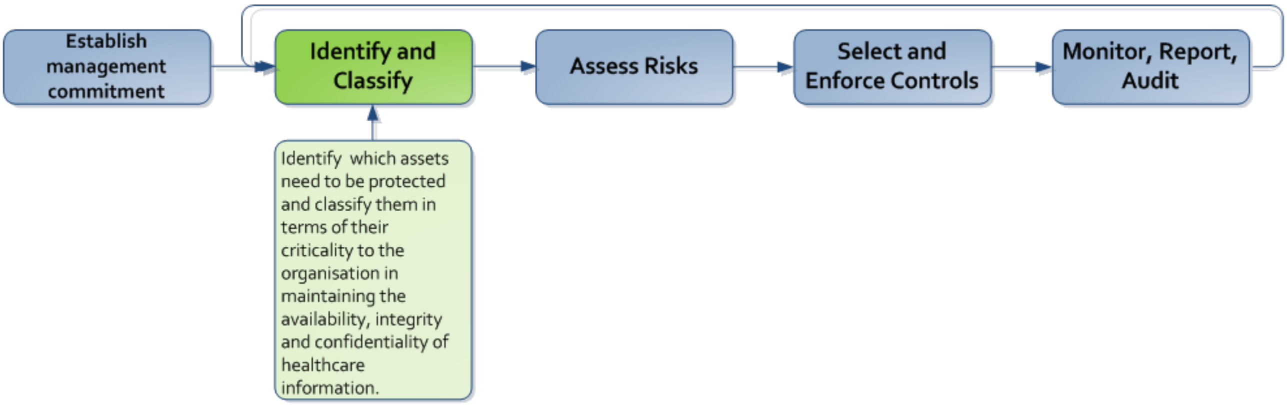
A health organisation's management is ultimately responsible for the security of personal health information, even if the organisation relies upon managed services provided by third-party organisations. Security is one of the key enablers for ensuring that a health organisation's privacy obligations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

The process of assessing information security risk, and selecting and enforcing appropriate controls may require financial investment. 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 signals the importance of information security within the organisation.

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

- 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 associated 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 with sufficient authority 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.

3.1.2 Identify and classify



At the heart of information security is a set of assets to be protected. Assets can include data (for example, patient healthcare information, personnel information), software (for example, medical software, operating systems), hardware (for example, laptops, mobile devices, network equipment), supporting services (for example, telecommunications services, cloud computing), and human assets (for example, 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 that 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.

3.1.2.1 Approaches to asset identification

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

Common healthcare information assets are identified in the figure below.

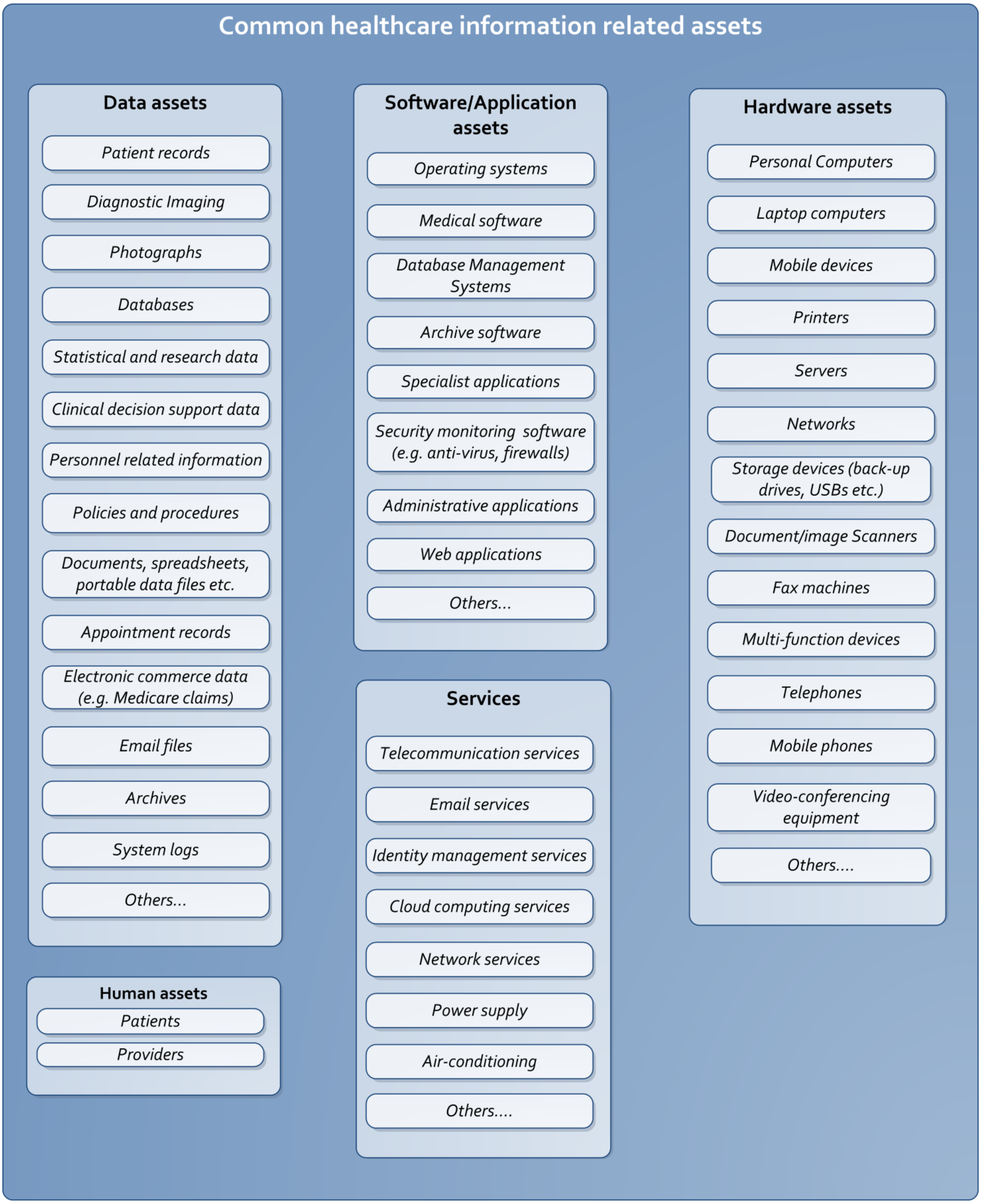


Figure 7: Common healthcare information related assets

Common healthcare information assets identified above 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 their 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.

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. The figure below shows the set of eHealth process patterns contained in the NESAF.

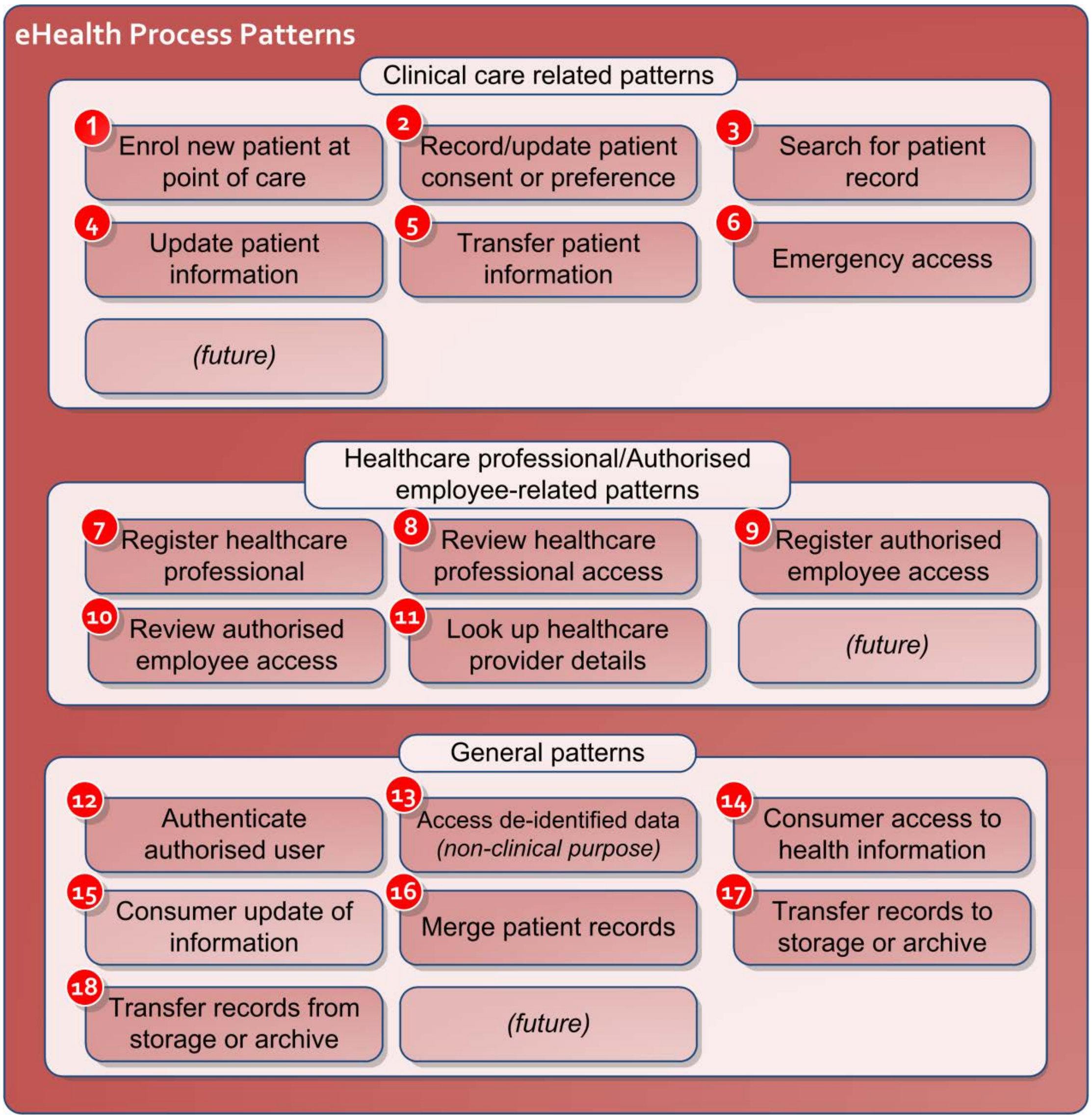


Figure 8: NESAF eHealth process patterns

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

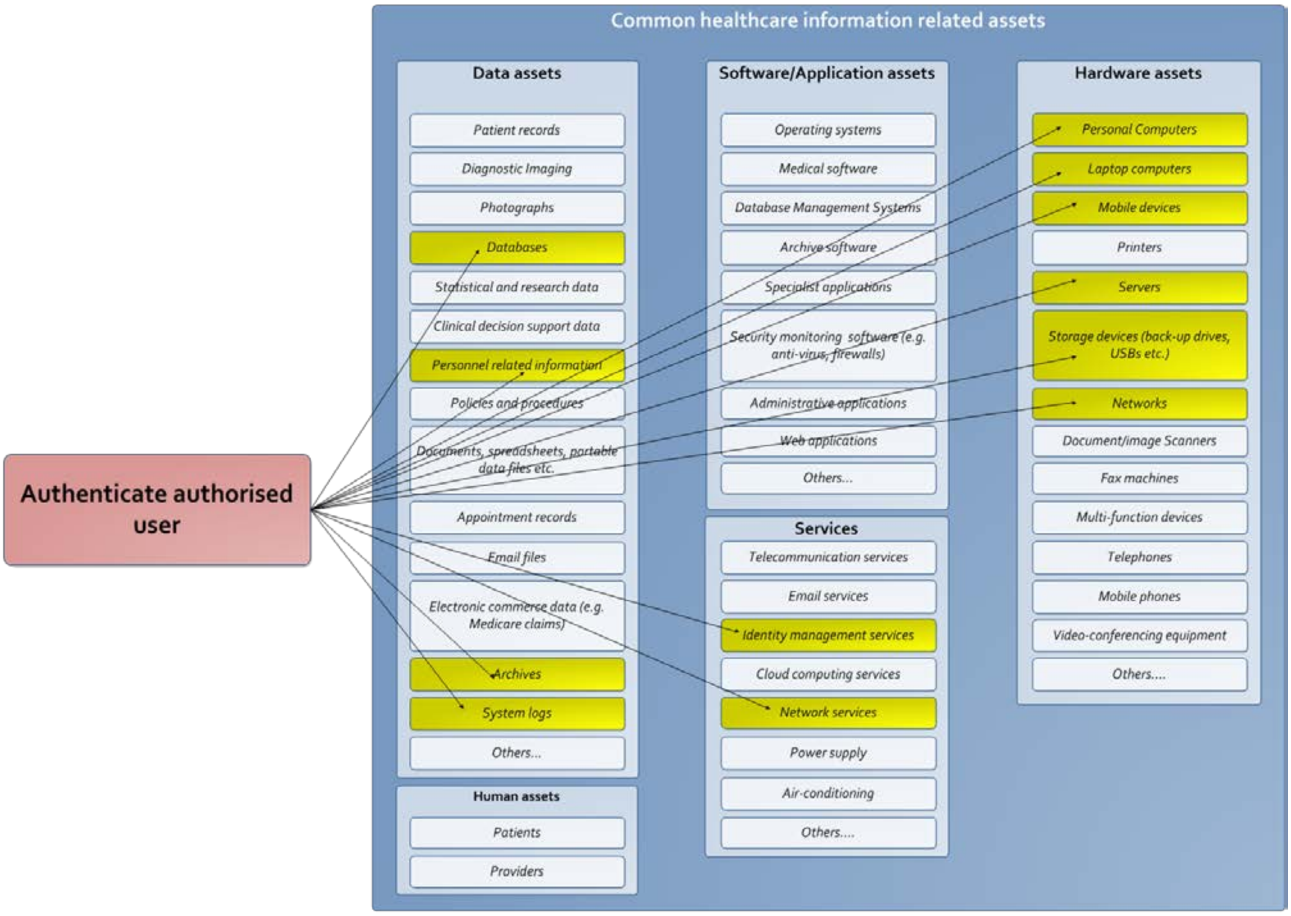


Figure 9: Example of using eHealth process patterns to identify related information assets

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 identified and appropriately protected.

3.1.2.2 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 identify the threats to them. 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 (for example, third party service providers).
- Information flows and interfaces.
- Security architecture:
  - o Technical, people and process controls in use.
  - o Network design.
  - o Physical and environmental security (for example, 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 (for example, existing and/or planned controls, applicability of relevant laws, regulation and policies) that is important in assessing risk.

3.1.2.3 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 to that asset or group that indicates the severity of the impact on the organisation should a loss of availability, integrity or confidentiality of that asset to occur. 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.

The NESAF provides an indicative data security classification scheme for guidance (refer to Section 4.3). This classification scheme has the following benefits:

- It provides 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.
- It 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.
- It enables resources to be focused on protecting the most sensitive information assets within the organisation.
- It 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, people, process or technology, to protect information based on its classification. Information should be handled and controlled appropriately based on its classification during every phase of its lifecycle, as depicted below.

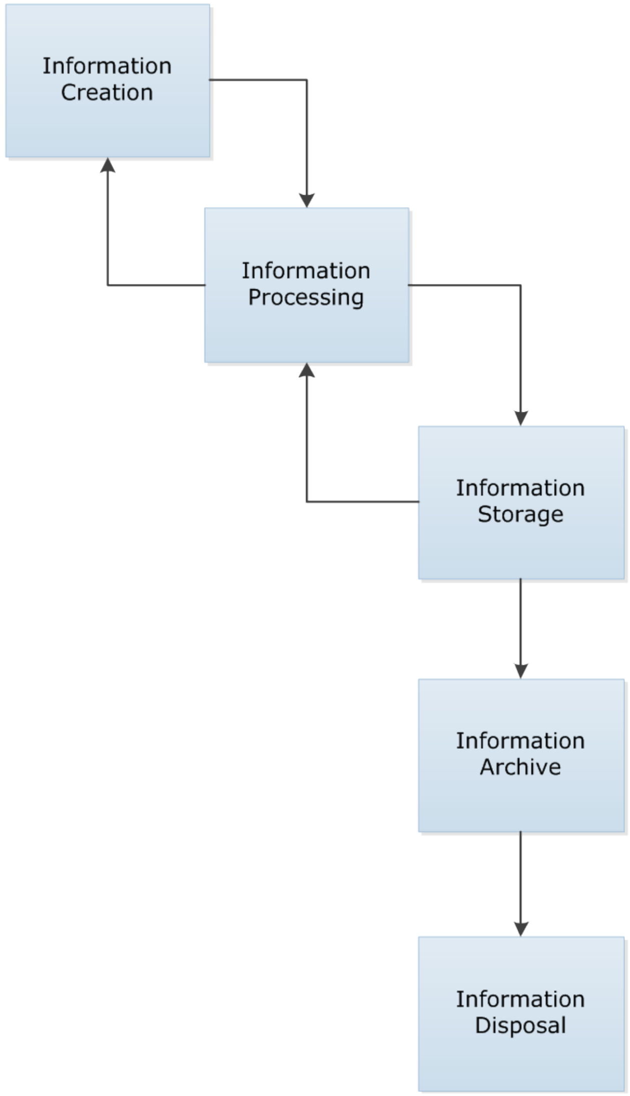
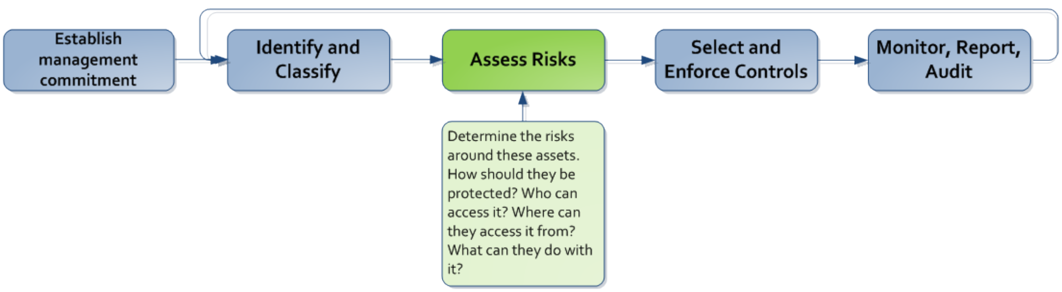


Figure 10: Information lifecycle

3.1.3 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 risks 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 or there is no applicable asset.

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 are 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 user's 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 the risk to an acceptable level for the organisation.

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 3.1.2.

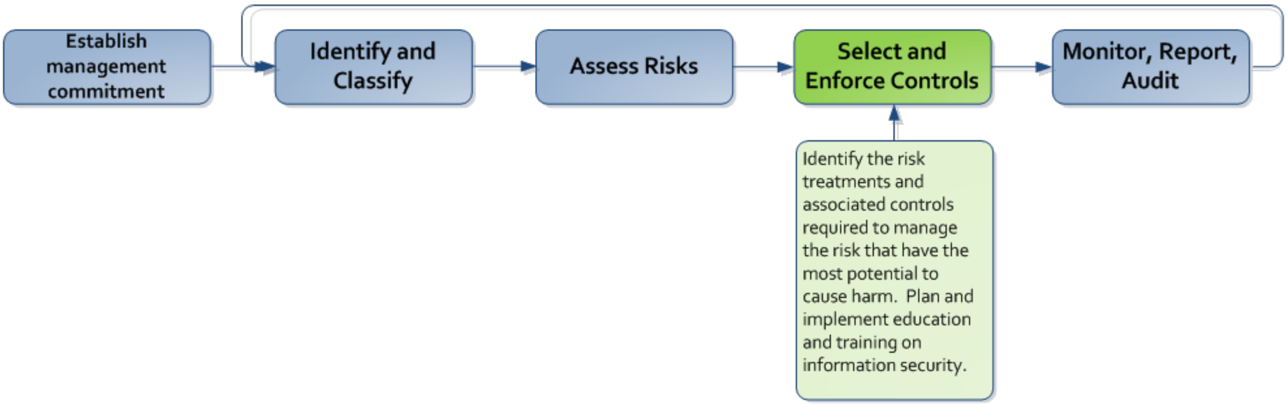
1 Threats should be identified and documented. Common threats to health information security are provided in the NESAF Risk Assessment tools (see Section 4.4). Additionally, organisations should consider any relevant threats that are specific to them. Look at the organisation's geographical location (floods, fire, burglaries, 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. (See Section 4.4.)

3 Assess current security controls in place in order to understand the likelihood that a potential vulnerability may be exploited.

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. (See Section 4.5.)

3.1.4 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, for example, 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, for example, 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 different types of organisations, as well as the volume of these exchanges.

Figure 10 illustrates the trade-off that organisations should consider in relation to selecting and implementing appropriate controls. The risk should be reduced until the cost of the control becomes disproportionate to its benefit. As we move from left to right deploying more mitigating controls the cost goes up while the risk goes down. 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.

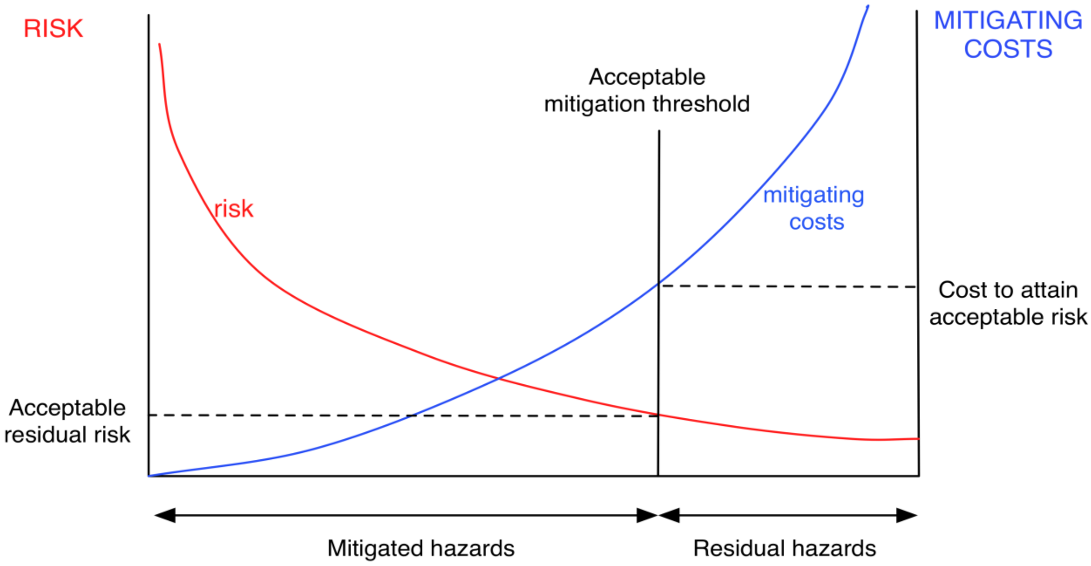


Figure 11: Cost-benefit trade-off: risk treatment options

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

3.1.4.1 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 Section 4.6.

3.1.4.2 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 who 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

- *NESAF v4.0 Framework Model and Controls* [10] contains information on NESAF Controls that may be useful to organisations in developing training and awareness information for staff.
- Section 4.6 contains a template for use in the development of an action plan.

3.1.5 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 (for example, 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 risks?

- 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.

4 NESAF tools

This chapter provides the following “tools” for organisations to use as a guide when implementing the NESAF:

- Elements of an information security and access policy (Section 4.1)
- Security and access role descriptions (Section 4.2)
- Asset Classification (Section 4.3)
- Common threats to health information and associated vulnerabilities (Section 4.4)
- Risk assessment tools (Section 4.5)
- Security Risk Action Plan template (Section 4.6)

4.1 Elements of an information security and access policy

Security policies provide management 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.

4.1.1 Guidance for developing an Information Security and Access policy

Policies should be:

- Consistent with the organisation's culture, strategy 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 (perhaps 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 the 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.

4.1.2 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 enable and manage 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.

4.1.3 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.

4.2 Security and access role descriptions

This section 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.

Table 2: Roles and responsibilities in information security management

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's 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.
Information Technology Security Manager	• Co-ordinates the strategic security direction provided by the Business Owner/directors. • Responsible for the day-to-day management of information security within the organisation. • In a small to medium organisation this role may be included in the IT manager's duties.

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.

4.3 Asset classification

Governments in Australia typically use security classification schemes with levels ranging from Public Information, Unclassified, X-in- Confidence (where X can be Commercial, Staff, Audit etc.), Protected and Highly Protected. These classifications enable the appropriate levels of protection to be applied to the data including who may access it.

A health organisation may use a classification along the lines of the example shown in the following table.

Table 3: Asset classification example

Data Asset	Classification
Individual patient healthcare information	Protected
Statistical & research data (de-identified)	Unclassified

Data Asset	Classification
Clinical decision support data	Public Information
Personnel related information	HR-In-Confidence
Commercial information	Commercial-In-Confidence

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

4.3.1 Information purpose

ISO/TS 14265:2011 [16] is a 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 14265:2011 [16] should be consulted for a fuller treatment of the considerations and the purpose definitions.

The following table summarises the classification of purposes defined in *ISO/TS 14265:2011* [16].

Table 4: 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.
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.

Purpose code	Classification	Description
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 (above).
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 generalisable 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.
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.

4.4 Common threats to health information and associated vulnerabilities

The tables in this section provide example summary lists of common threats to health information with respect to the following threat 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 5: 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, for example, shared Ethernet broadcast traffic to any machine	Loss of confidentiality
	Fire	• Lack of physical security • Lack of fire detection devices • Lack of fire suppression devices	Loss of availability
	Malicious Code	• Lack of anti-virus software • Lack of anti-virus software update processes • Inadequate staff awareness and education on virus issues • Lack of security policy • Uncontrolled downloading and use of files off the Internet	• Loss of integrity • Loss of availability
	Malicious destruction of data and facilities	• Lack of physical security • Lack of logical access control leading to damage to/deletion of data • Lack of processes to ensure terminated employees' accounts are disabled from system access	• Loss of availability • Loss of integrity
	Masquerading	• Lack of identification and authentication mechanisms • Unprotected passwords • Lack of identification of sender and receiver	• Loss of confidentiality • Loss of integrity

Threat Category	Threat	Example Vulnerabilities	Example Potential Consequences
	Social engineering	• Lack of security policy • Lack of awareness of staff allowing unauthorised people into the organisation's 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
	Theft and 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 • Privacy breach
	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 business continuity plan and disaster recovery plan 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 business continuity plan or procedures for recovery of data and IT • Lack of uninterruptable power supply • Lack of power conditioning equipment	Loss of availability
Accidental	Fire	• Location in an area susceptible to fire • Inadequate physical access control to buildings • Lack of fire detection systems • Lack of fire suppression systems • Lack of business continuity plan and disaster recovery plan • Lack of backup	Loss of availability

Threat Category	Threat	Example Vulnerabilities	Example Potential Consequences
	Failure of communications services	• Lack of redundancy and backup • Inadequate network management • Lack of planning and implementation of communications cabling • Inadequate incident handling • Lack of service levels with external communications providers	Loss of availability
	Failure of outsourced operations	• Unclear obligations in outsource agreements • Lack of business continuity plan and disaster recovery plan • 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
	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

Threat Category	Threat	Example Vulnerabilities	Example Potential Consequences
	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 business continuity plan or disaster recovery plan	Loss of availability
	Transmission error	• Inappropriate cabling • Inadequate incident handling • Lack of backup facilities or processes • Lack of business continuity plan or disaster recovery plan	Loss of availability

A number of other threat classification schemes are available that can be used 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.

Here is a list of possible threats taken from *AS ISO 27799-2011* [17]:

1 Masquerade by insiders (including masquerade by health professionals and support staff)

Masquerade by insiders consists of system use by those who make use of accounts that are not their own. As such, it constitutes a breakdown in secure user authentication. Many cases of masquerade by insiders are committed simply because it makes it easier for people to do their work. For example, when one health professional may replace another at a workstation and continues to work on an already active subject of care record, there is a strong temptation to skip the inconvenience of the first user logging out and the second user logging in. Nevertheless, masquerade by insiders is also the source of serious breaches in confidentiality. Indeed, the majority of breaches of confidentiality are committed by organisational insiders. Masquerade by insiders can also be carried out with the intention of covering up cases where harm has been caused.

2 Masquerade by service providers (including contracted maintenance personnel such as system software engineers, hardware repair personnel and others who may have a pro forma legitimate reason to access systems and data)

Masquerade by service providers consists of contracted personnel using their privileged access to systems (such as during on-site testing and repair of malfunctioning equipment) to gain unauthorised access to data. As such, it is a breach of – or failure to properly provide for – secure outsourcing arrangements. Though rarer than masquerade by insiders, masquerade by service providers can also be the source of serious breaches in personal health information confidentiality.

3 Masquerade by outsiders (including hackers)

Masquerade by outsiders occurs when unauthorised third parties gain access to system data or resources, either by impersonating an authorised user or by fraudulently becoming an authorised user (for example through so-called "social engineering"). In addition to hackers, masquerade by outsiders is also committed by journalists, private investigators and "hacktivists" (hackers who work on behalf of, or in sympathy with, political pressure groups). Masquerade by outsiders constitutes a failure of one or more of the following security controls:

- user identification;
- user authentication;
- origin authentication; and
- access control and privilege management.

4 Unauthorised use of a health information application

It can be surprisingly easy to obtain unauthorised access to a health information application (for example by a subject of care walking up to an unattended workstation in a physician care office and browsing the screen). Authorised users can also perform unauthorised actions such as maliciously altering data. In the UK, Dr. Harold Shipman attempted to hide the notorious murder of scores of his patients by altering records on his computer system.

The critical importance of correctly identifying subjects of care and correctly matching them to their health records leads health organisations to collect detailed identifying information on patients treated. This identifying information is of great potential value to those who would use it to commit identity theft and so must be rigorously protected.

In general, unauthorised use of health information applications constitutes a failure of one or more of the following:

- workgroup access control (for example, by allowing a user to access the records of subjects of care with whom the user has no legitimate relationship);
- accountability and audit control (for example, by allowing inappropriate user actions to go unnoticed); and
- personnel security (for example, by providing inadequate training to users or not making clear that their access to records is subject to audit and review).

5 Introduction of damaging or disruptive software (including viruses, worms and other "malware")

Most IT security incidents involve computer viruses. Introduction of damaging or disruptive software constitutes a failure in anti-virus protection or in software change control. While typically within the remit of network system operators, the proliferation of email worms and viruses as well as exploitation by hackers of weaknesses in server software have combined to greatly complicate measures taken to prevent the introduction of damaging or disruptive software.

6 Misuse of system resources

This threat includes users using health information systems and services for personal work, users downloading non-work-related information from the Internet on to computers intended solely to support health information systems, users setting up databases or other applications for non-work-related matters, or users degrading the availability of health information systems by, for example, using network bandwidth to download streaming video or audio for personal use. Such misuse constitutes a failure to enforce acceptable use agreements or to educate users about the importance of maintaining the integrity and availability of health information resources.

7 Communications infiltration

Communications infiltration of electronic communications occurs when an individual (a hacker, for example) tampers with the normal flow of data across a network. The most common result is a denial-of-service attack (in which servers or network resources are effectively taken off-line), but other forms of communication infiltration are possible (such as a replay attack, in which a valid but out-of-date message is retransmitted in a way that makes it appear current). Communications infiltration constitutes a failure of intrusion detection and/or network access controls and/or risk analysis (specifically vulnerability analysis) and/or system architecture (which needs to be designed with defence against denial-of-service attacks).

8 Communications interception

If not encrypted during transmission, the confidentiality of information contained in a message can be breached by intercepting the communication. This is simpler than it sounds, as anyone on a local area network can potentially install a so-called “packet sniffer” on their workstation and monitor much of their local area network traffic, including reading e-mails during transmission. Hacker tools are readily available to automate and simplify much of this process. Communications interception constitutes a failure in secure communications.

9 Repudiation

This threat includes users denying that they sent a message (repudiation of origin) and users denying that they received a message (repudiation of receipt). Establishing unambiguously whether personal health information flowed from one health provider to another can be an essential feature of investigations into medical malpractice. Repudiation can constitute a failure to apply controls such as digital signatures on e-prescriptions (an example of repudiation of origin) or controls such as read receipts on email messages (an example of repudiation of receipt).

10 Connection failure (including failures of health information networks)

All networks are subject to periodic service outages. Quality of service is a major factor in the provisioning of network services in healthcare. Connection failure can also result from misdirection of network services (for example malicious alteration of routing tables that cause network traffic to be diverted). Connection failures can facilitate the disclosure of confidential information by forcing users to send messages by a less secure mechanism, such as via facsimile or over the Internet.

11 Embedding of malicious code

This threat includes e-mail viruses and hostile mobile code. While in no way unique to health information systems, the increasing use of wireless and mobile technologies by healthcare providers increases this threat's potential for damage. Embedding of malicious code constitutes a failure to apply anti-virus software controls or intrusion prevention controls effectively.

12 Accidental misrouting

This threat includes the possibility that information might be delivered to an incorrect address when it is being sent over a network. Accidental misrouting could constitute a failure in user education or a failure to maintain the integrity of directories of health providers (or both).

13 Technical failure of the host, storage facility or network infrastructure

These threats include hardware failures, network failures or failures in data storage facilities. Such failures typically constitute a failure of one or more of the operations management controls listed in Clause 10 of *ISO/IEC 27002:2005* [18]. While in no way unique to health information systems, the loss of availability of such systems can have life-threatening consequences for patients.

14 Environmental support failure (including power failures and disruptions of service arising from natural or man-made disasters)

Health information systems can be critical during natural disasters and other events that can be life threatening to large numbers of people. These same disasters can wreak havoc on the environmental support systems needed to maintain operations. A proper threat and risk assessment of health information will include an assessment of how critical such systems are in times of natural disaster and how robust their operations will be under such disaster scenarios.

15 System or network software failure

Denial-of-service attacks are greatly facilitated by weaknesses in, or misconfiguration of, operating system or network operating system software. System or network software failure constitutes a failure in software integrity checking, system testing or software maintenance controls.

16 Application software failure (for example, of a health information application)

Failures in application software can be exploited in a denial-of-service attack and can also be used to compromise the confidentiality of protected data. Application software failure constitutes a failure in software testing, software change controls, or software integrity checking.

17 Operator error

Operator error accounts for a small but significant percentage of unintentional disclosures of confidential information and a large proportion of unintentional dispositions of data. Operator error constitutes a failure in one or more of the following:

- operations controls;
- personnel security (including effective training); and
- disaster recovery (including data backup and restoration).

18 Maintenance error

Maintenance errors are mistakes by those responsible for maintaining systems hardware and software. Maintenance errors can be committed by staff members as well as by third-party employees contracted to perform maintenance duties. Such errors can, in turn, endanger the confidentiality of protected data. Misconfiguration of software during installation is a common cause of vulnerabilities later exploited by hackers. Maintenance errors constitute a failure in hardware maintenance controls, software maintenance controls, software change controls or some combination of the above.

19 User error

Error by users can, for example, result in confidential information being sent to the wrong recipient. User errors can sometimes constitute a failure in:

- user controls (including user interfaces designed with security in mind); or
- personnel security (including training).

20 Staff shortage

The threat of staff shortage includes the possibility of the absence of key personnel and the difficulty of replacing them. Vulnerability to this threat depends on the extent to which shortage of staff would affect the business processes. In healthcare, an epidemic that greatly increases the demand for timely access to health information may also create a staff shortage that jeopardises the availability of such systems. A failure of this kind constitutes a failure in business continuity management (see Clause 14 of *ISO/IEC 27002:2005* [18]).

21 Theft by insiders (including theft of equipment or data)

Insiders typically have greater access to confidential information than outsiders and are therefore in a favourable position to steal the information in order to sell it or to disclose it to others. While comparatively rare, the threat of theft of personal health information by insiders increases with the fame or notoriety of the data subject (for example, a celebrity or head of state) and decreases with the potential severity of punitive consequences (for example, the loss by a physician of their licence to practice). Theft by insiders constitutes a failure of one of many possible controls, including controls on hardcopy output, documents or media, physical security, or physical protection of equipment.

22 Theft by outsiders (including theft of equipment or data)

Theft by outsiders of data and equipment is a serious problem in some hospitals. Theft may result in breaches of confidentiality, either because confidential data resides on a server or laptop computer that is stolen or else because the data itself is the target of the theft. Theft by outsiders may constitute a failure in one of many controls, including mobile computing controls, secure media transport, incident handling, compliance checks or physical theft protection.

23 Wilful damage by insiders

Wilful damage by insiders includes acts of vandalism and other cases where physical damage is caused to IT systems or their supporting environment by people who have been granted access. The users of health information systems are typically dedicated health professionals and wilful damage is rare. Wilful damage by insiders constitutes a failure of human resources security (see Clause 8 of *ISO/IEC 27002:2005* [18]).

24 Wilful damage by outsiders

The threat of wilful damage by outsiders includes acts of vandalism and other cases where physical damage is caused to IT systems or their supporting environment by people who have not been granted access to such systems. While in most industrial sectors, acts of this kind constitute a failure to effectively apply physical security controls, access by subjects of care and their friends and relatives to operational areas of hospitals, clinics and other health organisations make such threats much more difficult to prevent than in most other operational environments. The security controls in Clause 9 of *ISO/IEC 27002:2005* [18] need to be carefully selected and applied to minimize such threats.

25 Terrorism

The threat of terrorism includes acts by extremist groups wishing to damage or disrupt the work of health organisations or to harm healthcare providers or to disrupt the operations of health information systems. While no such large-scale attacks have occurred yet, planners need to consider the threat of terrorism, especially when large-scale health information systems are designed, since an attack on such systems could increase the effectiveness of bioterrorist and other attacks that cause a health-related crisis.

4.5 Risk assessment tools

Table 6: Table for determining impact severity

Impact	**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.

Impact	Impact Severity				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
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 (such as 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 7: Likelihood assessment table

Likelihood type	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Description	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.
Sharing	No sharing	Sharing between trusted parties with a history	Sharing with new parties, but with effective	Sharing with new parties, but with limited to weak	Public access or sharing with parties that cannot be

		of being trustworthy.	protection in place (such as legalisation, audit trails, access controls etc.)	protections in place.	trusted.
Number of people with access	Two or less	Small to medium sized business (3–10 people).	Large business (such as hospital).	Multiple large businesses collaborating using shared records.	Multi-jurisdictional system (such as national or international).

Table 8: Matrix for determining risk levels

Likelihood (probability)	**Potential Consequence (Impact)**				
	Insignificant	**Low**	**Medium**	**High**	**Very High**
Almost Certain	Medium	High	High	Extreme	Extreme
Likely	Medium	Medium	High	High	Extreme
Possible	Low	Low	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Medium	High

Table 9: Sample risk assessment tool

Risk ID	**Threat**	**Vulnerabilities**	**Risk Level**		
			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

4.6 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 complementary access control services and constraints as part of the Service. Conduct security education and awareness training.	IT Manager	By <date>	Infrastructure team	Low

Acronyms

Acronym	Description
AGIMO	Australian Government Information Management Office
AHPRA	Australian Health Practitioners Registration Authority
CCA	NEHTA's Compliance, Conformation and Accreditation programme
CCOW	Clinical Context Object Workgroup (HL7 standard)
DSML	Directory Services Mark-up Language
GBAC	Governance Based Access Control
GSEF	Gold Standard Enrolment Framework
HPI-I	Healthcare Provider Identifier Individual
HPI-O	Healthcare Provider Identifier Organisation
ICT	Information and Communications Technology
IMAGE	Identity Management for Australian Government Employees
IRAL	Identity Registration Authority Level
ISMF	Information Security Management Forum
ISMS	Information Security Management System
LAN	Line Area Network
MAC	Mandatory Access Control
NASH	National Authentication Service for Health
NeAF	National e-Authentication Framework
NEHTA	National E-Health Transition Authority
NESAF	National E-Health Security and Access Framework
OTP	One time password
PAS	Platform as a service
PHI	Protected Health Information
PKI	Public Key Infrastructure
SAML	Security Assertion Markup Language
SEHR	Shared Electronic Health Record
SOE	Standard Operating Environment
SPML	Service Provisioning Markup Language
TLS	Transport Layer Security
VOIP	Voice Over IP
VPN	Virtual Private Network

Acronym	Description
WAN	Wide Area Network
XACML	XML Access Control Language

Glossary

Term	Definition
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. *AS ISO 27799-2011* [17].
Authentication	Means that one can verify whether the sender is who they say they are. *RACGP security standards and templates* [19]
Authorised Employee	An authorised employee is an individual that will act on behalf of the healthcare organisation and may be associated with different types of roles within the healthcare organisation, inclusive of healthcare providers and administrative staff who have a legitimate role in accessing systems containing healthcare information.
Availability	Refers to the property of being accessing and usable on demand by an authorised entity. *AS ISO 27799-2011* [17]
Clinical Safety	Clinical safety is concerned with identification and reduction of harm to patients to acceptable levels.
Confidentiality	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/IEC 27002:2005* [18]
De-identified	A record that cannot be linked to an individual.
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. *RACGP security standards and templates* [19]
Health information system	Repository of information regarding the health of a subject of care in computer-process-able form, stored and transmitted securely, and accessible by multiple authorised users. *AS ISO 27799-2011* [17]
Health professional Healthcare professional	A person who is authorised by a recognised body to be qualified to perform certain health duties. *AS ISO 27799-2011* [17]
Healthcare	Any type of service provided by professionals or paraprofessionals with an impact on health status. *AS ISO 27799-2011* [17]
Healthcare Identifier Service.	The Healthcare Identifier Service assigns a unique national Healthcare Identifier to each healthcare recipient and healthcare provider to establish and maintain accurate records to support the communication and management of

Term	Definition
	health information.
Healthcare organisation	Generic term used to describe many types of organisations that provide healthcare services. *AS ISO 27799-2011* [17]
Healthcare provider	A person who is involved in or associated with healthcare delivery. A synonym for clinician and healthcare professional.
Healthcare Provider Identifier Individual (HPI-I)	A Healthcare Provider Identifier Individual (HPI-I) is a national unique 16-digit identifying number assigned to health practitioners who provide healthcare services to the general public.
Healthcare Provider Identifier Organisation (HPI-O)	A Healthcare Provider Identifier Organisation (HPI-O) is a national unique 16-digit identifying number assigned to organisations involved in delivering healthcare services.
Information security	Preservation of confidentiality, integrity and availability of information.
Integrity	Refers to the property that data has when it has not been altered or destroyed, or a system has when it can perform its intended function in an unimpaired manner, free from deliberate or accidental unauthorised manipulation of the system. *AS ISO 27799-2011* [17]
Jailbreaking	Process that allows a user to install software not authorised or approved by a mobile device manufacturer.
Malicious code	Programs such as viruses and worms designed to exploit weaknesses in computer software and replicate and/or attach themselves to other software programs on a computer or a network.
Personal health information	Information about an identifiable person which relates to the physical or mental health of the individual or to provision of health services to the individual. *AS ISO 27799-2011* [17]
Personnel	People accessing health data through means owned or provided by the organisation. Includes, staff, contractors, consultants, visiting medical officers etc.
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. Can be thought of as an electronic “chain of custody”.
Public Key Infrastructure (PKI)	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.
Relying Party	An entity that relies upon an authentication credential .
Risk	The probability that a given threat will exploit a given vulnerability. *HB 174-2003* [20]
Risk assessment	The process of identifying risks to a business and

Term	Definition
	determining the probability of occurrence, the resulting impact, and identifying actions that would treat the risk.
Threat	An action or event that may result in a detrimental outcome to a system or information asset. *HB 174-2003* [20]
Trojan	A program that appears legitimate, but performs some illicit activity when it is run.
Vulnerability	A weakness that can be exploited that may cause damage to a system or information assets. *HB 174-2003* [20]

References

1. NEHTA. *National eHealth Security and Access Framework v4.0: Overview*. Sydney: NEHTA; 2014. Available from: http://www.nehta.gov.au/our-work/security.

2. NEHTA. *National eHealth Security and Access Framework v4.0: Overview*. Sydney: NEHTA; 2014. Available from: http://www.nehta.gov.au/our-work/security.

3. NEHTA. *National eHealth Security and Access Framework v4.0: Business Blueprint*. Sydney: NEHTA; 2014. Available from: http://www.nehta.gov.au/our-work/security.

4. NEHTA. *NESAF v4.0: Factsheet for consumers.* Sydney: NEHTA; 2013 Available from: http://www.nehta.gov.au/our-work/security.

5. NEHTA. *NESAF v4.0: Factsheet for clinicians.* Sydney: NEHTA; 2013 Available from: http://www.nehta.gov.au/our-work/security.

6. NEHTA. *NESAF v4.0: Factsheet for healthcare organisations.* Sydney: NEHTA; 2013 Available from: http://www.nehta.gov.au/our-work/security.

7. NEHTA. *National eHealth Security and Access Framework v4.0: Implementer Blueprint*. Sydney: NEHTA; 2014. Available from: http://www.nehta.gov.au/our-work/security.

8. NEHTA. *National eHealth Security and Access Framework v4.0: Framework Model and Controls*. Sydney: NEHTA; 2014. Available from: http://www.nehta.gov.au/our-work/security.

9. NEHTA. *National eHealth Security and Access Framework v4.0: Standards Mapping*. Sydney: NEHTA; 2014. Available from: http://www.nehta.gov.au/our-work/security.

10. NEHTA. *National eHealth Security and Access Framework v4.0: Framework Model and Controls*. Sydney: NEHTA; 2014. Available from: http://www.nehta.gov.au/our-work/security.

11. Australian Government Attorney-General's Department. *Protective Security Policy Framework.* [Internet]. [cited 2013 Aug 15]. Available from: http://www.protectivesecurity.gov.au/Pages/default.aspx.

12. Australian Government. *ISM – Information Security Manual.* [Internet]. [cited 2013 Aug 15]. Available from: http://www.dsd.gov.au/index.htm.

13. Australian Government. *The Privacy Act.* [Internet]. [cited 2014 Jun 02]. Available from: http://www.comlaw.gov.au/Details/C2014C00076.

14. Australian Government. *Australian Privacy Principles, Schedule 1, Privacy Act 1988.* [Internet].Australian Government; 2014 [cited 2014 Jun 02]. Available from: http://www.comlaw.gov.au/Details/C2014C00076.

15. NEHTA. *National eHealth Security and Access Framework v4.0: Standards Mapping*. Sydney: NEHTA; 2014. Available from: http://www.nehta.gov.au/our-work/security.

16. International Organization for Standardization. *ISO/TS 14265:2011 Health Informatics - Classification of purposes for processing personal health information*. ISO; 2011. Available from: http://infostore.saiglobal.com/store/.

17. Standards Australia. *AS ISO 27799-2011: Information security management in health using ISO/IEC 27002*. Standards Australia; 2011. Identical to ISO 27799:2008. Available from: http://infostore.saiglobal.com/store/.

18. International Organization for Standardization. *ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security*

management. ISO; 2005. Available from: http://infostore.saiglobal.com/store/.

19. Royal Australian College of General Practitioners. *Computer and information security standards and templates.* [Internet]. [cited 2013 Aug 09]. Available from: http://www.racgp.org.au/your-practice/standards/ciss/.

20. Standards Australia. *HB 174-2003 Information security management - Implementation guide for the health sector*. Standards Australia; 2003. Available from: http://infostore.saiglobal.com/store/.