nehta

NESAF Release 3.1

Executive Summary (S1201)

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 – Executive Summary
Document owner:	National eHealth 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

This page is intentionally left blank

1 Introduction

1.1 Purpose

The purpose of this document is to provide an Executive Summary of the National eHealth Security and Access Framework Revision 3 (NESAF R3) for adoption.

1.2 Intended audience

This document is intended for use by consumers and readers of the National eHealth Security and Access Framework to promote discussion and guide adoption of the frameworks core components and stimulate awareness of the obligations individuals and organisations have but also to allow for a better understanding of how security and access is an enabler of services.

1.3 Scope

The scope of this document relates to providing a high level overview of the National eHealth Security and Access Framework (NESAF) that is suited to describing the purpose, structure and benefits of the Framework for executive audiences. The scope of business for the NESAF will be all aspects of public and private sector healthcare business that have information or connectivity traceability to national systems.

1.4 Overview

This document describes at a high level, the purpose, benefits, structure and risk-based approach of the NESAF.

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 this document. Please direct your questions or feedback to feedback.saf@nehta.gov.au.

2 Executive summary

2.1 Introduction

With the expansion of eHealth services, and increased public use of the internet, Government authorities and health organisations face a challenge to protect data and information by developing robust security for these online services. One of the major reasons for developing stringent security is to engender trust in both individuals and businesses when they are using the eHealth services. In particular, Federal State, Territory Governments and private operators must:

- Protect service users from personal data loss.
- Ensure that such data are accessible to authorised persons only.
- Make sure that the information is not modified or destroyed without prior authorisation.

Australia is committed to fostering the use of information as trusted tool of medicine within the Australian healthcare landscape, so that it ultimately becomes as critical as the surgical scalpel for the surgeon, or lifesaving drugs for the ill. To enable this to happen, the information must be available at the right time, and in the right form, regardless of the origins of the information. It must also be supported by strict, traceable provenance and control.

The flow of eHealth healthcare information moves with the patient, typically starting at the point of care (doctor's office) to pathology, pharmacies, diagnostic imaging and other care services. This accepted flow of health records shows that they traverse multiple health areas where information security must be considered, and appropriate process and control implemented.

Advances in technology are going to have a major impact on healthcare operations, particularly in the area of information sharing, both within organisations, and between organisations. These advances will also make healthcare information more accessible to consumers on an 'anytime, anywhere' basis. As a result of this, it is essential that an appropriate security and access framework is developed to underpin healthcare information, and to ensure its confidentiality and integrity. It is equally important that this framework is tailored to meet the needs of the Australian public, as well as the private health sector. The security framework must be capable of protecting the confidentiality of personal healthcare information, while at the same time supporting improved and unhindered healthcare.

Healthcare information has the greatest value when:

- it is accurate
- it is up to date
- it is accessible where and when it is needed.

Unless there is an effective security framework in place, information assets may become unreliable or compromised, for example if they are accessed by unauthorised third parties. This would lead to degradation in the value of the information, and may also cause the information assets to be withdrawn, meaning that information may not be accessible where and when required. The mission of the National eHealth Security and Access Framework (the NESAF) is to:

- Ensure that access to consumer health information is consistently controlled and monitored as it moves through independent organisations, business processes and systems in the Australian health sector.

- Make sure that the provenance of all electronic health information is traceable from its creation (at a verifiable trusted source), through its transition and possible augmentation on route to its destination.

To achieve this, the NESAF helps organisations engaged in national eHealth to adopt a consistent approach and application of health information security standards. It also provides 'better practice' guidance in relation to eHealth specific security and access practices. Some of the key benefits of a National eHealth Security and Access Framework for use in the Australian environment include:

- Promotion of a consistent, risk-based approach to eHealth security and access.
- Consistent interpretation of relevant standards for application in the Australian eHealth environment.
- Provision of a holistic view of security and access requirements within an organisation, which includes controls that are implemented at a business, healthcare, information technology and eHealth specific level, with greater focus and detailed guidance provided in relation to eHealth specific controls.
- Contemporary better practice guidance on specific eHealth security and access practices.
- A document suite that provides different views on the framework for different audiences - business, clinical, technical and consumer.

Central to all eHealth information exchanges is trust, individuals and businesses must be able to trust in the veracity, security and accuracy of any eHealth transaction. Any breach of security in eHealth information, any failure of access control or traceability will diminish trust within the eHealth system, which in turn would seriously compromise the adoption and uptake of eHealth, severely impacting the expected benefits from investing in eHealth.

It is expected that broad application of the NESAF within healthcare organisations will help engender trust within the national eHealth system, thus increasing adoption and uptake of these systems, and maximising the expected benefits from these investments.

Undoubtedly, eHealth security in Australia is unique; there is no other industry where such widespread change in access, creation and delivery of information is occurring. As the significant investment in Australian eHealth unfolds, the emerging threat and risk to information becomes more prominent. The volume of information being exchanged and accessed is about to dramatically increase, the way information is used will see new and unique methods of access developed to support emerging clinical models, which means that implementing effective information security is of the highest priority.

We are obliged to take a proactive approach to security of information, and those organisations that supply or make use of eHealth information have a duty of care to ensure that the information they own, control or are custodian of is appropriately protected. There is an urgent need to ensure 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.

2.2 NESAF purpose

The vision for the NESAF is to:

'To increase certainty that health information is created and accessed in a secure and trustworthy manner'

The NESAF Vision Statement

The mission for the NESAF is to:

- Ensure 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.
- Make sure that the provenance of all electronic health information is traceable from its creation at a verifiable trusted source, through its transition and possible augmentation on route to its destination.

To achieve this vision and mission, the NESAF supports organisations engaged in national eHealth to adopt a consistent approach to and application of health information security standards, and provides better practice guidance in relation to eHealth-specific security and access practices.

2.3 Benefits

Some of the key benefits of the NESAF for use in the Australian eHealth environment include:

- Promotion of a consistent, risk-based approach to eHealth security and access.
- Consistent interpretation of relevant standards for application in the Australian eHealth environment.
- Provision of a holistic view of security and access requirements within an organisation. This includes controls that are implemented at a business-, healthcare-, information technology- and eHealth-specific levels, with a greater focus and detailed guidance provided in relation to eHealth-specific controls.
- Contemporary better practice guidance on specific eHealth security and access practices.
- A document suite that provides different views on the framework for different audiences – business, clinical, technical and consumer.

It is expected that broad application of the NESAF within healthcare organisations will help engender trust within the national eHealth system, thus increasing adoption and uptake of these systems and maximising the expected benefits from these investments.

2.4 The NESAF document framework

The NESAF document framework comprises a suite of documents designed to provide specific views of the NESAF for business, clinical, technical and consumer audiences (refer to Figure 1).

The third revision of the framework concentrates on the following:

- Core Framework
- Business Blueprint
- Implementer Blueprint
- Framework and Controls

The NESAF development team will be seeking further engagement on the guides as well as exploring the additional guides discussed during the workshops held in October and November 2011.

It is expected that a range of guides and case studies will be produced over the course of 2012.

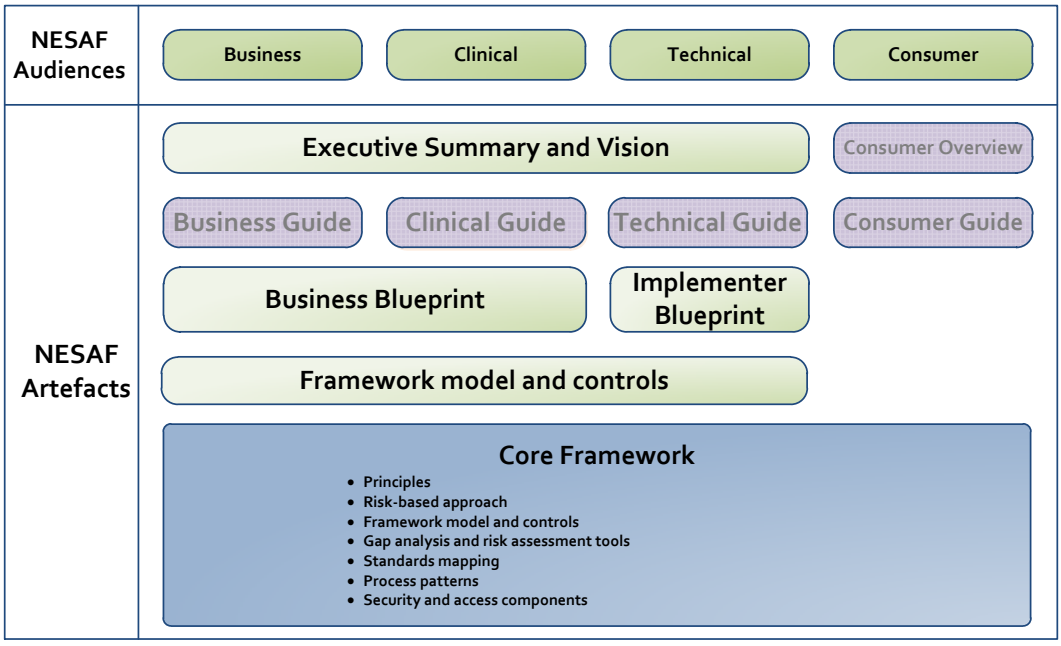

Figure 1: The NESAF document framework

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.

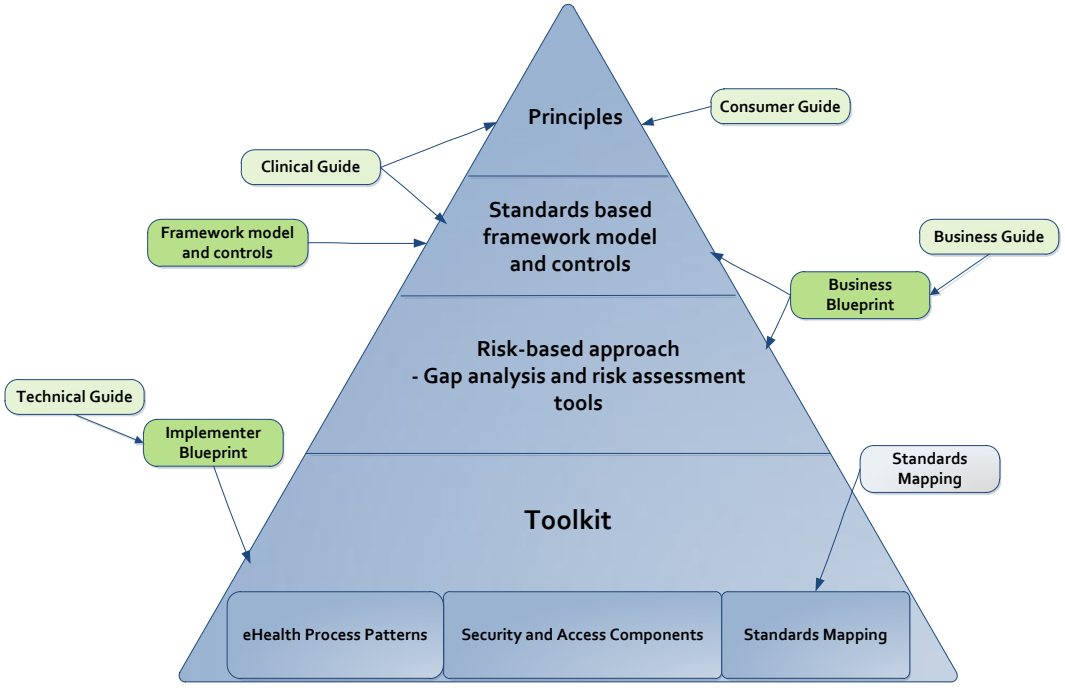

Figure 2: Structure of the NESAF core framework

The core framework includes:

Principles	To guide the design and implementation of secure eHealth systems.
Framework model	That identifies key security and access control areas, control objectives and controls.
Risk-based approach	To support implementation of the framework.
	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.
Toolkit (contained in the Implementer Blueprint)	**eHealth process patterns** that assist businesses to identify core security and access functions in the context of their business.
	A **reference library** of process patterns, security and access functions.
	Service descriptions 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.

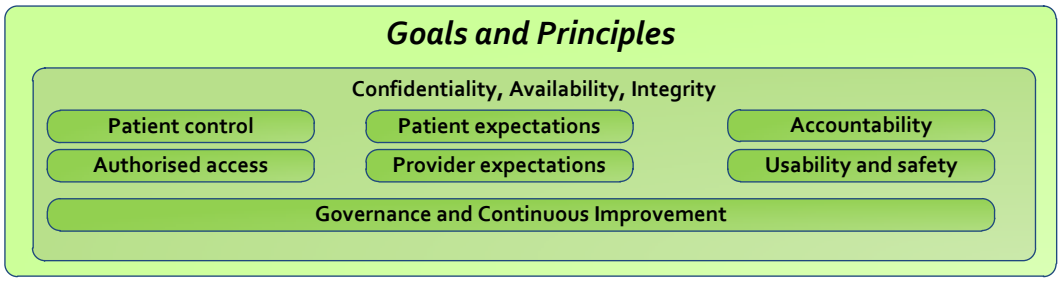

Figure 3: Goals and principles of the NESAF

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 following NESAF principles support these goals:

Patient control - Patients can:

- Be aware of what is happening with their healthcare information
- Check what options they have for exercising a degree of control over who can access their healthcare information.
- See 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.

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.

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 areas relating to eHealth. The model is based on Australian Standards for information security management, and information security management in health.

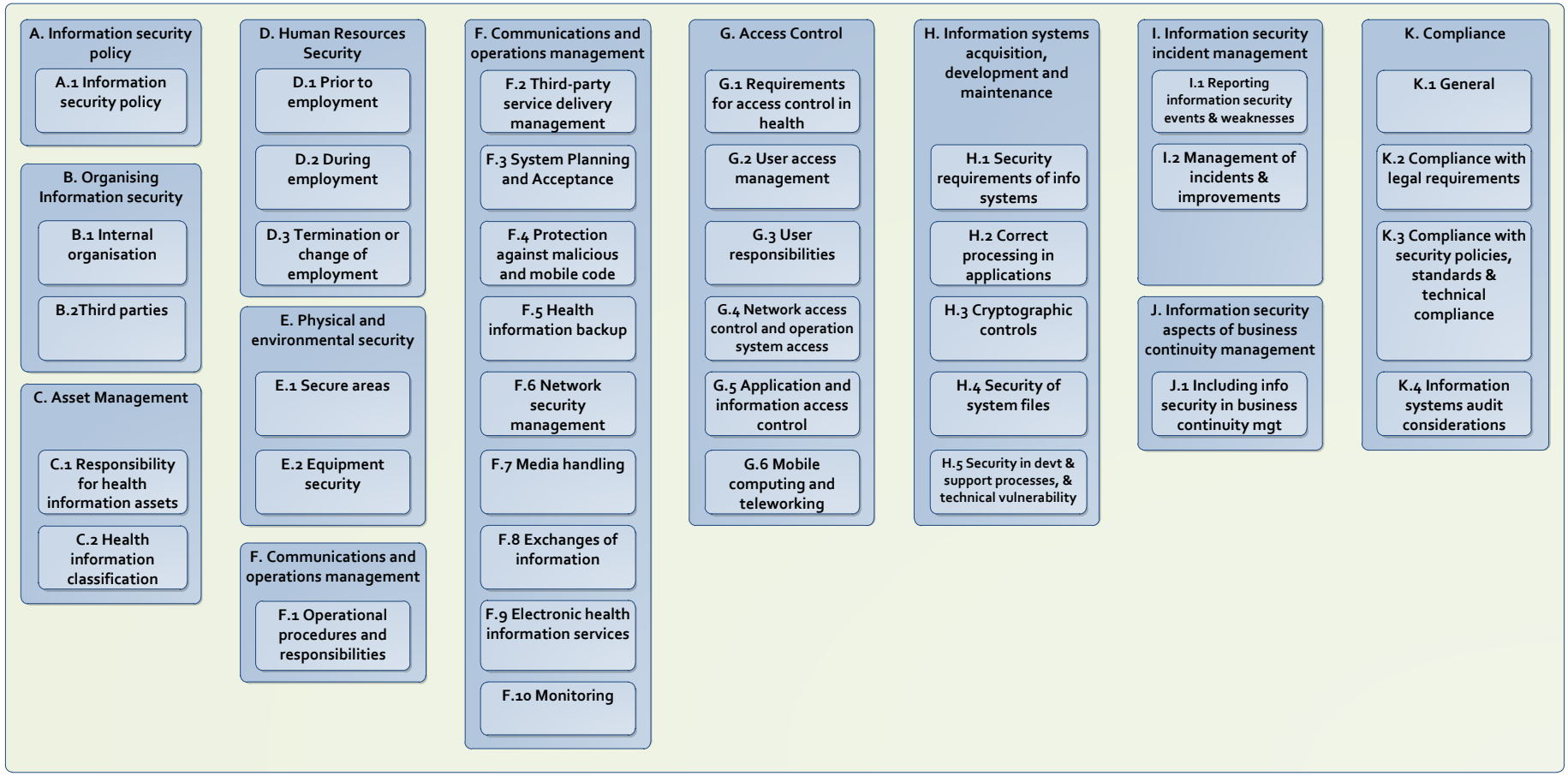

Figure 4: Standards-based framework model

Within each control 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. The full set of control objectives is included in the *Business Blueprint* [S1131].

3.3 Layered approach to information security

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. 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 the *Implementer Blueprint* [S1132].

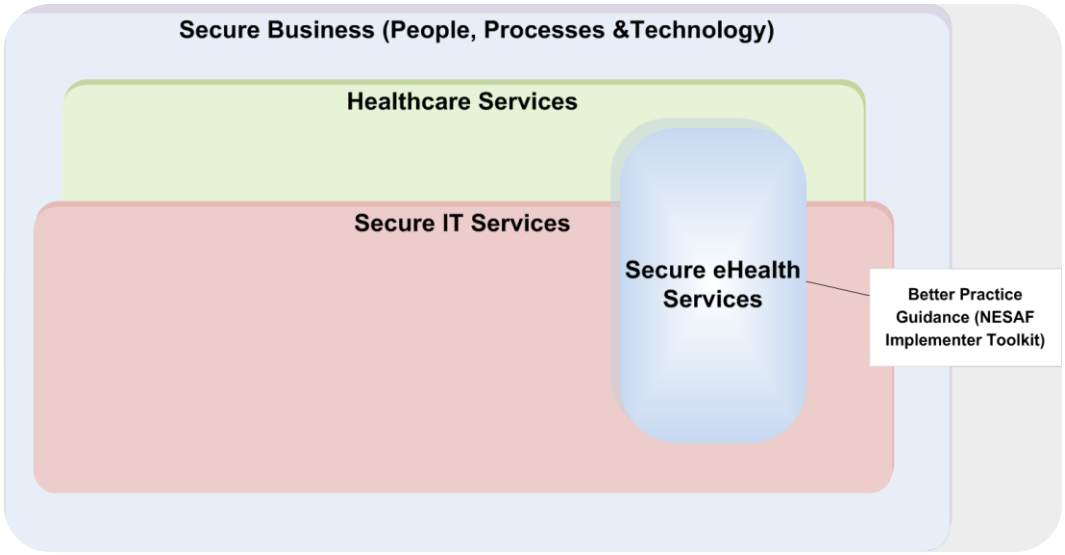

Figure 5: Coverage of NESAF controls

4 Risk-based approach

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

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

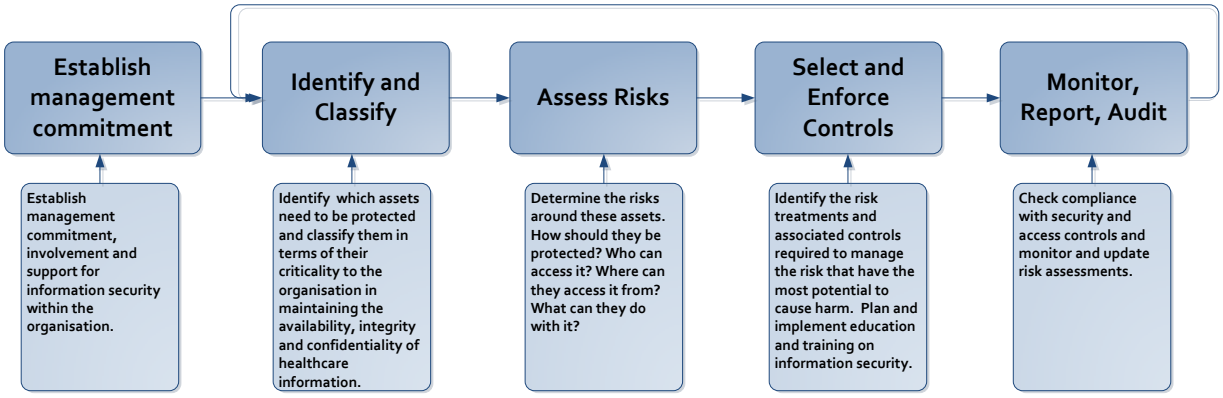

Figure 6: NESAF process flow

An outline of each of the steps is explained in the *Business Guide* [S1114], and further detail (including supporting tools and templates) is provided in the *Business Blueprint* [S1131].

The *Business Blueprint* contains the full set of NESAF controls, and indicates sources of additional guidance, including those for which better practice guidance is contained in the *Implementer Blueprint* [S1132].

5 Implementer Toolkit

The Implementer Toolkit provides a library of eHealth Process Patterns and Security and Access Components that provide better practice guidance in relation to eHealth-specific controls within the NESAF.

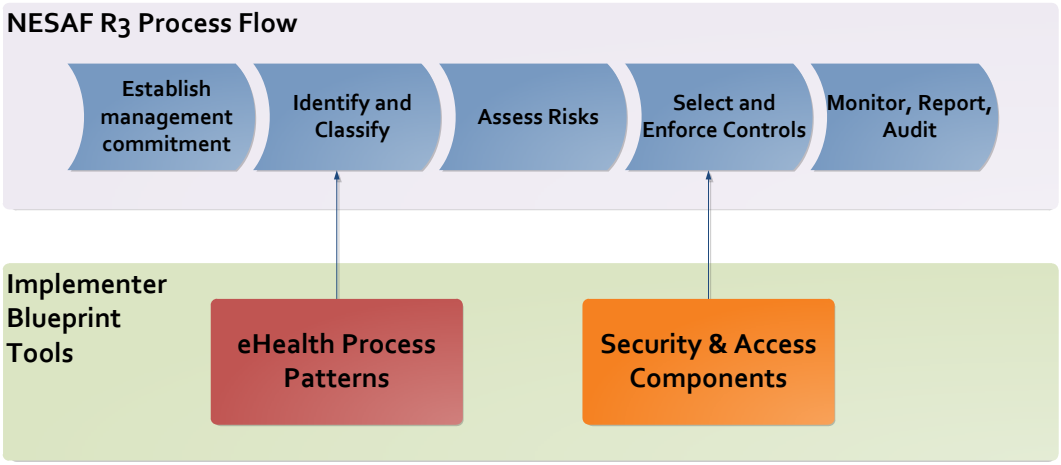

Figure 7: Implementer Blueprint

5.1 eHealth Process Patterns

To assist in the identification and classification of healthcare information assets to be protected, a catalogue of common eHealth process patterns is included in the *Implementer Blueprint* [S1132].

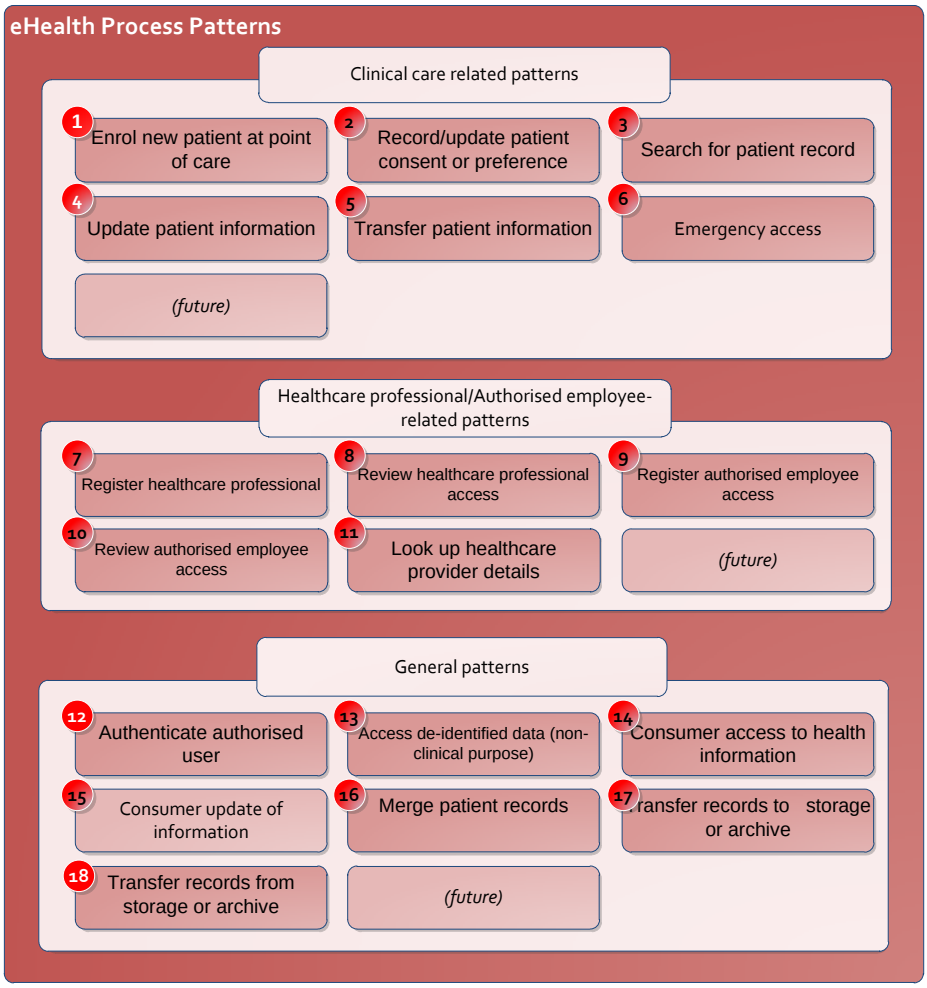

Figure 8: The NESAF Process Patterns

These process patterns can be linked together, based on current or future business processes within the organisation, as illustrated below.

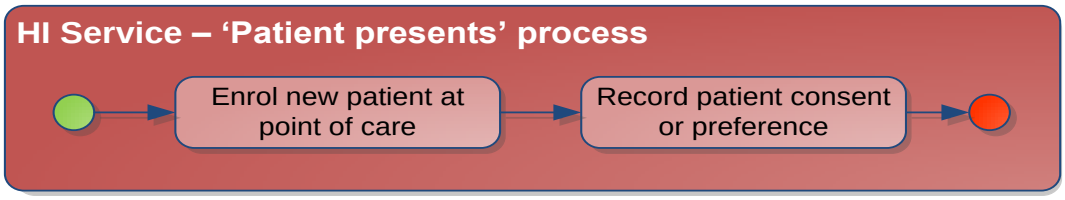

Figure 9: Example of a NESAF set of linked processes

5.2 Service descriptions

The NESAF identifies a catalogue of generic security and access components that are commonly required in eHealth.

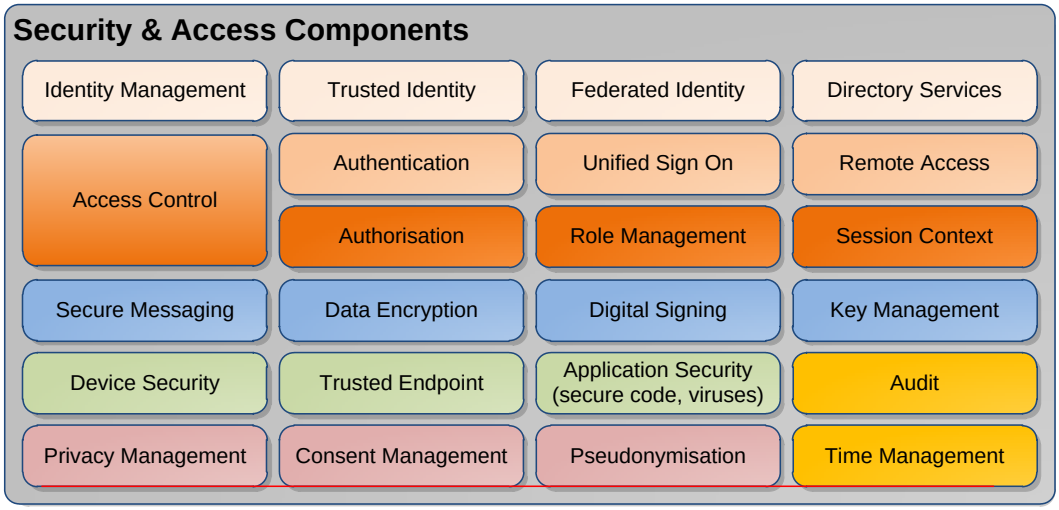

Figure 10: The NESAF Security and Access Components

Within each eHealth process pattern, the NESAF identifies the security and access functions that are commonly involved in that process pattern. A sample model is shown below.

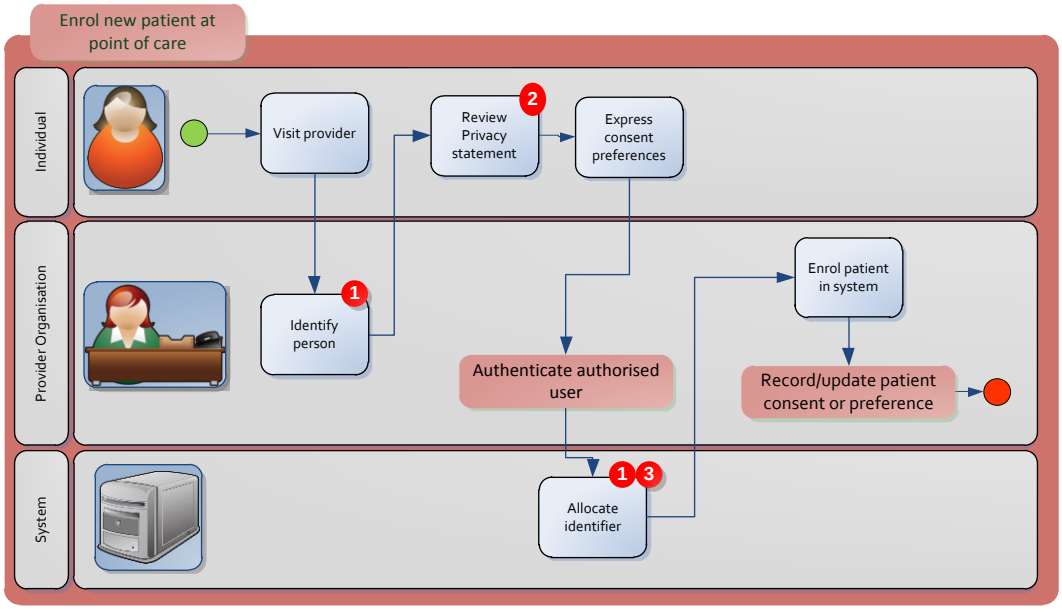

Figure 11: NESAF Example - Enrol a new patient at point of care

For each security and access component, a comprehensive service description has been developed. The service descriptions provide a single source of reference to deliver a set a better practice guidance. The model for trusted identity is shown below to illustrate the structure of each service description.

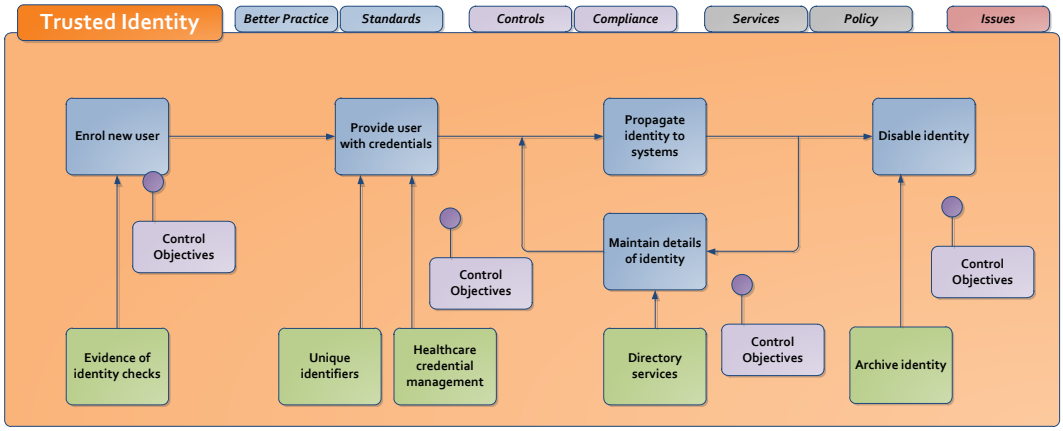

Figure 12: NESAF example - Trusted Identity

The service definition provides a detailed suite of additional information in relation to:

- **Better practice** – Identifies work done to implement these services from health and/or other domains to inform the development of eHealth services.
- **Standards** – Identifies what existing standards and other frameworks might be relevant to this area.
- **Controls –** Identifies controls are typically used in this area.
- **Compliance** – Identifies any area that may be monitored for compliance in relation to this service.
- **Services** – Identifies what existing services can be leveraged to help in implementation programs for this service e.g. for trusted identity, the Healthcare Identifiers service is a strong candidate for unique identification services available across Australia.
- **Policy** – Identifies any relevant policy settings (including legislative or regulatory requirements) around the usage of this service.
- **Issues –** Identifies any known areas or points of difficulty that may arise when designing an implementation.

6 References and Materials

Reference	Description
[NEHTA1]	National E-Health Transition Authority *Healthcare Today: eHealth: an information revolution*. Accessed at: http://www.nehta.gov.au/publications/nehta-publications
[NEHTA2010]	National E-Health Transition Authority *National EHealth Security and Access Framework – Release 1*. 20101217
[NEHTAS1131]	National E-Health Transition Authority *National EHealth Security and Access Framework – Business Blueprint*. v2.0 20113007
[NEHTAS1114]	National E-Health Transition Authority *National EHealth Security and Access Framework – Business Guide*. v2.0 20113007
[NEHTAS1132]	National E-Health Transition Authority *National EHealth Security and Access Framework – Implementer Blueprint*. v2.0 20113007