nehta

National eHealth Security & Access Framework (NESAF) v4

Overview v1.0

6 June 2014

Approved for external use

Document ID: NEHTA-1545:2014

National E-Health Transition Authority

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

Disclaimer

The National E-Health Transition Authority Ltd (NEHTA) makes the information and other material ('Information') in this document available in good faith but without any representation or warranty as to its accuracy or completeness. NEHTA cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control

This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

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		See NESAF v4.0 release note for details

Table of contents

Table of figures

1 Introduction

1.1 Purpose

This document explains the underlying principles behind the NESAF, the benefits of adopting the framework and additional implementation resources.

1.2 Intended audience

This document is intended for the following:

- Practice managers of healthcare organisations
- Healthcare provider organisations
- Individual healthcare providers
- Technical professionals (for example, ICT security analysts, business analysts, IT professionals)
- Consumers

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, that is, general, business, and technical, as illustrated below.

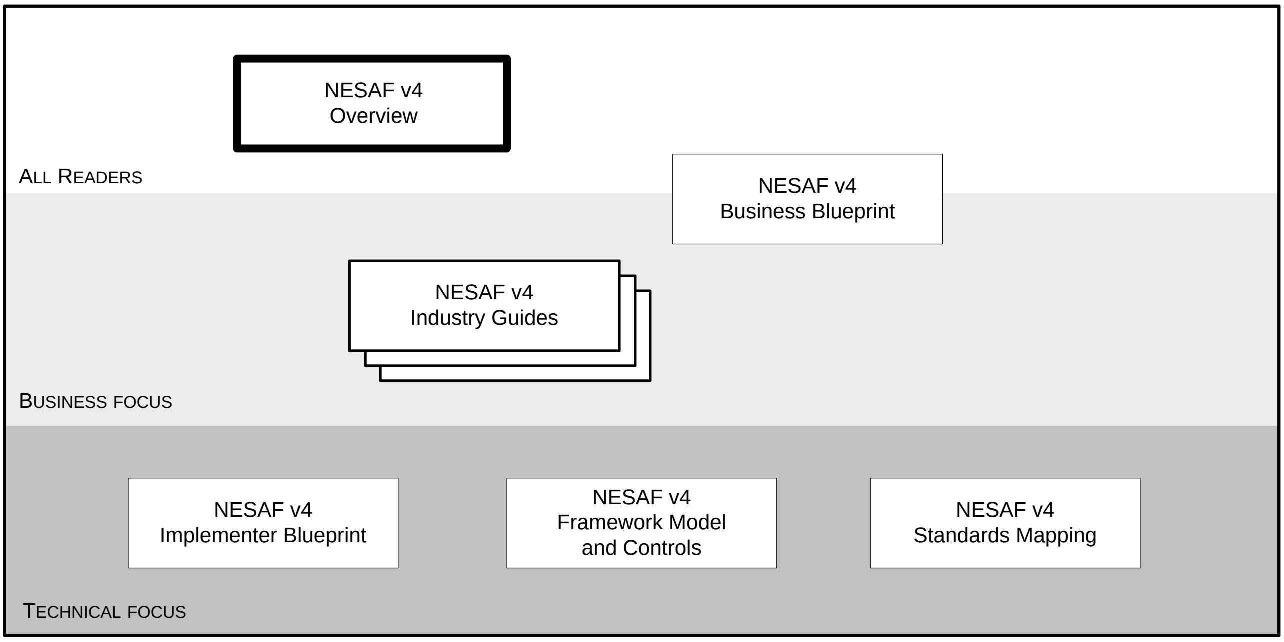

Figure 1: NESAF document framework

As this map would suggest, all readers with an interest in the NESAF should read both the *NESAF v4.0 Overview* [1] and the *NESAF v4.0 Business Blueprint* [2]. 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 3.3 for additional details.

1.4 Questions and feedback

We encourage your comments or suggestions the NESAF and this document itself. Please direct your questions or feedback to help@nehta.gov.au.

2 Background

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. 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.

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 eHealth services. In particular, federal, state, and territory governments, as well as private operators must:

- protect users from personal data loss;
- ensure that such data are accessible to authorised persons only; and
- make sure that the information is not modified or destroyed without prior authorisation.

Healthcare information has the greatest value when it is accurate, is up to date and is accessible where and when it is needed. Australian governments are committed to fostering the use of information as a trusted tool of medicine, so that it ultimately becomes as critical as the scalpel for the surgeon, or lifesaving drugs for the ill.

The flow of eHealth healthcare information moves with the patient, typically starting at the point of care (doctor’s surgery) 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.

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, which in turn would seriously compromise the adoption and uptake of eHealth, severely impacting its expected benefits.

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. Unless there is an effective security framework in place, information assets may become unreliable or compromised.

The National E-Health Transition Authority (NEHTA) in consultation with subject matter experts (security experts, privacy, clinicians and consumers, amongst others) have developed such a framework. This standards-based framework model provides better practice guidance in relation to eHealth-specific security and access practices.

The NESAF identifies 11 key security and access areas relating to eHealth and is scalable to different organisation types and sizes, as well as catering for varying complexity in information exchange.

The model is based on Australian Standards for information security management, and information security management in health. The NESAF provides a risk-based approach from risk identification and analysis to establishing appropriate security and access controls.

The 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. 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 possibly 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 will dramatically increase, as will new 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 custodians of is appropriately protected.

2.1 Purpose of the NESAF

The **vision** for the NESAF is to increase certainty that health information is created and accessed in a secure and trustworthy manner.

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 en route to its destination.

To achieve this vision and mission, the NESAF supports organisations engaged in eHealth at a national level 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.

2.2 Goals and principles of the NESAF

The goals and principles of the NESAF provide guidance for the application of the framework in the design and implementation of secure eHealth systems to manage and protect healthcare information.

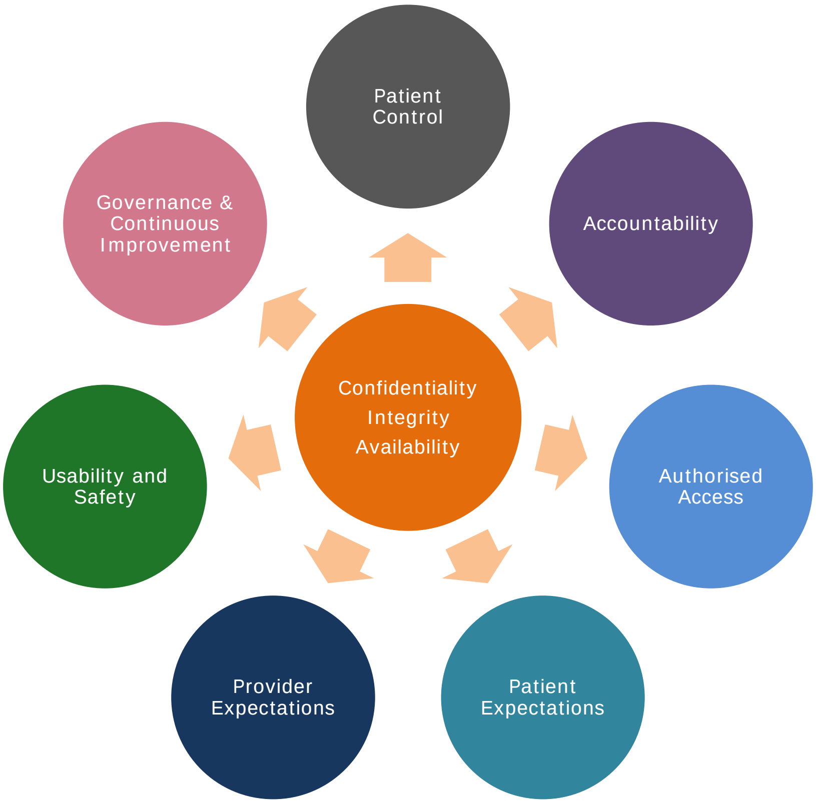

Figure 2: Goals and principles of the NESAF

Confidentiality, integrity and availability of healthcare information are the goals of information security. These goals are supported by the following principles:

- **Patient Control:** A patient is aware of their healthcare information, their ability to control who can access their healthcare information and how their healthcare information is used.
- **Accountability:** All access to personal health information must be accounted for through audit and audit review procedures.
- **Authorised Access:** Any individual, accessing, processing, or disclosing personal health information must have an authenticated right and authorised reason for those activities.
- **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.
- **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.
- **Usability and Safety:** Security as an integral part of healthcare information systems and should support the goals of the organisation by ensuring users find that the secure way is the easy way.

- **Governance and Continuous Improvement:** Organisations must provide commitment and support to healthcare information security and access. Continuous improvement and governance mechanisms should be used to regularly measure, reassess and improve information security and access control.

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 levels specific to the domains of business, healthcare, information technology and eHealth, with a greater focus and detailed guidance provided in relation to eHealth-specific controls.
- A document suite that provides different views on the framework for different audiences – business, clinical, technical and consumers.

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.

3 Structure of the NESAF

3.1 Layered approach to information security

Security of eHealth information requires the use of a layered approach or defence in depth, which 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 2.

The framework focuses in greater depth on the controls used to secure eHealth services, with better practice guidance provided in the *NESAF v4.0 Implementer Blueprint* [3].

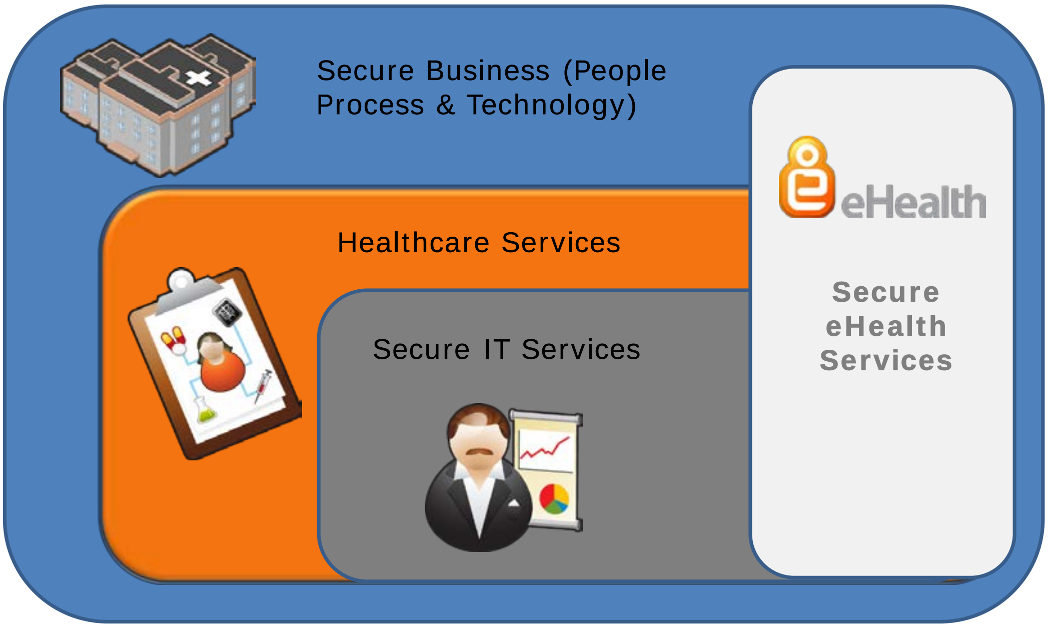

Figure 3: Coverage of NESAF controls

3.2 Risk-based approach

The NESAF sets out a risk-based approach, a process to assist businesses/organisations to identify specific threats that they may need to mitigate with 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 to identify appropriate security and access controls may include policies, practices, procedures, software and other technical solutions.

Figure 4 outlines key steps that a business should undertake in order to identify and implement suitable information security and access controls.

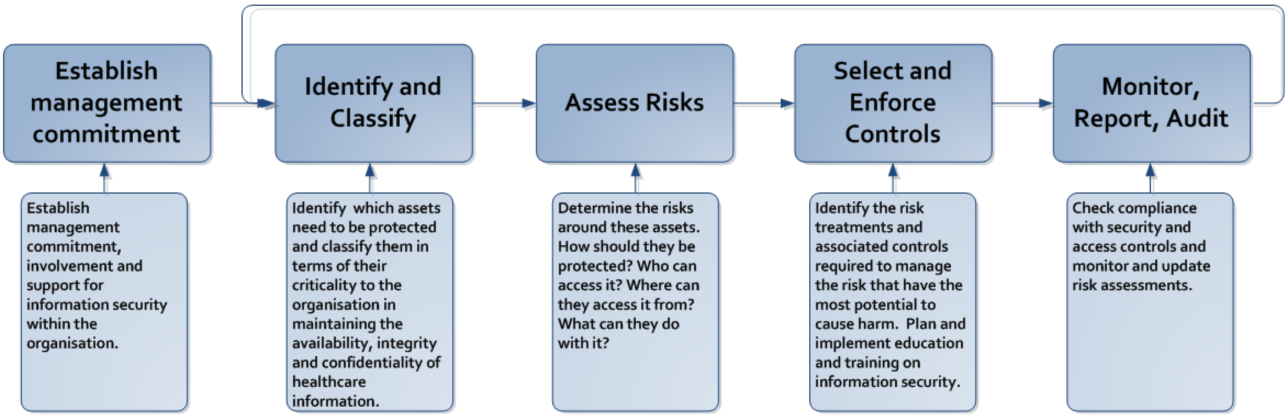
Establish management commitment
Identify and Classify
Assess Risks
Select and Enforce Controls
Monitor, Report, Audit
Establish management commitment, involvement and support for information security within the organisation.
Identify which assets need to be protected and classify them in terms of their criticality to the organisation in maintaining the availability, integrity and confidentiality of healthcare information.
Determine the risks around these assets. How should they be protected? Who can access it? Where can they access it from? What can they do with it?
Identify the risk treatments and associated controls required to manage the risk that have the most potential to cause harm. Plan and implement education and training on information security.
Check compliance with security and access controls and monitor and update risk assessments.

Figure 4: NESAF risk-based process flow

An outline of each of the steps is explained in the *Implementer Blueprint* and further detail (including supporting tools and templates) is provided in the *Business Blueprint*.

3.3 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.

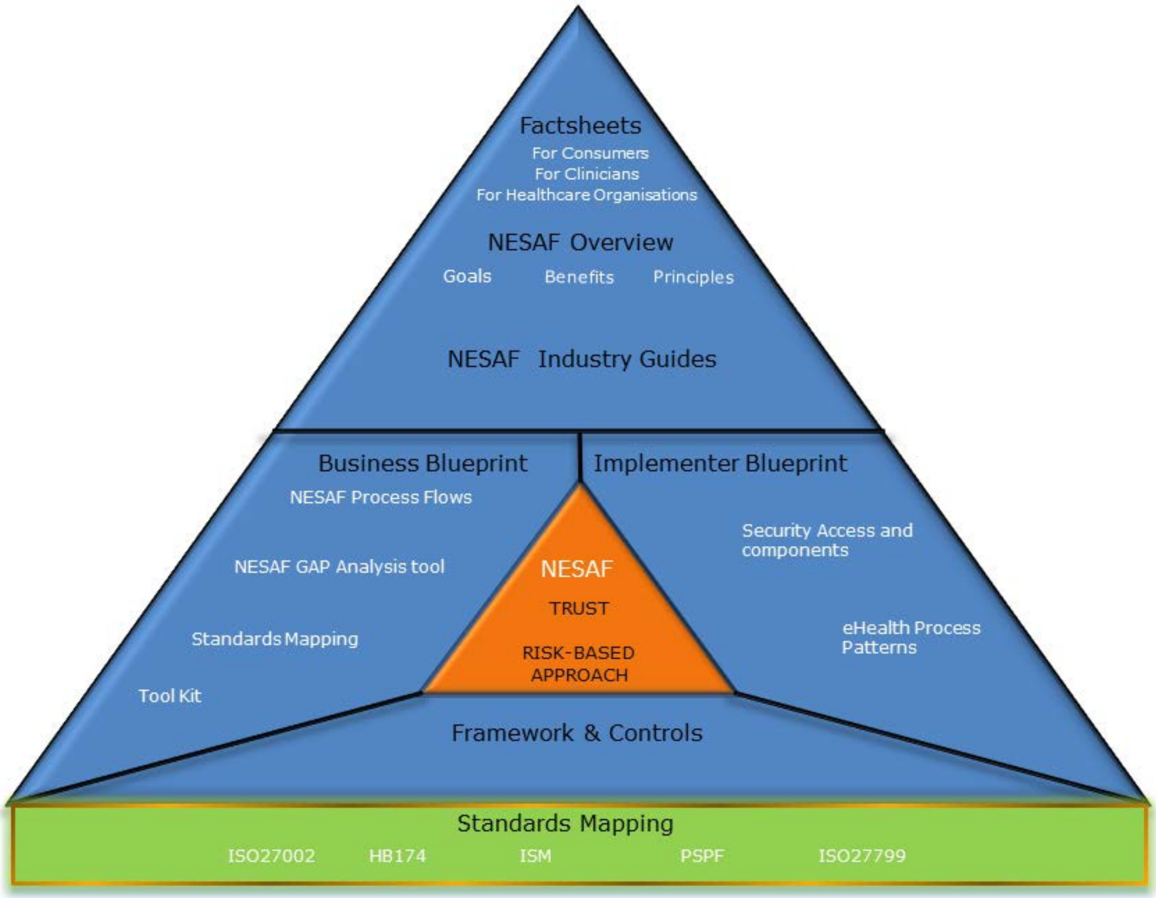

Figure 5: NESAF themes and documents

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.
NESAF v4.0 Healthcare Organisation Factsheet [6]	Healthcare organisations	An introduction to the NESAF 4.0, targeted at healthcare organisations.
NESAF v4.0 Overview [1] (this document)	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 [2]	• 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.

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