2012

A Holistic Approach to eHealth Security in Australia: Developing a National eHealth Sercurity and Access Framework (NESAF)

Yvette Lejins
National E-Health Transition Authority (NEHTA), feedback.saf@nehta.gov.au

John Leitch
National E-Health Transition Authority (NEHTA)

Originally published in the Proceedings of the 1st Australian eHealth Informatics and Security Conference, held on the 3rd-5th December, 2012 at Novotel Langley Hotel, Perth, Western Australia

A HOLISTIC APPROACH TO EHEALTH SECURITY IN AUSTRALIA: DEVELOPING A NATIONAL EHEALTH SECURITY AND ACCESS FRAMEWORK (NESAF)

Yvette Lejins, John Leitch
National E-Health Transition Authority (NEHTA)
feedback.saf@nehta.gov.au

Abstract
The Australian ehealth landscape is confronted with new challenges for healthcare providers in appropriately managing and protecting personal health information. The vision of the National eHealth Security and Access Framework (NESAF) is to adopt a consistent approach to the application of health information security standards and provide better practice guidance in relation to eHealth specific security and access practices. The eHealth information security landscape has a number of unique attributes, many that are faced by other business that provide a service or products – but we see that there is no industry in Australia where such widespread changes in the access to, the creation and delivery of information is transpiring. As the significant investment in Australian eHealth unfolds the emerging threat and risk assessment for information security and access is more prominent. There is an increasing volume of information being exchanged and accessed, and that this will occur in novel ways supporting emerging clinical models and to meet patient needs and growing expectations from the information age. One key area that must be examined is data provenance, ensuring that all electronic health information is traceable from its creation at a verifiable trusted source, and through its transition and possible augmentation enroute to its destination for immediate and potential futures uses. This will support better health outcomes for patients, and also the use of the information to support tertiary and secondary uses. For example, Clinical Research may generate personal health content in the context of a clinical trial and its context of use bound to the research environment in which it was generated. The goals and principles of the NESAF are intended to guide in the design and implementation of secure eHealth systems to manage and protect healthcare information. This paper presents a description and discussion of the NESAF framework, and the work that has driven its formulation.

Keywords
eHealth Security, information security, National eHealth Security and Access Framework, NESAF, PCEHR, provenance, NEHTA, Australia, healthcare

INTRODUCTION

Australia is committed to the use of information as a trusted tool of medicine, as critical to the provision of healthcare as the surgical scalpel or lifesaving drugs. To do this, information must be available at the right time and in the right form, regardless of its origin, all the while supporting traceable provenance and control. The flow of healthcare information shadows 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 transitions through an array of points where health information security must be considered and appropriate process and control implemented.

As healthcare operations benefit from advancing technologies which promote information sharing within organisations, between organisations, and is accessible by consumers on an anytime anywhere basis, it is increasingly essential to embed an appropriate information security and access framework that is tailored to meet the needs of the Australian public and private health sectors. This is essential to preserve the integrity and protect the confidentiality of personal health information and personally identifiable information, while balancing the need to support improved and unhindered healthcare.

Healthcare information has greatest value when it is accurate, up to date and is accessible where and when it is needed. Without effective security, information assets may become unreliable and untrustworthy, may not be accessible where or when needed, or may be compromised by unauthorised third parties. The mission of the National E-Health Security and Access Framework (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.

- Ensure 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 mission, NESAF supports organisations engaged in national eHealth to adopt a consistent approach and application of health information security standards, and provides better practice guidance in relation to eHealth specific security and access practices. Some of the key benefits of a National E-Health 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, that includes controls that are implemented at a business, healthcare, information technology and eHealth specific level, 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 NESAF within healthcare organisations will contribute to engendering trust within the national eHealth system, thus increasing adoption and uptake of these systems and maximising the expected benefits from these investments.

Undoubtedly the eHealth security landscape is unique - there is no industry in Australia where such widespread change in access, creation and delivery of information is transpiring. As the significant investment in Australian eHealth unfolds the emerging threat and risk landscape to information becomes more prominent. Increasing volumes of information will be exchanged and accessed, in novel ways, to support emerging clinical models and to meet patient needs. eHealth is about to move en masse and security must be an upmost consideration.

Trust is the essential enabler, and centric to all electronic health information exchange. Any breaches and failures of security and access control will diminish trust within the eHealth system and seriously compromise adoption and uptake of eHealth and the expected benefits derived from these investments.

A proactive approach to security of information is therefore obligatory, 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 too is appropriately protected. There is an imminent 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.

This paper is based on the work undertaken by the authors on the NESAF and based primarily on, and reflective of, the NEHTA NESAF ehealth information security documentation (NEHTA, 2012a; 2012b; 2012c; 2012d).

THE NESAF'S CHALLENGE

'To increase certainty that health information is created and accessed in a secure and trustworthy manner'.
The NESAF Vision statement

Information security and privacy is critical to the broad adoption, utilisation and confidence in eHealth products and solutions, medical technologies and electronic exchanges of health information. The 2008 National E-Health Strategy (Department of Health and Aging, 2008) highlighted both the government's intention to digitise the Australian health system and the great benefits digital technologies can bring to the health sector. A digitally enabled health sector allows a greater capacity to share and access health data, and increases collaboration and interoperability. As a consequence, the Australian health system will be able to do more with existing resources, allowing the right health resources to be deployed against real need, ultimately leading to better health outcomes for all Australians.

A more digitised health sector, particularly when high-speed broadband is more widely available, will improve the capacity of health professionals to consult with patients via teleconferencing facilities. Telemedicine will reduce travel costs and increase the reach of medical professionals, providing much needed medical support to rural and remote patients and for those with afflictions that limit mobility.

That is why the National Digital Economy Strategy sets a goal that by 2020, 90% of high priority consumers can access electronic health records, with 495,000 telehealth consultations delivered by 2015 (Office of the Prime Minister and Cabinet, 2011).

What is the NESAF?

The NESAF is not the entire solution. The NESAF provides a means to identify and better understand the questions around individuals and organisations obligations to secure accessible health information. The NESAF provides a consistent, risk based approach to eHealth security and access. As it stands, it is a document framework comprising of a suite of documents designed to provide specific views of the NESAF, for business, clinical and technical audiences. The development of the NESAF is not a radical new approach or methodology on how to address security and access concerns in the eHealth landscape, but rather leverages the numerous security frameworks that are already available, which are tried and tested, and embraces these to develop a framework that fills the gaps, and will be fit for purpose for our unique and rapidly evolving Australian eHealth landscape. Indeed, ISO/IEC 27002, and its health related interpretation ISO27799 are the main standards that underpin the framework.

The NESAF is not intended to replace existing privacy principles, laws and governance that address information handling, but provides guidance to people responsible for designing and implementing eHealth systems, on the way security controls should be established and appropriate access should be operationalised in their systems.

End user system security is a prime focus area for the NESAF. Within the greater eHealth community - the doctors' practice, the pharmacy, the pathology laboratory, and the rural hospital, they all have unique business practices and processes and therefore have varying levels of security and controls in place for the protection of the information they are custodian to. The NESAF is designed to harmonise with and inform existing guidelines and approaches, and to consistently guide healthcare providers, system implementers and consumers in the security and access aspects of eHealth solutions.

The NESAF recognises that complexities of security in health cannot be solved by the IT Professional alone, and unlike traditional information security frameworks and standards, this framework has focussed aspects to different targeted audiences (clinical, consumer, technical and business users) and the NESAF information and frameworks are presented accordingly.

The NESAF is more than guidelines and approaches, the core framework of the NESAF includes:

- A set of **principles** that are intended to guide the design and implementation of secure eHealth systems.
- The framework **model** that identifies key security and access control areas, control objectives and **controls**.
- A **risk-based approach** to support implementation of the framework, including:
  - **Gap analysis and risk assessment tools** that organisations can use to assess their level of risk and compliance with each of the security and access control areas within the framework model.
- A **toolkit** that provides a comprehensive library of information relevant to specific eHealth processes (e.g. authenticate healthcare professional) and security and access functions (e.g. authentication). Key components of the toolkit include:
  - **EHealth process patterns** that assist businesses to identify core security and access functions in the context of their business.
  - **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.
  - A **legislative and policy framework** document that identifies key legislation and policy within Australia that relates to eHealth.

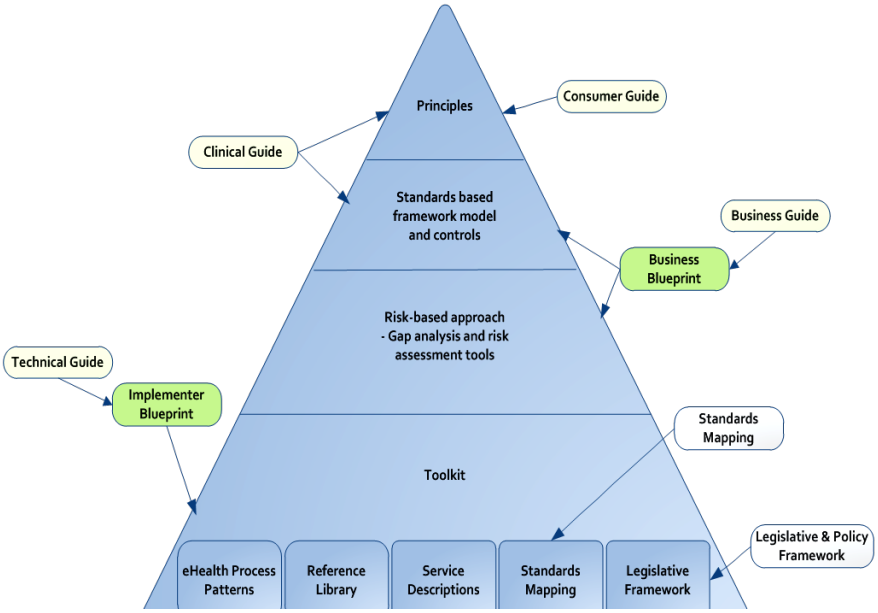

Figure 1: Structure of the Core NESAF Framework (NEHTA, 2012c).

As depicted in Figure 1, the toolkit embedded in the implementer blueprint forms the foundation of the work that supports the principles of NESAF.

Goals and Principles of 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 2).

Figure 2: Goals and Principles of the NESAF

The components of Confidentiality, Availability and Integrity (CAI) of healthcare information are the goals of health information security. These are shown in figure 3.

Within the three pillars of CAI, the NESAF principles underpin these goals:

- **Patient Control:** Patients have control over their health information. They are able to express their wishes (which may change over time) as to who can access their healthcare information, and how their healthcare information is used.
- **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 Access:** Patients have the right to obtain access to their health information. This includes the right to access information concerning when and by whom their health information has been collected, accessed, used and disclosed by others.
- **Provider expectations:** Healthcare providers expect to have available and be able to rely upon healthcare 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.

- **Secure information systems:** Security requirements for information systems that support the health service delivery should be identified and implemented as part of their design or development to ensure that security is an integral part of those systems.
- **Organisational commitment:** Organisations must provide commitment and support to healthcare information security and access within the organisation and ensure that statutory, regulatory and contractual security requirements are met.

The goals and principles together guide the foundation of NESAF work.

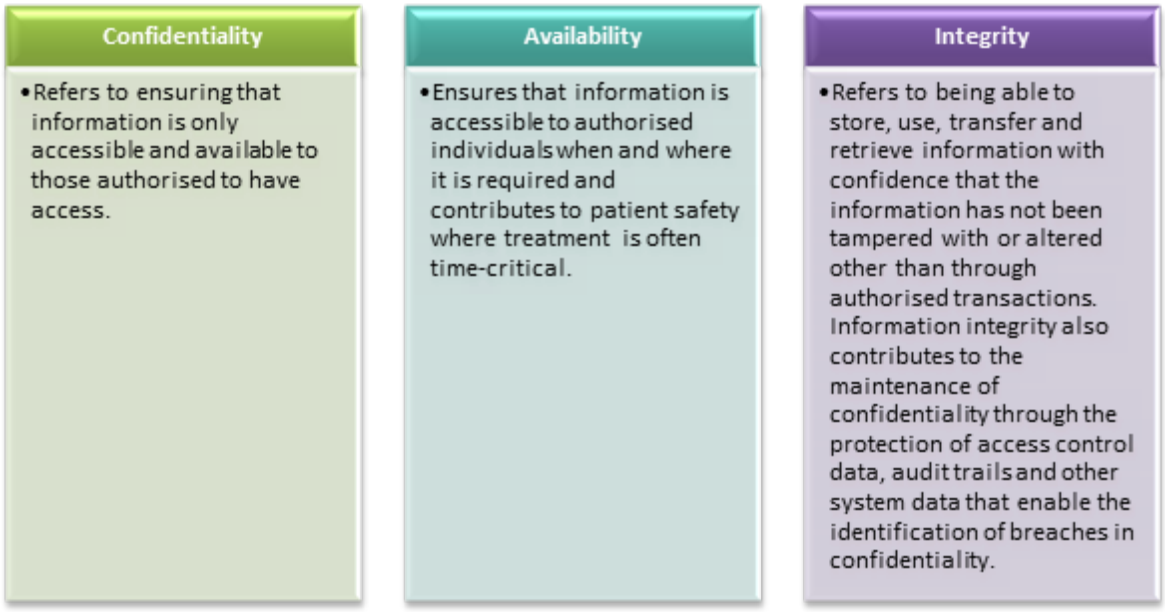

Figure 3: Goals of Health Information

What gap does the NESAF bridge for health security?

Successful eHealth initiatives around the world rely on patients and healthcare professionals trusting their information systems and solutions, and Australia is no different. This 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 the knowledge that the data is held privately, in line with patient wishes and clinical needs.

The delivery of eHealth in Australia will see a surge of personal healthcare data bought online by organisations that will need to have heightened understanding of their responsibilities and obligations, as well as ensuring that their systems are secure. While the security of patient information and the systems that store, access and exchange this information may be secondary to their core business of facilitating patient care, ensuring an operationally realistic balance between the two is the main goal.

Existing security and health frameworks and standards exist in the space, but have limitations including:

- They are not scalable to address the future state for eHealth in Australia.
- They are organisation centric – inward protection focus rather than outward and exchange / journey / provenance of information.
- There is a lack of Australian-specific focus in relation to health security issues.
- The target audience is primarily technical IT staff – with less emphasis on business, clinicians and consumers.
- They are Australian legislation-agnostic the NESAF is heavily influenced by legislation, such as Commonwealth and State privacy laws.
- They can be overwhelming in content and application leaving them wondering - Where do I start?

As reflected in Medical Codes of Practices, and Medical oaths, practitioners have long placed a high value (that is highly recognised by the consumer community), on the protection of an individual's health information.

There are strict obligations that practitioners must undertake to respect patient privacy and to protect their information. Consumers understand and have expectation of trust that their health information will not be used, shared and disclosed unless it is authorised by them. They also have expectation that their information will be recorded accurately. As the immense benefits of connecting the islands of health information come to play, so does a breeding ground of emerging risks. To date these controls have been effective in maintaining the community's confidence in the health system and there is little tangible evidence of significant security failures or critical breaches. However, the investments being made in eHealth in Australia will result in increasingly larger quantities of information being transferred, and this information being exchanged in novel ways supporting emerging clinical models and patient needs; the consumer feels vulnerable.

Value Proposition of the NESAF

Healthcare organisations today continue to face many, and often increasing challenges when managing health information risks across the enterprise, and between organisations. The connected healthcare system provides a rich breeding ground for risk to individual privacy, confidential information, data integrity, and service availability. As a result, organisations look at ways to help address those challenges when making information security and security arrangements. There is an ever-increasing reliance on Health IT-based information systems, which are becoming more complex, integrated and interoperable. The NESAF consists of a comprehensive set of information security and access-specific Principles, controls sets and control objectives, reflecting the findings from a wide range of Australian health projects, such as Personally Controlled Electronic Health Record (PCEHR), the National Authentication Service for Health (NASH), Secure Messaging Delivery (SMD), Healthcare Identifiers Service, and Conformance, Criteria and Accreditation (CCA). In addition it draws on main security controls in other security related standard; HL7PASS, OASIS, ISO/IEC 27002 (27799), COBIT and RACGP.

Included in the NESAF are areas that are extremely important to many organisations including control objectives aimed at complying with legal and regulatory requirements. These include National Privacy Principles, Information Privacy Principles, and Australian Government Frameworks – National E-Authentication Framework (NeAF), Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM). Consequently, the NESAF is designed to be used by many organisations as the basis for their internal information security and access standards and guidelines, and as a key resource to assist them in meeting their compliance obligations.

The NESAF framework will make security easier to implement by being:

- Logical and platform independent. There is no bias toward technologies or software. The principles are independent of any specific technological platform used to implement it.
- Structured at a high level – toolkits and implementation guides lead you through a process.
- Simple and scalable. Can be tailored for small, medium or large organisations.
- Tailored to all aspects of health business, not just a focus on IT Systems.

The NESAF is currently being applied to a number of eHealth initiatives and settings. This includes proof of concept work being undertaken within the NEHTA programs of work (including the PCEHR), as well as application into State led eHealth implementation projects, the RACPG security guidelines and discrete health system security implementations. The NESAF has demonstrated the capability of being scalable and has confirmed its value in the market. The proof of concept work has allowed for valuable feedback to be gained and allowed further refinement to enhance the frameworks value.

How can NESAF be applied?

Healthcare organisations may apply NESAF for various purposes. Some of the possible scenarios for NESAF usage including:

- **Assessing existing eHealth systems – The** NESAF can be used to benchmark the current security arrangements for these systems in 'business as usual' mode. The results of the assessment can be used just to identify and understand current risks, but can also inform planning for treatment of the risks and implementation of measures to address them.
- **Project guidance for new capabilities -** For new systems being implemented, upgrades being made to existing environments or connections being made to new external or national systems, NESAF can play a useful guidance role for security and access.
- **Product or service design -** Although NESAF does not provide a prescriptive recipe or a compliance regime, it can guide product designers in identifying the types of security controls which products should support.

- **Product procurement activities -** As a hybrid of the project and product applications, NESAF can also play a role in procurement guidance. If a project needs to build a system which utilises new vendor solutions procured through the project, NESAF can help to translate the information security risks into functional requirements to be met through the vendor solution.

There are two key starting points for implementation of the NESAF. These are the NESAF ***Business*** and the ***Implementer*** Blueprints.

The NESAF ***Business Blueprint*** is a document that describes how healthcare businesses and organisations will implement the NESAF. The implementation of secure eHealth systems is generally a localised activity, but one which is more likely to produce better results across the sector if the security domain is treated in a consistent manner. To this goal of consistency, the NESAF ***Business Blueprint*** describes a set of control areas derived from recognised security standards such as ISO 27002 and ISO 27799. It creates a view of the elements of the core framework specifically targeted at providing guidance for business and clinical audiences in the implementation of NESAF. The NESAF ***Business Blueprint*** describes an approach for gathering assets, assessing the risks around those assets and then devising a treatment plan. NESAF uses a standards-based approach to analysing the security and access requirements from an eHealth environment, and utilises a risk-based approach to determining the assets which need protection and the types of protection measures which are suitable.

To assist in identifying and classifying the health assets to be protected, the NESAF ***Implementer Blueprint*** contains a set of generalised eHealth process patterns which can assist during the initial phases of a NESAF assessment. It is anticipated that main users of this blueprint will be system analysts and designers. An effective union between secure software and an appropriate operations environment can help to deliver suitable secure eHealth environments. The blueprint provides information to better inform decisions made for design and implementation of secure eHealth systems.

The systems outlined by the ***Implementer Blueprint*** use generalised controls, and translates these into system or technical measures which can deliver the necessary levels of security. The approach used for this translation process is based on using a library of technical components which can be aggregated to support the security requirements of the high level process models from the systems being secured.

To assist in the analysis, assessment and outcome planning phases, there are:

- Generalised eHealth patterns which describe common transactions required in eHealth systems.
- Better practice guidance for specific topics in eHealth implementation projects.

The outcome from the NESAF risk assessment is a set of risks to be treated via NESAF controls. There are approximately 140 controls in the NESAF, and they cover a wide range of areas for securing health environments. Health organisations will select a set of controls to treat the risks, and the controls will guide a future program of work.

Not all of the controls in the NESAF have a direct connection to building eHealth systems. Some relate to more general organisational processes which are used across the business, some relate to healthcare processes, some are in the domain of secure IT operations, and only a subset directly connect to eHealth.

The NESAF characterises a set of domains for designing risk treatments across this framework. The domains are shown in Figure 4.

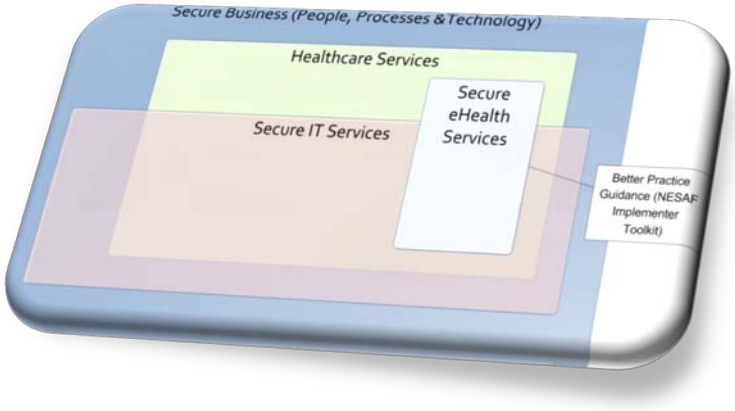

Figure 4: Domains for designing risk treatments

CONCLUSION

The success of eHealth initiatives is dependent on consumers and healthcare professionals trusting their information systems and solutions. The application of the NESAF will promote improvement of the security of transactions and ensure that they are consistently controlled and monitored, and traceable provenance is established. This trust stems from people having confidence in the systems content, in their ability to appropriately collect access, use and disclose data held by these systems and the knowledge that the data is held privately, in line with patient wishes and clinical needs. The NESAF will be a foundation to accompany and inform eHealth solution implementations, and provide a basis for consistent implementation of security within Australia.

REFERENCES

Department of Health and Aging. (2008). National E-Health Strategy. Retrieved from http://www.health.gov.au/internet/main/publishing.nsf/Content/National+Ehealth+Strategy

Office of the Prime Minister and Cabinet. (2011). "Connecting with Confidence – Optimising Australia's Digital Future. A Public Discussion Paper". Retrieved from http://www.egov.vic.gov.au/focus-on-countries/australia/trends-and-issues-australia/information-and-communications-technology-australia/cyber-security-australia/connecting-with-confidence-optimising-australia-s-digital-future.html

NEHTA. (2012a). NESAF Release 3.1 Business Blueprint. Retrieved from http://www.nehta.gov.au/component/docman/doc_download/1473-nesaf-r31-business-blueprint

NEHTA (2012b). NESAF Release 3.1 Framework Models and Controls. Retrieved from http://www.nehta.gov.au/component/docman/doc_download/1475-nesaf-r31-framework-models-and-controls-

NEHTA. (2102c). NESAF Release 3.1 Implementer Blueprint. Retrieved from http://www.nehta.gov.au/component/docman/doc_download/1476-nesaf-r31-implementer-blueprint

NEHTA. (2102d). eHealth Information Security. Retrieved from http://www.nehta.gov.au/connecting-australia/ehealth-information-security