National eHealth Security and Access Framework Release Note v4.0

6 June 2014

Approved for external information

Digitally signed by National E-Health Transition Authority Ltd
Date: 2014.06.04 13:24:23 +10'00'

Summary

End Product: EP-1544:2014 National eHealth Security and Access Framework v4.0

The National eHealth Security and Access Framework (NESAF) v4.0 is a risk-based approach that identifies 11 key security and access areas relating to eHealth. It gives healthcare provider organisations the necessary security processes, tools and information to adjust to Australia's evolving eHealth environment.

The framework is based on international standards for information security management systems in health (ISO27001), information security management (ISO27799), and the *Australian Government Information Security Manual 2014*.

Release rationale

This release consolidates stakeholder feedback from independent reviews by reputable security firms as well as updates based on lessons learned during the application of the framework from the March 2012 release.

The NESAF has also been updated to reflect changes to:

- Processes relating to online registration for the PCEHR;
- The use of NASH certificates; and
- Australian privacy legislation.

For detailed changes, see pages 4 to 7.

Package inclusions

Note that, while the end product bundle and release note are v4.0, the document version numbers have been reset to v1.0.

Updated (supersedes previous version)

Identifier	Name
NEHTA-1553:2014	NESAF v4 – Release Note v4.0
NEHTA-1545:2014	NESAF v4 – Overview v1.0
NEHTA-1546:2014	NESAF v4 – Business Blueprint v1.0
NEHTA-1550:2014	NESAF v4 – Implementer Blueprint v1.0
NEHTA-1549:2014	NESAF v4 – Framework Model and Controls v1.0
NEHTA-1552:2014	NESAF v4 – Standards Mapping v1.0

Removed from bundle (but still available)

The clinical, consumer and business fact sheets published in the NESAF v3.1 bundle are still available from https://www.nehta.gov.au/our-work/security. No changes have been made to these factsheets since their last release.

Stakeholders

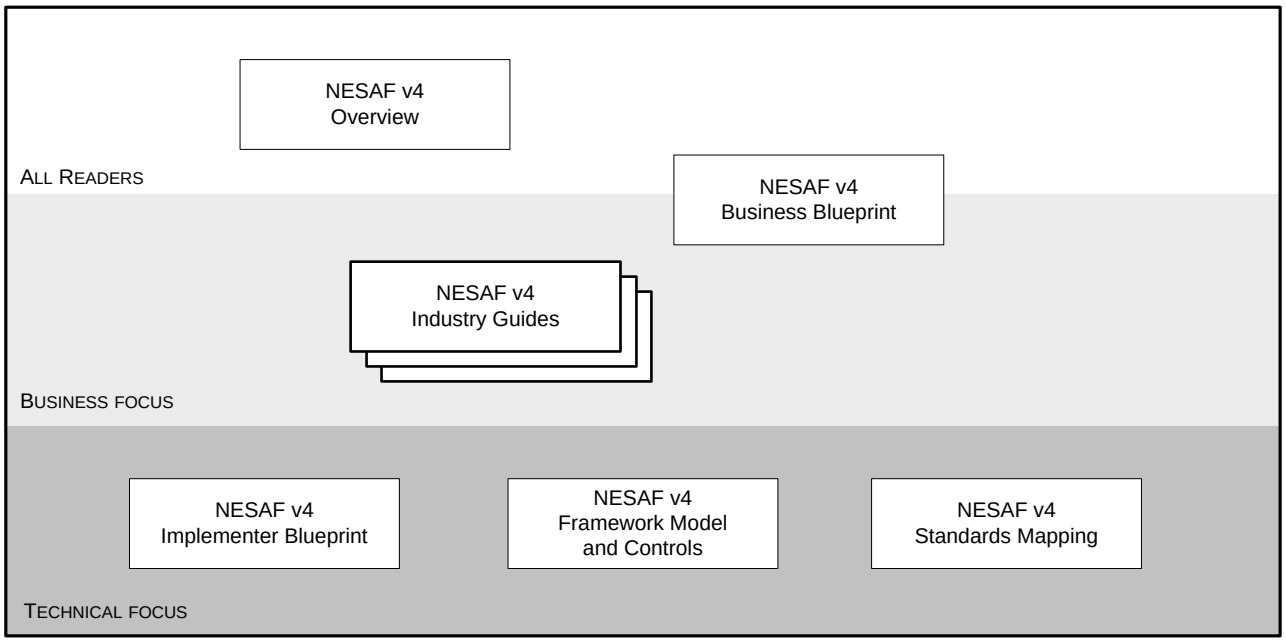
The following stakeholders were involved in the development of this release:

- ICT industry
- information security experts

Audience

NESAF v4 is intended for public and private sector healthcare provider organisations who are seeking information security advice or planning to apply the NESAF.

The document map below shows the focus of the NESAF v4 suite of documents for different audiences. Note that the industry guides are currently undergoing industry consultation before release. (See page 2 for more details.)



Known issues

None known

Support

This release will be supported until 30 June 2016.

For further support or to provide feedback, please email help@nehta.gov.au

Future releases

The following industry guides have been developed for NESAF v4. They are currently undergoing industry consultation and will be published in a future minor release.

Secure Mobile Application Guide for Healthcare Environments

This guide explores the common security pitfalls and risks for healthcare provider organisations that are developing, or planning to develop, mobile applications for their clinical setting. It offers security controls for healthcare provider organisations to consider.

Leveraging industry best practices and existing NESAF principles, this guide provides guidance in areas such as policies, business processes and technological controls. It encourages security early or “built-in” as a feature and considered throughout the system development lifecycle, rather than something that is addressed after a security incident in production.

BYOD Guide for Healthcare Environments

Mobile devices such as smartphones and tablets are used extensively in Australia, leading to an increase in these devices being used in a work environment (bring your own device or BYOD). When used in a healthcare setting, BYOD initiatives enable clinical transformation by allowing resident-based and affiliated clinicians to use their personal devices on the healthcare provider organisation’s internal network to access patient information and communicate with colleagues, care team members and patients, regardless of their physical location.

BYOD enhances clinicians’ communications, streamlines their workflow processes and provides faster access to patient data. It also increases their overall satisfaction because they no longer depend on a desktop computer or fixed location. This consequently broadens the threat landscape to compromise the confidentiality, integrity and availability of the device and the information residing on them.

The guide provides guidance on dealing with the security implications of BYOD devices to manage patient care within a healthcare provider organisation. It provides details aligned to the security controls in NESAF v4 and other best practices resources.

Cloud Guide for Healthcare Environments

Healthcare provider organisations are increasingly looking to make use of information technology to better manage the healthcare information that they collect, use and exchange with other healthcare provider organisations. In order to do this, healthcare provider organisations may need to decide whether to start or continue to develop an in-house information technology capability or make use of out-sourced options such as cloud components.

Cloud computing is a model that enables convenient on-demand network access to a shared pool of computing resources. With it, organisations can access stable powerful computing resources without having to design, build and operate the underlying computing infrastructure themselves.

By using cloud computing, a healthcare provider organisation can concentrate on accessing and using information electronically, with all the benefits that brings with it, without needing specialist skills and capabilities in information technology infrastructure within the organisation. Use of cloud computing can result in significant cost savings for an organisation.

While cloud services offer flexibility, scalability and economies of scale, they have both positive and negative impacts on security that need to be understood. As organisations make use of cloud services, the security risks associated with the organisation’s data will also change. Confidentiality, availability and integrity of this data may be at greater risk if appropriate measures are not put in place. The guide adopts the NESAF approach and provides guidance to healthcare provider organisation to securely transition to cloud services while mitigating risks.

Detailed changes

NESAF v4.0

All documents in the NESAF v4 suite have been substantially updated to remove duplication and better target the intended audience. Each document includes a revised document map and quick reference summary of other documents in the suite. The tables below cover additional document-specific changes.

NESAF v4.0 Overview

Section	Description	Rationale
Title	Revised title. Was “Executive Overview”, is now “Overview”.	The intended audience of this document is wider than expected for an executive summary. The change of name is more reflective of the expected audience.
2.4	Redesigned the NESAF document framework to align more closely. Provided an explanation for each of documents within the framework.	The new document framework illustrates in one diagram the NESAF suite of specifications that can be referenced for users. The diagram is also complimented with a table detailing the description of each specification and their intended audiences as a quick reference.
3.2	Removed the standards-based framework model diagram	Duplication removed as this information is in detail in the implementer and business blueprint documents
3.3	Redesigned the coverage of NESAF controls diagram	To align more closely within a healthcare setting
5	Removed the following sections from the executive overview: 5.0 - Implementer toolkits 5.1 - eHealth process patterns 5.2 - Service descriptions	Duplication removed as this information is detailed in the *Implementer blueprint* and *Business blueprint* documents.
6	Updated references and terms and abbreviations.	New terminologies used are defined to improve readers understanding.

NESAF v4.0 Business Blueprint

Section	Description	Rationale
1	Changed Section 1 to provide a background to eHealth in Australia as opposed to an introduction.	Duplication removed as this appeared in the *Overview* and *Implementer blueprint* documents.
2	Changed Section 2 as the Introduction with purpose, scope, overview, and benefits and target audience. Included the new framework diagram with rewording and paragraph changes.	The new document framework illustrates in one diagram the NESAF suite of specifications that can be referenced for users. The diagram is also complemented with a table detailing the description of each specification and their intended audiences as a quick reference.

Section	Description	Rationale
3	Removed “Structure of the NESAF core framework” diagram and explanation.	Duplication removed as this appeared in the *Overview* and *Implementer blueprint* documents.
3.1	Removed section and diagram (coverage of NESAF controls) addressing a layered approach to security.	Duplication removed as this appeared in the *Overview* and *Implementer blueprint* documents.
3.2	Added standards and framework map diagram and explanation into Section 3.2.	Identifies the primary and secondary standards and government frameworks that were used in the creation of the NESAF.
4.0	Rewording and reworking of sentences in Risk based approach Added NESAF principles diagram to the risk-based approach Figure 4 in version 4 of the NESAF.	Provides better clarity on the cost and benefits of implementing controls that are based on a risk assessment. The benefits proportional to the cost of the controls and the associated risks.
4.1.1 to 4.1.4	Removed useful references.	Duplication removed as this appeared in the *Overview* and *Implementer blueprint* documents.
5.1 to 5.6	Added sections 5.1 “Key elements of an information security policy” 5.2 “Security and access role description”. 5.3 “Asset Classification” 5.4 “Common threats and associated Vulnerabilities”	These sections have been updated and moved from the appendices into the main body of the document to provide better readability and highlight the guidance and tools available to assist with implementation of the NESAF Section 5.4 has been included to provide better guidance and tools to assist in implementation of the NESAF
5.5 to 5.6	Added sections 5.5 “Gap assessment tools” 5.5.1 “Gap assessment scorecard” 5.6 “Risk assessment tools” 5.6.1 “Security risk action plan	These sections have been updated and moved from the appendices into the main body of the document to provide better readability and highlight the guidance and tools available to assist with implementation of the NESAF
6	Removed terms and abbreviations. Added references section.	Provides references to information sourced from external entities or governments for better access directly from the document with no need to reference back to the standards mapping document.
7	Added terms and abbreviations.	New terminologies used are defined to improve readers understanding.
Appendices	Moved into to Section 5.	Better structure and alignment of the document and tools.

NESAF v4.0 Implementer Blueprint

Section	Description	Rationale
Overall	• Updates to all of NESAF controls to reflect the source of control areas such as ISO27001. • Updates to all external links.	Updated controls allow for consistency to the *NESAF Framework and Controls* specification. All external references for readers have been updated to reflect any changes.

Section	Description	Rationale
4.1	Updates to eHealth process pattern “Enrol New Patient at Point of Care”.	Updated consent preferences to accurately reflect the responsibilities required from Healthcare provider organisations as per the Privacy Act. The change also provides implementers added clarity with their responsibility when collecting, using or disclosing health information and the way consent is collected.
5.3	Updates to eHealth process pattern “Register Authorised Employee”.	Changes incorporated to reflect current business scenarios. This is, NASH credentials are not issued to OMO/RO. Instead registered authorised employees such as Organisation Maintenance Officer and Registered Officer are issued with Department of Human Services (DHS) credentials.
4.2	Updates to eHealth process pattern “Record/Update patient consent or preference at point of care”.	Provided clarity on responsibilities for healthcare providers and organisation in the collection, use and disclosure of health information.
4.3	Updates to eHealth process pattern “Search for Patient Record”.	Updated this process pattern to accurately reflect the current processes when searching for patient records against the HI Service.
4.5.2	Updates to eHealth process pattern “Transfer Patient Information”.	Updated sections to the sending of health information electronically to other healthcare by detailing the security threats that may affect this process pattern.
4.6	Updates to eHealth process pattern “Emergency Access”.	Updated to reflect additional mandates as described by the Privacy Act when accessing patient records in an emergency event at a healthcare setting.
5.1	Updates to eHealth process pattern “Register Healthcare Professional”.	The process was updated to reflect a better description of the processes surrounding the request and use of NASH credentials.
5.3	Updates to eHealth process pattern “Register Authorised Employee”.	Provided added clarity for issuance of local or non-national (NASH) credentials to authorised employees i.e. employees of healthcare provider organisations that are not healthcare providers.
7.7.2	Updates to privacy rules from National Privacy Principles (NPP) to Australian Privacy Principles (APP) and the implications to healthcare provider organisations with added responsibility of notifying authorities in the event of a security breach.	Update to the NPP to APP needs to be incorporated as it affects the ways that agencies manage personal information.
7.3.3.3	Updates to registration process for PCEHR to www.my.gov.au.	To reflect the changes to the online registration of a PCEHR.
9	Updates to terms and abbreviations to reflect new terminology.	New terminologies used are defined to improve reader understanding.

NESAF v4.0 Framework Model and Controls

Section	Description	Rationale
2	New section created called “NESAF Controls”.	Help to identify the controls related to NESAF framework.
B.2	Clarified trans-border privacy recommendations.	Update to the NPP to APP needs to be incorporated as it affects the ways agencies manage personal information.
C.2	Clarified health information classification.	Provided additional guidance and clarification to the existing control “notes” section.
F.2	Monitoring added additional information around PCEHR and the rules for tracking and monitoring access.	Update to reflect current PCEHR legislation.
E.1	Clarified and provided examples of secure processing facilities.	Provided additional guidance and clarification to the existing control “notes” section.
E2.4	Provided example of methods to securely destroy removable media.	Provided additional guidance and clarification to the existing control “notes” section.
F4.1	Provided examples of middleware services.	Provided additional guidance and clarification to the existing control “notes” section.
G3	User responsibility added additional information to user responsibility for passwords.	Provided additional guidance and clarification to the existing control “notes” section.
3	Added References section.	Provides references to information sourced from external entities or governments for better access directly from the document with no need to reference back to the standards mapping document.
4	Added terms and abbreviations	New terminologies used are defined to improve readers understanding.

NESAF v4.0 Standards Mapping

Section	Description	Rationale
2.2	Updates to Standards Mapping image to reflect updated standards and guide such as the RACGP. To improve readability a legend has been included to allow users to differentiate between primary, secondary and relevant frameworks.	To reflect new standards and to improve user understanding.
2.4	Moved HB174 to a primary standard.	To remain consistent with standards mapping diagram.
References	Updates to references such as links to external resources.	Ensures all external links referenced are valid.

Previous releases

NESAF v4.0 is derived directly from the previous releases and includes refinements and minor inclusions to improve the value of the product set.

NESAF 3.1

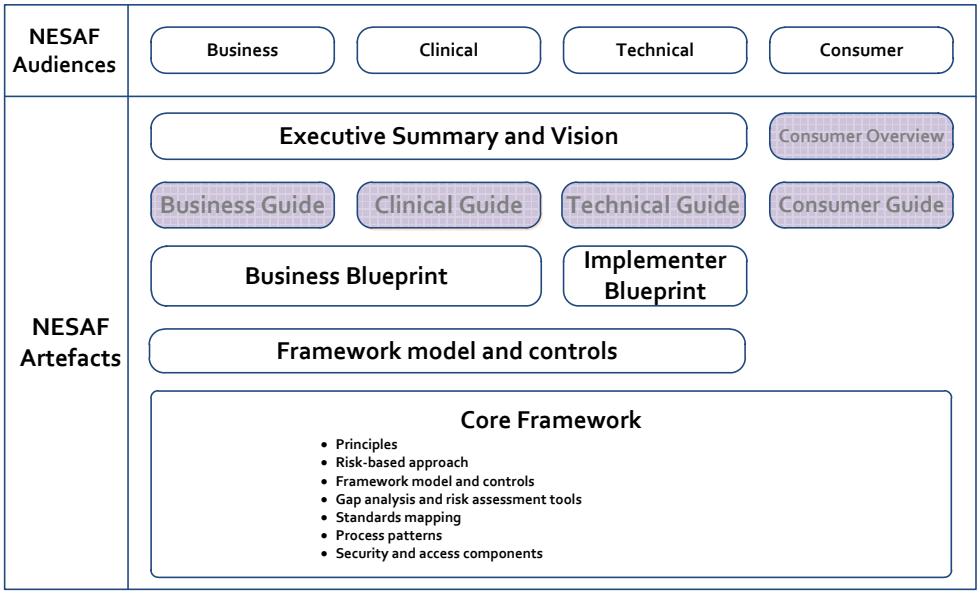
Release rationale

This interim release consolidates stakeholder feedback; lessons learned during application of the framework and carried forward actions from the November 2011 release.

Release inclusions

The March 2012 Release for the National E-Health Security and Access Framework (NESAF) is constructed from the following artefacts:

- NESAF - Executive Summary (S1201) v3.1
- NESAF - Business Blueprint (S1131) v3.1
- NESAF - Implementer Blueprint (S1132) v3.1
- NESAF - Framework Model and Controls (S1720) v3.1
- NESAF - Standards Mapping (S1410) v3.1



Release history

NESAF R3.1 is derived directly from the previous releases and is an interim release to include refinements and minor inclusions to improve the value of the product set.

Stakeholders

The following stakeholders were involved in the development of this release:

- government/jurisdictions
- professionals/clinicians and peak bodies
- healthcare industry associations
- healthcare provider organisations
- ICT industry
- consumer groups
- standards organisations
- information security experts
- privacy and policy groups

Capabilities

- **Additions:** No significant additions have been made that change the form or function of the Product Descriptions.
- **Changes:** Added all accepted level II and Level III changes in accordance with the NESAF Product Management Plan Section 3.3 Changing agreed products and Section 4 Configuration Management - Status Accounting.
- **Removals:** No significant removals have been made that change the form or function of their guidance provided within the NESAF Product Descriptions.
- **Known issues:** NEHTA has identified a number of open issues in this release.

For a detailed list of changes, please refer to the v3.1 release note.

Document date: 6 June 2014

Contact for enquiries
Telephone: 1300 901 001 or email: help@nehta.gov.au