

nehta

NESAF Release 3.1

Release Note

Version 1.0

Approved for release

National E-Health Transition Authority Ltd

Level 25

56 Pitt Street

Sydney, NSW, 2000

Australia.

www.nehta.gov.au

Disclaimer

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. The current revision of this document is located on the NEHTA Web site and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is of the latest revision.

Security

The content of this document is confidential. The information contained herein must only be used for the purpose for which it is supplied and must not be disclosed other than explicitly agreed in writing with NEHTA.

Copyright © 2011 NEHTA.

This document contains information which is protected by copyright. All Rights Reserved. No part of this work may be reproduced or used in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems—without the permission of NEHTA. All copies of this document must include the copyright and other information contained on this page.

Document control

Name of document:	NESAF R3.1 – Release Note
Document owner:	National E-Health 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
1.0	20120330	NESAF Team	Version 1.0 Approved for release

Document publication

Publication:	<input checked="" type="checkbox"/> Internal <input checked="" type="checkbox"/> External <input checked="" type="checkbox"/> Public
Published version and date:	<p>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.</p>

This page is intentionally left blank

Table of contents

1	Summary	7
1.1	Background.....	7
1.2	Release rationale	7
1.3	Acknowledgement.....	7
1.4	Scope.....	7
1.5	Package inclusions	7
1.6	Release history.....	8
1.7	Stakeholders	8
1.8	Audience	8
2	Capabilities.....	9
2.1	Additions	9
2.2	Changes	10
2.3	Removals.....	12
2.4	Known issues	12
3	Support	14
4	Future releases.....	15

This page is intentionally left blank

1 Summary

1.1 Background

The purpose of the Security and Access Programme is;

- To deliver the prime objective of a common approach to information access that cultivates a network of trust between all participants in a patient's healthcare journey.
- To inform and provide a holistic national approach to enhancing information access and security better practices for Australian eHealth solution designers (incl. NEHTA), implementers and healthcare organisations.

1.2 Release rationale

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

1.3 Acknowledgement

NEHTA is thankful to the contributors and reviewers of the National E-Health Security and Access Framework, including the participants of our domain focus groups covering issues for Consumers, Clinicians and Healthcare Professionals, Policy and Privacy, Vendors, Government and NEHTA Work Programmes, and in particular to our joint working group (based on domain focus group representation); the NEHTA reference groups and NEHTA's Clinical Leads.

The NESAF Programme wishes to acknowledge the Department of Health and Aging sponsorship of the NESAF tranche 3 as well as the continued, guidance and efforts of the National Health CIO Forum in supporting the development of this work.

Through your contributions and deliberations this framework acts as a guide to developers and implementers of e-health solutions and ensures the various security control and personal health information access aspects of these solutions can be suitably addressed in design and operation.

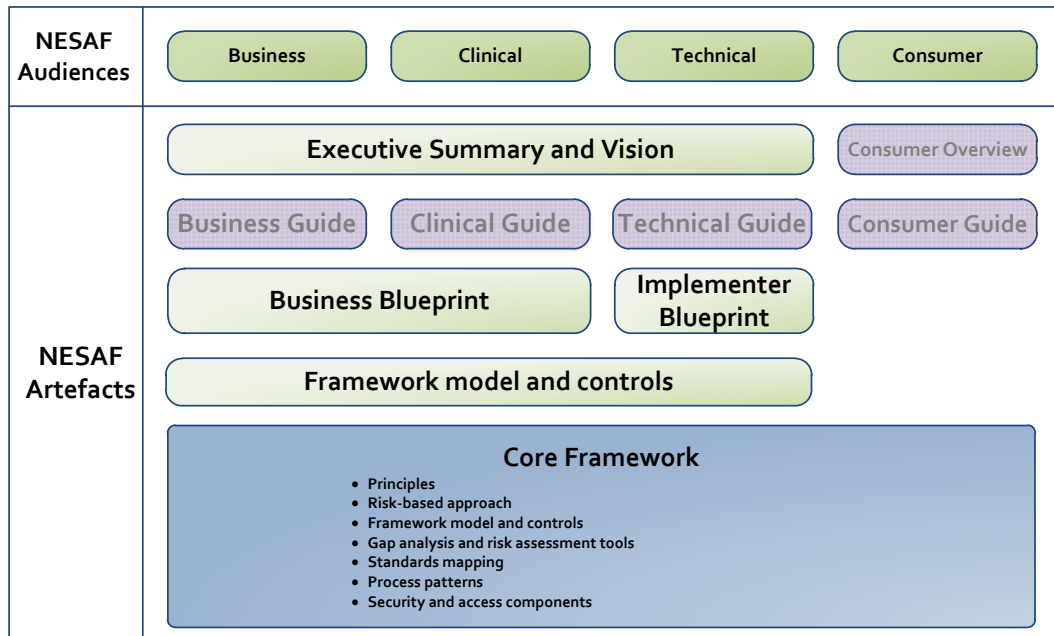
1.4 Scope

These notes cover the additions, changes and removals since Release 3 was published in November 2011

1.5 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



1.6 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.



1.7 Stakeholders

The following stakeholders have been involved in the development of this release:

- Government/Jurisdictions
- Professionals/Clinicians and Peak Bodies
- Healthcare Industry Associations
- Healthcare Organisations
- ICT Industry
- Consumer Groups
- Standards organisations
- Information Security Experts
- Privacy and Policy Groups
- Internal Stakeholders

1.8 Audience

- All public and private sector healthcare business that have information or connectivity traceability to national systems.

2 Capabilities

2.1 Additions

No significant additions have been made that change the form or function of the Product Descriptions.

Document	Section	Feedback	Condition	NESAF Comments	Status
Business Blueprint	2.1	Comment in the intro that as a rule security controls are currently “inwardly” organisational centric focussed. The NESAF looks at it more holistically	Accepted	Included into last sentence, 2nd paragraph of section 2.1	Implemented.
Business Blueprint	Figure 7	Include “Staff” as a human asset (Will require specific clarification on the exact boundaries of this)	Accepted with Conditions	Amended to include staff. Needs confirmation from team.	Implemented.
Business Blueprint	6	Include ‘Privacy’ def, include ‘Clinical Safety’ def in the context of this framework	Accepted	Wording provided by privacy team	Implemented.
Business Blueprint	B.1.4	Special interest groups – in the instance of this – groups like RACPG are useful to cite	Accepted	Initial references expanded on, future analysis will be conducted to create a document similar to the standards mapping	Implemented.
Business Blueprint	3.1	Section should cover goals, expectations and principles. Break the patient and provider expectations out of the principles and place them in their own discussion point alongside a discussion of ICT vendor and government expectations.	Accepted	FIXED. (Partially) Restructured as per comment with a clearer relationship of INFOSEC goals, with expectations and NESAF principles. ICT and Government expectations were not added. This is therefore a new stakeholder consultation point.	Implemented.

Implementer Blueprint	7.3.3.1	"An entity may have several identities, which may be at different levels of trust and invariably for many different trust systems. Normally the entity has fewer "Trusted Identities" and often these trusted identities are linked to the system identity." It may be worth adding some privacy discussion here.	Accepted	A sentence is to be added at the end of the paragraphs under the 'summary' heading: It is recognised that the goals of privacy (e.g. providing anonymous care where it is lawful and practicable to do so) need to be balanced against practicalities of associating health care information with an individual (i.e. through the use of a Healthcare Identifier).	Implemented.
Standards Mapping		New standards to be referenced.	Accepted	ISO/IEC 24760 Information technology - Security techniques - A framework for identity management. ISO/IEC 9798 (all parts), Information technology - Security techniques - Entity authentication. ISO/IEC 291014 Information technology - Security techniques - Privacy reference architecture. ISO/IEC 291155 Information technology - Security techniques - Entity authentication assurance framework.	Implemented.

2.2 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.

Document	Section	Feedback	Condition	NESAF Comments	Status
Business Blueprint	4.1.4	Second last paragraph – call out the volume of exchanges of information, and with a varying number of potential health organisations and practitioners.	Accepted	Consensus agreed and change incorporated	Implemented.
Business Blueprint	B.1.3	In relation to health – in conf. agreement – need to think about the privacy Act – relevant to your	Accepted	Additional guidance provided	Implemented.

Document	Section	Feedback	Condition	NESAF Comments	Status
		justification / State. Need to talk about the expectations for appropriate handling and disclosure.			
Business Blueprint	H.2.3.	"It should be possible to amend" – in the CBR workshop we were advised that you cannot amend errors of information legally around a patient. Just needs to have amended removed and this made clear.	Accepted	Remove 'amend or' from the first sentence. This change also goes into all other references made to H.2.3. This means framework model and controls + implementer blueprint.	Implemented.
Business Blueprint	3.2 and 5.0	To increase useability and ease of locating key reference documents, i.e. '[NEHTA2011B] to NEHTA framework model and controls and [NEHTA2011A] as the Implementer Blueprint. Can the url be included into the reference table?	Accepted	Updated references for implementer, business blueprints + framework and controls to the Vendor portal. This was verified with OW.	Implemented.
Implementer Blueprint	6.5.3	Is there an appropriate component to capture data quality? Merging is a data quality sensitive activity. Data quality is not directly within scope of the framework. However, to best bridge this relationship NESAF Team will endeavour to undertake the following: (NESAF blueprints to include a blurb surrounding data quality measures. This will help bridge the gap between the out of scope dilemma)	Accepted with Conditions	FIXED. Updated Section 6.5.2	Implemented.

Document	Section	Feedback	Condition	NESAF Comments	Status
Implementer Blueprint	7.3.3.3	I am a bit concerned with the definitions and alignment with NeAF here. High does not allow for what AHPRA does, since it uses GSEF for new registrations. 100-point is not even equivalent to Moderate in NeAF since 100-point does not guarantee both a photo and hand signature specimen. NeAF 3 (Moderate) is Gatekeeper General Category EOI requirements.	Accepted	FIXED Aligned with NeAF Updated references to standards	Implemented.

2.3 Removals

No Significant removals have been made that change the form or function of their guidance provided within the NESAF Product Descriptions.

2.4 Known issues

NEHTA has identified the following open issues in this release:

Document	Section	Feedback	Condition	NESAF Comments	Status
Framework Model & Controls	J.1.1	Given we are talking about lessons learnt, should there also be a "People" aspect?	Accepted	In NESAF 3.x the controls include a control type (people, process, technology) and responsibility domain (Business, Information Technology, Clinical) which provides a level of granularity to relating controls to the "People" aspect. The NESAF Taxonomies and Classification project will address these concerns initially	Deferred to next release, Release 4.0
Implementer Blueprint	7.4.2.5 and 7..4.6	G.2.3: Object capability based access control is not mentioned yet provides the most provably secure access control model.	Accepted	FIXED Include/rework content using some of the text in the comment The NESAF Taxonomies and Classification project will address these concerns initially	Ready for team review.

Document	Section	Feedback	Condition	NESAF Comments	Status
Implementer Blueprint	4.1.3	Will there be an Enrol patient online or via another entry point?	Accepted	DEFERRED, has wide ranging implications to all process patterns where authentication occurs and the need to separate people actors from system actors is required. The NESAF Taxonomies and Classification project will address these concerns initially	Deferred to next release, Release 4.0
Implementer Blueprint	4.2.3	Authentication/Authorisation/Access Control/session-context should feature here since the staff member needs to access system/records to perform their function. There are actually two "Authenticate Authorised User" sub-processes required here, one for the provider organisation user, and another for the patient since the org user needs to first ensure the patient is who they say they are before modifying consent directives.	Accepted	DEFERRED, has wide ranging implications to all process patterns where authentication occurs and the need to separate people actors from system actors is required. The NESAF Taxonomies and Classification project will address these concerns initially	Deferred to next release, Release 4.0

3 Support

“NEHTA’s support strategy provides support based on major releases.

Version 3.1 of the National E-Health Security and Access Framework will be supported by NEHTA for two (2) years from the date of its release as a NEHTA Managed Publication.

To obtain support please contact feedback.saf@nehta.gov.au

4 Future releases

The core framework will now go into service operations, the Security and Access Programme will now undertake a series of supporting project aimed at broadening the application capabilities of information security for eHealth through the development of:

- Information Security Taxonomies;
- Asset Valuation and Classification schemes;
- E-Health Misuse Cases.

The creation of a core information security competency within NEHTA will also allow for a range of projects to be undertaken in support of design, development and implementation initiatives within the eHealth scape.