Australian Government
Australian Digital Health Agency

National Secure Messaging Network Conformance Profile

24 February 2025 v1.0

Approved for external use

Document ID: DH-4111:2025

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000
Telephone 1300 901 001 or email help@digitalhealth.gov.au
www.digitalhealth.gov.au

Acknowledgements
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.

Disclaimer
The Australian Digital Health Agency ("the Agency") 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. The Agency 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.

OFFICIAL

Document information

Key information

Owner Branch Manager – Connected Care Branch, Digital Solutions Division

Contact for enquiries Australian Digital Health Agency Help Centre
Phone 1300 901 001
Email help@digitalhealth.gov.au

Table of contents

1 Introduction

The National Secure Messaging Network (NSMN) is a national standards-based network of interoperable systems to allow any healthcare provider in Australia to discover other healthcare providers and securely deliver clinical messages to them.

The Agency seeks to ensure that NSMN participants can communicate with one another consistently, effectively, and securely through the application of this conformance profile to all NSMN systems.

1.1 Purpose

This document outlines the conformance requirements that apply to all software products that participate in the NSMN. The NSMN Blueprint [AGENCY2023a] defines 4 distinct NSMN system types:

- Client System (collectively the Sending System and Receiving System)
- End Node (collectively the Sending Edge and Receiving Edge nodes)
- Core Node
- Provider Directory

There are specific conformance requirements that apply to each of the NSMN system types as well as requirements that apply to all participating software products.

1.2 Intended audience

This document is primarily intended for software vendor organisations and service providers implementing the NSMN in their software products, and their software developers. Additional audiences include:

- NSMN Governance Committee
- NSMN Technical Working Group.

1.3 Scope

This document is limited to defining conformance requirements for software products that participate in the NSMN for secure message exchange. Any additional requirements for software products that are unrelated to secure message exchange via the NSMN are out of scope.

This document does not cover usability or commercial aspects of participating software products or their participation in other programs and digital health initiatives.

This conformance profile is applicable to the roles that are defined in the NSMN Blueprint [AGENCY2023a]:

- Core Node
- Sending Edge Node
- Receiving Edge Node
- Sending System
- Receiving System

- Provider Directory.

2 Relevant Specifications

This conformance profile relates to the NSMN Interoperability Specification [AGENCY2023b]. NSMN participants are required to implement the Interoperability Specification as well as the requirements in this conformance profile.

3 Conformance Requirements

The Client System role encompasses both the Sending System and the Receiving System which are typically functions of a Clinical Information System.

Similarly, the End Node role encompasses both the Sending Edge Node and the Receiving Edge Node.

Refer to the *National Secure Messaging Network Blueprint* [AGENCY2023a] for the architectural description of the NSMN roles.

In this conformance profile, requirements are defined for each discrete role, to cater for the scenario where a software product may perform only one system or node role rather than both e.g a product may be a Sending System but not a Receiving System. This document refers to “the system” and the system will be one or more of these roles.

Software products must conform to the requirements for each of the roles that they implement and perform.

Requirements follow a standard form, utilising the following language:

SHALL: When appearing in a conformance requirement, the verb SHALL indicates a mandatory requirement. Its negative form SHALL NOT indicates a prohibition.

SHOULD: When appearing in a conformance requirement, the verb SHOULD indicates a recommendation. Its negative form SHOULD NOT indicate an option that should not be supported.

MAY: When appearing in a conformance requirement, the verb MAY indicates an optional requirement.

Content of requirements defined as ‘*Notes’* provides context and implementation guidance only and does not form part of the normative requirement.

Number	Requirement	Applicability					
		Sending system	**Receiving system**	**Sending edge**	**Receiving edge**	**Core node**	**Provider directory**
20	**Personal data in error messages** Error messages intended to be displayed to a user SHALL NOT include patient personally identifiable data in the error message. *Notes: privacy conventions require patient personal details are not disclosed in error messages.* *Back-end systems and systems designed to run unattended that do not display error messages automatically conform to this requirement.* *Error messages shared with downstream systems need to conform to this requirement.*	Yes	Yes	Yes	Yes	Yes	Yes
30	**Error message details** Error messages intended to be displayed to a user SHALL provide sufficient detail for the user to understand the error condition, differentiate it from other error conditions, and have sufficient information to be able to take corrective action. *Notes: error messages need to contain sufficient details for a user to understand the error and to take corrective action. Insufficient details may result in delivery delays which may have a clinical impact.* *Back-end systems and systems designed to run unattended that do not display error messages automatically conform to this requirement.* *Error messages shared with downstream systems need to conform to this requirement.*	Yes	Yes	Yes	Yes	Yes	Yes

Number	Requirement	Applicability					
		Sending system	**Receiving system**	**Sending edge**	**Receiving edge**	**Core node**	**Provider directory**
40	**Audit log** The system SHALL record events in an audit log. Events include all interactions with secure messaging systems, including transmissions and error messages sent and received. The audit log SHALL record, but not restricted to: • event type • event date • event time • sender endpoint information • recipient endpoint information • message identifier(s) *Notes: an audit trail may be used in technical fault identification and provide evidence about point of failures etc.* *Endpoint information that may be the systems own endpoint needs to be included in the audit log as this contributes to the completeness of the audit log.*	Yes	Yes	Yes	Yes	Yes	Yes
25	**Personal data in audit log** Data captured in an audit log SHALL NOT include patient personally identifiable information. *Notes: IHI's and other identifiers are personal information and must not be stored in audit logs.*	Yes	Yes	Yes	Yes	Yes	Yes

Number	Requirement	Applicability					
		Sending system	**Receiving system**	**Sending edge**	**Receiving edge**	**Core node**	**Provider directory**
45	**Audit log access** The system SHALL ensure the audit log can only be accessed by an authorised person. *Note: Access to the audit log must be restricted to prevent unauthorised viewing or modification of the audit log.*	Yes	Yes	Yes	Yes	Yes	Yes
50	**Visual alerts** The system SHALL have a means to visually alert a user that a message or notification has been received. *Note: A received message or notification can be unnoticed in a user's inbox. This lack of awareness of the existence of message may result in delays in actioning a time critical message. A mechanism to alert the user of a message or notification would assist in minimising a potential delay.* *The mechanism might be a message box, background text or message or icon on the screen or system tray.* *The user and the addressee might be different people, especially if the user is a receptionist or personal assistant but the addressee is a healthcare provider. See the glossary for more information about roles and actors.*	Yes	Yes	N/A	N/A	N/A	N/A
60	**Message preview** The system SHOULD provide a preview of the message payload prior to sending the secure message. *Note: Providing a message preview gives the user a chance to ensure the message and recipient are correct and as intended.*	Yes	N/A	N/A	N/A	N/A	N/A

Number	Requirement	Applicability					
		Sending system	**Receiving system**	**Sending edge**	**Receiving edge**	**Core node**	**Provider directory**
100	**Interoperability Specification - general** The system SHALL conform to the following requirements and solution constraints contained in the Interoperability Specification that describe the behaviour of "General RSC": • section 3.9	Yes	Yes	Yes	Yes	Yes	Yes
110	**Interoperability Specification – roles** The system SHALL conform to the sections in the Interoperability Specification that are relevant to roles the system performs. *Note: the system needs to conform to the relevant sections 3.3 -> 3.8 and will depend on the roles of the system.*	Yes	Yes	Yes	Yes	Yes	Yes

Acronyms

Acronym	Description
NSMN	National Secure Messaging Network
RSC	Requirement Solution Constraint (as documented in the Interoperability Specification)

Glossary

Term	Meaning
Addressee	The person or organisation that is intended to read and digest the information in the message. The Receiving System is used by the message recipient and uses internal processes to ensure the information in the message is routed to the addressee, who may also be the recipient. The addressee benefits from the NSMN but sits external to the NSMN. The addressee cannot be a system or software product.
Core Node	A system responsible for exchanging Sealed Messages securely with other Core Nodes in the NSMN and providing message sending and receiving services for their connected Edge Nodes. A Core Node is also responsible for maintaining and exposing a Provider Directory containing address information for its Receiving Edge Nodes.
Message recipient	The user of a receiving system. The message recipient is the first person to read a secure message. The message might be intended for an addressee that may or may not also be the message recipient.
Provider Directory	An electronic directory of healthcare providers and associated entities that conforms to the Australian Provider Directory Implementation Guide (PD 2) specification.
Receiving Edge Node	The interface between the internal information systems used by a message recipient and a Core Node. A Receiving Edge Node is a delivery point in the NSMN with a logical address where a Sealed Message containing a Clinical Message or Acknowledgement Message can be received. After receiving a Sealed Message from a Core Node, Receiving Edge Nodes decrypt them, check their digital signature, and transmit their Payload to the Receiving System directly or via Relay System(s). A Receiving Edge Node is represented in a Provider Directory by one or more Endpoint entries.
Receiving System	An information system used by a message recipient. It is responsible for processing messages received via the NSMN and making their content available to message recipients so that related business processes can be executed.

Term	Meaning
Sending Edge Node	The interface between the internal information systems used by a message sender and a Core Node. The Sending Edge Node receives payloads (Clinical Messages or Acknowledgement Messages) to transmit from a Sending System or Relay System. A Sending Edge Node is responsible for signing, encrypting, and transmitting the payload, inside a sealed message, to a Core Node. A Sending Edge Node is also a delivery point in the NSMN with a logical address where a Sealed Message containing a Final Transport Response can be received.
Sending System	An information system used by a message sender for the creation, management, and release of messages to be transmitted via the NSMN.
User	A person (not a device) that uses a system in the NSMN. Includes healthcare providers, system administrators etc.

References

[AGENCY2023a] *National Secure Messaging Network Blueprint*, Australian Digital Health Agency, 2023

[AGENCY2023b] *National Secure Messaging Network Interoperability Specification,* Australian Digital Health Agency, 2023