Australian Government
Australian Digital Health Agency

National Secure Messaging Network Conformance Assessment Scheme

6 March 2025 v1.0

Approved for external use

Document ID: DH-4109:2025

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000
Telephone 1300 901 01 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 Executive Summary

In recent years, the Australian Digital Health Agency (the Agency), and its healthcare industry partners have been progressing towards the development of the National Secure Messaging Network (NSMN). The NSMN will enable reliable and secure electronic communication between Australian healthcare providers. The Agency is cognisant of the risks posed with non-secure messaging for clinical documents, and the need to have an interoperable system underpinning these communications. Based on a set of national and international standards, the NSMN defines a messaging solution that can be implemented by Clinical Information Systems (CIS) to enable interoperable exchange of clinical documents such as referrals, specialist letters and discharge summaries between healthcare providers.

The NSMN is formally defined by the Conformance Assessment Scheme (the Scheme) and governed by a NSMN Governance Committee. The committee is a voluntary, cooperative body made up of representatives from clinical peak body groups, jurisdictions, secure messaging vendors, clinical information system vendors and others with a drive to make secure messaging a successful, widely adopted and highly valued capability of the Australian healthcare industry.

The Scheme is a set of requirements and conformance assessment documents and processes that underpin the NSMN. It specifies the NSMN and provides the means for parties considering participating in the NSMN to clearly understand how they can do so, the capabilities required of their systems, and how they can demonstrate solution readiness. The NSMN proposes 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. Software developers participating in Secure Messaging are required to implement the Agency's NSMN Interoperability Specifications as well as the requirements in the NSMN Conformance Profile.

In administering this Scheme, the Agency delivers a conformance service that seeks to ensure the safe and secure use of the NSMN service by all participating software products and systems, through conformance assessment against the Interoperability Specifications and standards.

The following documents form part of the Scheme.

- The NSMN Blueprint [AGENCY2023a] outlines the NSMN solution and defines the NSMN roles.
- The NSMN Interoperability Specification [AGENCY2023b] details the technical requirements that underpin the NSMN. The Interoperability Specification Requirements are structured around the Blueprint solution roles.
- The NSMN Conformance Profile [AGENCY2025a] defines the conformance requirements for systems performing each of the six roles that are described in the NSMN Blueprint.

2 Introduction

2.1 Purpose

2.1.1 Purpose of document

The purpose of this document is to describe the process for assessing vendor systems conformance to the relevant specifications for participating in the NSMN. This document also describes the establishment and operation of the Scheme, under which NSMN participants will be assessed for conformance with the Agency's defined standards.

2.1.2 Purpose of Scheme

The Scheme describes the conformance assessment policies and processes administered by the Agency, to ensure that healthcare providers operating within the network are adhering to required standards. It describes the artefacts, including software and documentation that are produced by the Agency to support conformance assessment activities.

2.2 Scope

The scope of the Scheme is for testing the conformance of systems participating in the NSMN, particularly systems playing one or more of the roles described in the NSMN Blueprint.

The scope of the project may encompass requirements and roles described in the NSMN Interoperability Specification. These are as described under section 3.3 Objects of conformance assessment.

The scheme will guide the developer in understanding the complete conformance landscape for Secure Messaging.

2.3 Out of Scope

This document does not describe technical specifications or conformance requirements. The NSMN Interoperability Specification is published by the Agency and the conformance requirements are contained in the NSMN Conformance Profile.

The scope does not include any conformance activities in relation to other interrelated Agency programs, products, and services including, but not limited to: My Health Record (MHR), Healthcare Identifier (HI) service, and National Authentication Service for Health (NASH), Provider Connect Australia (PCA).

2.4 Intended audience

This document is intended for vendors implementing software that participates in the NSMN:

- Software developers participating in the NSMN

2.5 Contact details

Email: help@digitalhealth.gov.au

3 Requirements for conformance assessment

3.1 The approach to conformance testing

The NSMN conformance requirements have been created to assist software developers to design and develop software products and systems that:

- conform with applicable specifications and standards when connecting to and interacting with other participating software products and systems.
- conform with applicable specifications and standards when transmitting using secure message solutions.
- mitigate clinical safety, privacy, cyber security, policy and legal risks.

Responsibility for ensuring information systems participating in the NSMN have the required capabilities and are appropriately tested remains with the software developer.

3.2 Conformance domains

Logical functional groups of conformances requirements are described in the NSMN Blueprint [AGENCY2023a] and shown in the diagram below.

Main logical application components of the NSMN that interact with each other in delivering a service:

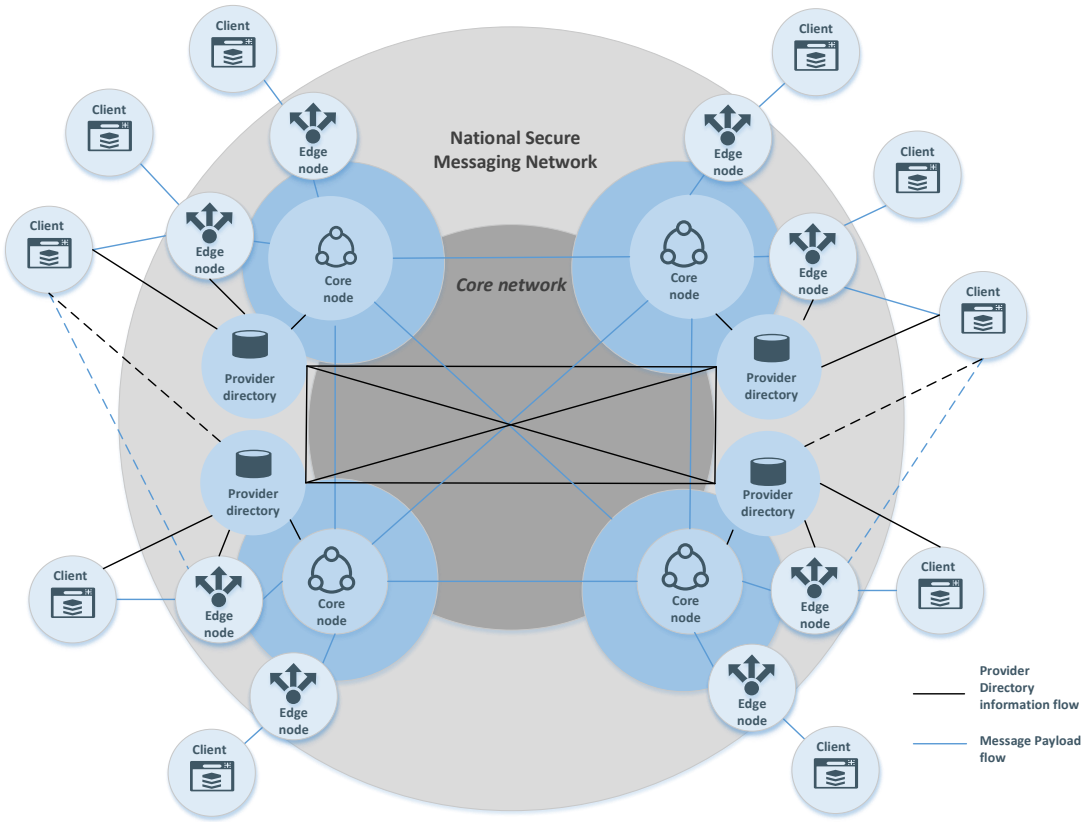

Figure 1 - NSMN Roles

Note:

1. *Participating CIS typically play both the Sending System and Receiving System roles. They are shown as "Client" in Figure 1.*
2. *Participating Edge Node systems typically play both the Sending Client and Receiving Client roles. They are shown as "Edge Node" in Figure 1.*
3. *Clients may have relationships and use more than one Edge Node to send and receive messages (although overtime it is expected that this flow will become redundant)*

3.3 Objects of conformance assessment

This Scheme applies to all NSMN participants that connect to interact with other participating software products and systems to transmit using secure messaging solutions. Software products may include CIS and other systems used by providers in the management and delivery of their care services.

These roles are defined in the NSMN Blueprint [AGENCY2023a].

- Sending System
- Sending Edge Node
- Core node
- Receiving System
- Receiving Edge Node
- Provider Directory

3.4 Relevant technical requirements

Relevant specifications for a software system participating in the NSMN network are listed in the following documents:

1. NSMN Blueprint [AGENCY2023a]
2. NSMN Interoperability Specification [AGENCY2023b]

3.5 Conformance requirements

Objects of conformance are expected to satisfy the mandatory and applicable conditional conformance requirements specified in all the conformance profiles that are applicable to the object of conformance.

4 Testing conformance to the specifications

4.1 Conformance assessment

The NSMN Conformance Assessment Scheme is a set of requirements and processes that underpin the NSMN. It provides the means for parties considering participating in the NSMN to clearly understand how they can do so, the capabilities required of their systems, and how they can demonstrate solution readiness.

Conformance, which relates to how products and services implement NSMN specifications, is conducted through self-assessment by the party implementing the software systems.

4.2 Conformance technical tools

Developer and testing tools for the NSMN can be found on the Agency's Developer portal:

- Clinical Package Validator - Tool to check conformance of HL7 messages, Packaged CDA documents and SMD messages.
- FHIR Provider Directory - Environment to test the conformance of a provider directory with the HL7 Australia Provider Directory FHIR Implementation Guide.

4.3 Success criteria

To claim conformance against the requirements of a conformance profile, the following criteria must be met:

The implementation under test must support the mandatory requirements, and any conditional requirements that are applicable to the implementation under test, in the relevant conformance profile.

4.4 Declaring conformance

Prerequisites for declaring the conformance of an implementation are:

- Self-testing is successful.
- A developer may then submit a Declaration of Conformance, to formally declare the conformance of their implementation. Submission of a Declaration of Conformance and supporting documentation to the Agency is evidence of completion of the conformance self-testing process and is necessary for the software product to be granted participation in the NSMN.

5 Ongoing validity of conformance

5.1 Conformance and implementation versioning

If the conformance requirements are superseded by a later version of the Interoperability Specification, then the vendor must declare conformance with the newer version as per terms of the NSMN Managed Operating Deed.

Conformant software products or systems may be required to undergo further conformance assessment if software version changes materially impact the way the software product or system interacts with the NSMN systems and interfaces.

5.2 Obligations for reassessment

The Declaration of Conformance outlines a series of obligations for organisations developing conformant software products, including circumstances in which a software product is required to be reassessed for conformance.

A software product may need to be reassessed for conformance if:

- there is a material change to the software product's NSMN system specific functionality.
- there is a material change to the NSMN system interfaces that it consumes.
- a new version of either this Scheme, or an Interoperability Specification, or a Conformance Profile, or a Conformance Test Specification is released.

5.3 Validity period

A Declaration of Conformance for an implementation has no expiry date. However, the declaration only applies to the version of the implementation, and version of the applicable Conformance Profile and Interoperability Specification, identified in the Declaration of Conformance.

A new Declaration of Conformance may need to be executed if an obligation for reassessment is triggered.

6 Scheme operations

6.1 Document version maintenance

The Agency has discretion to revise existing conformance profiles and technical specifications, and develop new conformance profiles and test specifications, under this Scheme from time to time. This activity may be undertaken periodically as a standard review process, in response to an incident or identified issue, or in response to a change in operating context – for example, a change to a risk or threat assessment.

It is recognised that organisations may be a considerable way into their development cycle when a new version of a profile is released. The timeframe within which conformance with the new profile is required to be achieved, shall be nominated at the time it is published, if applicable. The timeframe specified shall endeavour to provide all participating organisations reasonable time to achieve conformance and reasonable time for Provider organisations to upgrade to the new conformant versions of software products. If there are specific clinical safety or security aspects that require immediate redress, the Agency shall negotiate the required conformance timeframe with participating organisations.

It is recognised that participating Provider organisations may at times be operating versions of software products that are not the most current. Where a conformance profile is updated, the Agency may request that organisations provide advice regarding whether any prior versions of their software product still in use are conformant or non-conformant with the new profile. Where it is identified that participating Provider organisations are continuing to operate non-conformant software products or systems, a grace period shall be determined, after which the old versions shall be removed from the conformance register as per the NSMN Managed Operating Deed.

6.2 Issue detection

Issues can be detected through system monitoring, analysis, and direct reports made to the Agency. Issues may relate to system interactions, data quality, cyber security, end user or organisation workflows, or other anomalous aspects of the software product or system.

Issues can be reported by a range of sources, including:

- end users of the software product or system
- software organisations and software developers

6.3 Issue remediation

Software developers may be contacted by the Agency regarding identified instances of alleged non-conformant software behaviour. If requested, the obligation to provide evidence of past conformance rests with the Agency and current conformance rests with the software developer.

When there is agreement that non-conformance exists and needs to be addressed, the type and nature of the remediation required, the timeframe for remediation, and any interim risk-mitigation activities will be agreed between all relevant parties as per the NSMN Issue Management Plan.

6.4 Issue escalation

The Agency will work collaboratively with organisations that develop software products to resolve conformance issues in a timely manner as per the NSMN Issue Management Plan.

Acronyms

Acronym	Description
CDA	Clinical Document Architecture
CIS	Clinical Information Systems
CTS	Conformance Test Specification
FHIR	Fast Healthcare Interoperability Resource
HI	Healthcare Identifier
MHR	My Health Record
NASH	National Authentication Service for Health
NSMN	National Secure Messaging Network
SMD	Secure Message Delivery

Glossary

Term	Meaning
The Agency	Australian Digital Health Agency
The Scheme	Conformance Assessment Scheme
Provider system	The software product or system(s) used by a provider organisation in the care setting. Software products may include Clinical Information Systems (CIS) and other systems used by providers in the management and delivery of their care services
User	A user is any person who accesses a Provider System, typically an employee of the provider organisation

References

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

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

[AGENCY2025a] *National Secure Messaging Network Conformance Profile*, Australian Digital Health Agency, 2025