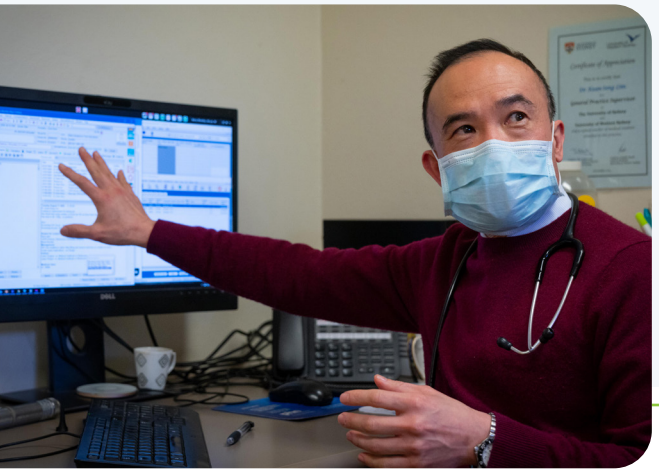
Interoperability case study



# Secure messaging

## Overview

Reliable, secure provider-to-provider communication is a key component of digitally enabled, integrated and coordinated care across the Australian health sector. Secure messaging is a core foundational capability required to enable interoperability and safe, seamless, secure and confidential information-sharing across all healthcare providers.

Although secure messaging has been used in the healthcare ecosystem for many years – with pockets of success – fragmented system vendors restricted the use of secure messaging. This led to significant challenges across these key areas:

- **Message structure and standardised content formats** – the implementation of secure messaging across the sector was not consistent as standards were interpreted and implemented in different ways.
- **Use of commercial security certificates** – secure messaging systems did not recognise other clinical information system (CIS) vendors' authentication.
- **Adoption drivers** – due to differing commercial imperatives and a lack of an accreditation scheme, there is no incentive for CIS vendors to adopt secure messaging standards or, where they choose to do so, there are no means to assess their conformity to standards.
- **Message acknowledgements** – the sender did not always know if their message was received as application acknowledgements were not always consistent.
- **System complexity** – there were too many steps in the process to send a message and it was difficult to use for the end user.
- **Access to reliable provider address information** – it was difficult to access up-to-date information about service providers, impacting confidence that the message was sent to the right clinician.

The secure messaging program was established by the Agency to disrupt the current landscape by executing change and encouraging adoption of the solution across the sector by providing standards, support and guidance for providers to overcome existing barriers to adoption and provide implementable solutions.

One of the key initiatives developed under this program was a set of specifications called Secure Message Delivery (SMD), developed in collaboration with Standards Australia, desktop software vendors and secure messaging service providers. This set of specifications defines a national approach to digital health communication using widely supported IT industry standards.

## Progressing interoperability

In July 2018, the Agency published Australia's National Digital Health Strategy which included a strategic priority that, by 2022, every healthcare provider would have the ability to communicate with other professionals and their patients via secure digital channels, thereby ending the dependence on paper-based correspondence and the fax machine or post.

To support this priority, the Agency released a Secure Messaging Industry Offer which aimed to have functionality available in software suppliers' production environments by June 2021.



Australian Government
Australian Digital Health Agency

This solution aims to accelerate the implementation of:

- FHIR API-federated lookup of healthcare providers
- HL7 standard message payload envelopes
- acknowledgement (ACK)
- NASH SHA2 certificates (as SHA1 is no longer supported from 2022)
- management of the expiry dates of the certificates (notifications).

The SMD program collaboratively defined message payload standards for eReferrals, specialist letters and discharge summaries which, when adopted by CIS and secure messaging vendors, ensures that documents that are sent and received are conformant to those standards, driving interoperability across the healthcare system.

A register of SMD-compliant products enables healthcare provider organisations to procure secure messaging software that is conformant with national digital health and SMD requirements.

# Scope and objectives

The broader objective of the program is to drive connection across the network, enabling vendors and healthcare providers to seamlessly communicate and exchange clinical information through the ubiquitous use of secure messaging.

Throughout 2019, a significant amount of stakeholder consultation and analysis was conducted to evaluate how the program had performed thus far, and what could be done to further drive the objectives of the program. The following eight key initiatives were identified to accelerate the adoption of secure messaging:

| | |
|---|---|
| 1 | Develop a secure messaging governance framework |
| 2 | Develop secure messaging use cases |
| 3 | Agree on secure messaging standards and develop a standards framework |
| 4 | Implement a federated secure messaging directory solution |
| 5 | Review NASH process and develop a suitable trust framework |
| 6 | Establish a change and adoption program |
| 7 | Develop a secure messaging lever framework |
| 8 | Establish an innovation and research function |

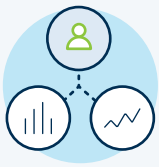
The refined objective of the Agency's secure messaging program is to mobilise these initiatives under a number of identified workstreams, to achieve national scaling.

# What are the results so far?

Overall, the work to date has provided the foundational components for achieving interoperability across the national healthcare system. The results are an interconnected network of systems, standard payloads, ubiquitous solution adoption and a federated directory searching capability.

However, to further develop and drive interoperability, more work needs to be done to progress these fundamental elements. This includes establishing a robust national platform that is built on a cohesive network and shares data at its most atomic level.

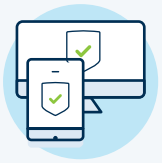
The clinical and social benefits of secure messaging include:



**improved clinical care** – facilitates access to clinical information to improve patient care

**streamlined administrative processes** – reduced time managing paper-based correspondence

**improved coordination of care** – improved communication between health and care providers as part of an end-to-end clinical workflow; facilitating transitions of care (admissions and discharge); and enabling shared care for complex and chronic conditions



**enhanced security and privacy** – improved privacy and security of patient information

# What are the challenges?

Challenges that were experienced throughout the development of this solution include:

### Inconsistent message payloads and template frameworks

There were no message payloads or template frameworks that provided a clear understanding of acceptable message payloads and templates between vendors.

### Low stakeholder engagement and a non-collaborative environment across the key stakeholders

A diverse range of vendors (CIS and SM) and users (e.g. GPs, specialists, allied health and jurisdictions) needed to be engaged and managed throughout the project journey, and the Agency does not have strong levers for change beyond stakeholder engagement and collaboration (i.e. hearts and minds).

### NASH certificate process and trust framework

Investigating and developing a set of rules that instils a level of confidence around certificate issuance and identity management so that commercial certificates can be accepted and can interoperate.

# Lessons learned

### Use agreed and consistent message payloads

Standard message payloads need to be established and promoted to deliver seamless interoperability through standardised sharing of information. This should include an appropriate conformance scheme to accredit systems with the agreed payloads.

### Facilitate strong stakeholder engagement and communication

A collaborative approach between the Agency, vendors, industry leaders and governing bodies can promote goodwill and a willingness for all stakeholders to work cohesively in developing and implementing a successful solution.

### Allow significant time for vendor software updates and user uptake timeframes

Consider private and jurisdictions CIS upgrades/ updates and uptake timeframes in project planning and implementation.

### Use national healthcare identifiers

The use of national healthcare identifiers is critical for identifying both recipients and senders of information exchange.

For any enquiries, please email
interoperability@digitalhealth.gov.au

Australian Government
Australian Digital Health Agency