Fact sheet

Secure messaging

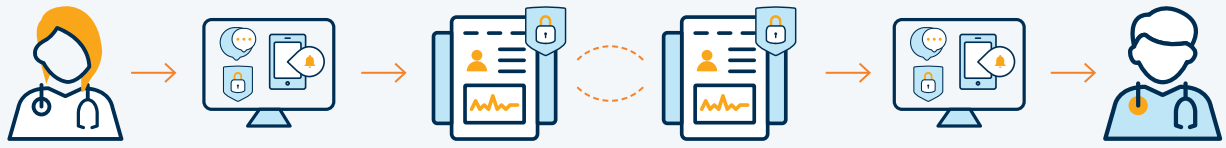
What is secure messaging?

Secure messaging is a core foundational capability that enables safe, seamless and secure exchange of clinical information between healthcare providers.[1] Secure messaging supports the secure delivery of messages containing clinical documents and other information between healthcare organisations, either directly or through one or more secure messaging providers.

The message is encrypted by the sender and decrypted by the receiver. The security of secure messaging is founded on the use of Public Key Infrastructure (PKI) such as NASH certificates, which are distributed by Services Australia.

How does secure messaging work?

For an organisation to send and receive secure messages, it will need a conformant clinical information system and be registered with one or more secure messaging providers. The diagram and process below outline a simplified overview of the secure messaging process.



STEP 1 The sending organisation creates an electronic message addressed to a service or practitioner, using an address book in their clinical information system or an external service directory.

STEP 2 The message is encrypted and passed through the sender's secure messaging provider to the receiver's secure messaging provider.

STEP 3 The receiver's secure messaging provider receives the message on behalf of the receiver, decrypts the message and passes it to the receiver's clinical information system.

STEP 4 The receiving clinical information system routes the received message to the intended service or practitioner and alerts the sender that the message has been successfully received.

Note: Secure messaging providers may also offer other models, such as web-based options for message creation and receipt. These options cannot integrate secure messages into a clinical information system (without manual effort). Your secure messaging provider can provide additional details.

Australian Government
Australian Digital Health Agency

Why should I implement secure messaging in my practice?[2]

Patients

may benefit through:

- patient data being appropriately and securely managed
- a reduced need to retell the same information
- confidential patient correspondence only being seen by treating clinicians
- improved clinical decisions due to the right information being available at the point of care
- a more streamlined patient experience.

Clinicians

may benefit through:

- improved timeliness of receipt of referrals and clinical information
- improved clinical decisions due to the right information being available at the point of care
- access to a broader range of referring practitioners
- streamlined administration due to reduction in paper-based processes
- improved coordination of care as a result of improved communication between healthcare providers
- confidence in privacy and security of transmitted patient data
- improved traceability and tracking of information for audit purposes.

Practice managers

may benefit through:

- a single channel for receiving referrals and correspondence
- reduced overheads and more cost-effective delivery of service from reduced use of paper correspondence (e.g. postage costs)
- improved coordination of care and service integration
- reduction in clerical error rates through reduced manual data collection
- improved practice efficiency from reduction in scanning and faxing.

Australian Government
Australian Digital Health Agency

The business case for secure messaging

Traditionally, healthcare providers have used post, fax, and more recently email, to share patient and clinical information. This medium of sharing information has few or no security measures. Secure messaging is part of the broader National Digital Health Strategy to safeguard patient information through enhanced security measures. Secure messaging also reduces the number of errors that occur with re-keying or transcribing, integrates more efficiently into clinical workflows, and enables an audit trail of successful delivery.

Costs of not embracing secure messaging

- Resources to monitor multiple communications channels (fax, eFax, email, post)
- Lost or misplaced communications (e.g. shared fax queues)
- Manual effort sending, receiving and scanning or re-keying information

Benefits of adopting secure messaging

- Access to a broader range of referring practitioners
- Single channel for referrals and communications
- Verifiable transmission and receipt
- Direct integration into clinical information system
- Access to timely clinical information
- Reduced costs (e.g. not needing to pay for postage stamps)

Next steps

- **Implementation guide:** Instruction on how to set up secure messaging.
- **User guide:** Information on the use of secure messaging in clinical practice.

1 ADHA, 'Secure messaging', 2019, Accessed 10 September 2020.

2 Haun, J, et. al, (2017) 'Clinical Practice Informs Secure Messaging Benefits and Best Practices' *Applied Clinical Informatics*, 8(4): 1003–1011, doi: 10.4338/ACI-2017-05-RA-0088.

Australian Government
Australian Digital Health Agency