Frequently Asked Questions

Secure messaging

Australian Government
Australian Digital Health Agency

What is it and why use it?

What is secure messaging?

Secure messaging is a core foundational capability that enables safe, seamless and secure exchange of clinical information between healthcare providers. 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. 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, the organisation 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.

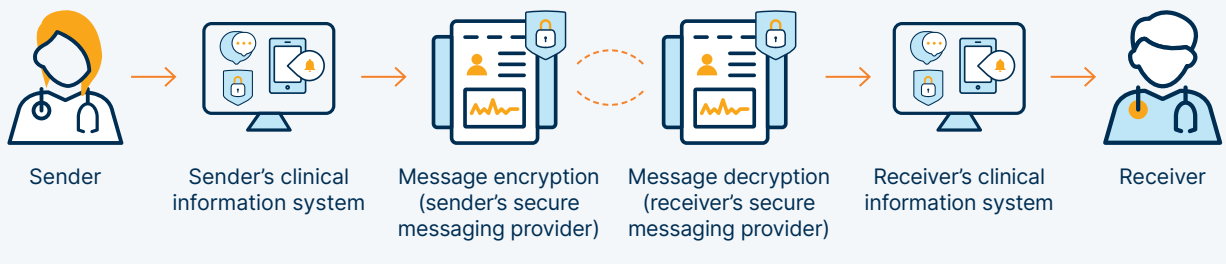
STEP 1 The sending organisation creates an electronic message addressed to a service or practitioner, using an address book in their clinical information system or an external service directory.

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 message 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 message provider can provide additional details.



Australian Government
Australian Digital Health Agency

Why not just use email?

Secure messaging offers security, auditability and privacy. The privacy and security risks of using unsecured or unencrypted email may include:

- email can easily be sent to the wrong recipient
- email is often accessed on portable devices, such as smart phones, tablets and laptops, which are easily lost or stolen
- email can be forwarded or changed without the knowledge or consent of the original sender
- email is vulnerable to interception.

Additionally, secure messaging can be fully integrated with clinical software. This allows automation in some administrative tasks for practice staff and doctors.

What are the benefits of secure messaging?

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.

What is the business case for secure messaging?

Traditionally, healthcare providers have used post, fax, and more recently email, to share patient and clinical information. These methods of sharing information have few or no security measures and leave healthcare providers exposed to breaches in privacy and security. It is also inefficient to receive information via multiple channels. Adoption of secure messaging is required to better protect important patient information through enhanced security measures. Secure messaging eliminates the need for re-keying or transcribing, integrates more efficiently into clinical workflows, provides a single channel for correspondence and enables an audit trail of successful delivery[1].

Additionally, secure messaging provides time and cost savings through integration with clinical software, automation of tasks and postage cost savings.

Note: An economic analysis undertaken as part of the development of the National Digital Health Strategy estimated the gross economic benefit of secure messaging could be around $2 billion over four years and more than $9 billion over 10 years.[2]

What is interoperability?

Interoperability relates to the ability to share information between different clinical systems. In secure messaging, interoperability also refers to the ability for one secure messaging provider to exchange messages with another secure messaging provider.

Many providers are now working together to ensure their systems are interoperable, creating more choice for organisations when deciding on a provider.

What can I receive through secure messaging?

The specifics of what documentation you can receive through secure messaging depends on your clinical information system.

However, most clinical information systems allow you to receive GP referrals, specialist reports, pathology results, radiology results, hospital discharge summaries and allied health consultation reports.

Setting up and using secure messaging

What software should I use for secure messaging?

The first step in setting up secure messaging involves choosing an appropriate secure messaging provider, compatible with your conformant clinical information system.[3]

See the Secure Messaging Implementation Guide for further guidance and a list of criteria for selecting a secure messaging provider, including hardware and clinical software compatibility, fees and charges, and training support.

What happens if I don't use a clinical information system?

Once registered with a secure messaging provider, the secure messaging system set-up/ commissioning process will vary depending on the chosen system and your existing technical environment. It may involve:

- remote software installation and configuration by the secure message provider
- access via a web-based portal that requires no local software installation.

Is secure messaging expensive to implement?

Secure messaging is cost-effective compared to other methods of sending (e.g. postage costs). Typically, there is a one-off installation fee and ongoing subscription costs for using secure messaging services. However, fees vary between secure messaging providers and may depend on your specific practice environment.

Also, some clinical information system vendors include secure messaging as a default within the clinical information system, so no additional subscription or set-up costs are charged.

Do I need a reliable internet connection?

A fast and reliable internet connection is needed to send and receive secure messages. It is expected that most ADSL2 and NBN connections will suffice, but it is recommended that practices select a plan with unlimited data and mobile internet as a backup in case of internet outages.

Australian Government
Australian Digital Health Agency

What equipment do I need?

Secure messaging systems are designed to work alongside existing clinical information systems, so you shouldn't need additional equipment or software beyond that supplied by your secure messaging provider.

However, you will need a reliable internet connection.

What is a security certificate?

A security certificate or digital certificate is an electronic 'credential' that establishes your identity when doing business or other transactions on the web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority so that a recipient can verify the authenticity of the certificate.

Security certificates can be kept in registries so that authenticating users can search other users' public keys.

What security certificates do I need?

A National Authentication Service for Health (NASH) PKI certificate (preferred) or a secure messaging provider issued commercial PKI certificate is required for secure messaging. PKI certificates are a digital certificate used to securely access online services, for example, secure messaging, My Health Record, and the Healthcare Identifiers Service (HI Service).

The NASH certificate is issued by Services Australia to eligible healthcare organisations who are registered with the HI Service.

How do I apply for a NASH PKI certificate?

NASH PKI certificates for healthcare provider organisations are only available through Health Professional Online Services (HPOS). HPOS can be accessed here.

What happens when my digital certificate expires?

Certificates are issued with an expiry date and must be renewed so you can continue to send and receive messages. Your clinical information system (depending on capability) may monitor the expiry of certificates and will let you know when you require a new certificate.

When the new certificate is received, contact your secure messaging provider and schedule a certificate update to prevent impact on your message activity.

How do I find other clinicians' secure messaging details?

Clinician and practice details are held in online directories such as the National Health Services Directory (NHSD) and other specialist directories. Your clinical information system will be able to search these directories to identify the appropriate recipient for the message and retrieve the technical information from a secure messaging provider directory to enable message delivery.

Your clinical information system may also have address book functionality for your regular contacts. Practice websites and correspondence can include secure messaging details along with other contact information.

How do I know if my message has been successfully delivered?

One of the benefits of using secure messaging is the mandatory acknowledgement associated with sending messages.

Your clinical information system will have functionality that lets you check whether a message has been successfully delivered (acknowledgement of receipt).

How do I encourage other healthcare organisations to use secure messaging?

To promote the exchange of secure electronic communications between healthcare providers in your geographic region, you can advertise your secure messaging identifier on external communication documents, such as reports and referrals, so that others know how to communicate with you.

1 ReferralNet, 'An introduction to secure messaging', 2018, accessed 10 September 2020.

2 ADHA, 'Secure Messaging', n.d., accessed 10 September 2020.

3 ADHA, 'Conformant clinical software products', 2020, accessed 10 September 2020.