



FOR SPECIALIST PRACTICES

# Secure Messaging

**WHAT IS IT AND WHY USE IT?..... 2**

What is secure messaging?.....2

How does secure messaging work?.....2

Why wouldn't I just use email?.....3

What are the benefits of secure messaging? .....3

What is the business case for secure messaging? .....4

What is interoperability?.....4

What can I receive through secure messaging?.....4

**SETTING UP AND USING SECURE MESSAGING ..... 5**

What software should I use for secure messaging? .....5

What happens if I do not use a Clinical Information System? .....5

Is secure messaging expensive to implement?.....5

Do I need a reliable internet connection? .....5

What equipment do I need to use secure messaging? .....5

What is a security certificate?.....5

What security certificates do I need?.....6

How do I apply for a NASH PKI Certificate?.....6

What happens when my digital certificate expires? .....6

How do I find other clinicians' secure messaging details? .....6

How do I know if my message has been successfully delivered? .....6

How do I support other healthcare organisations to use secure messaging? .....6



# What is it and why use it?

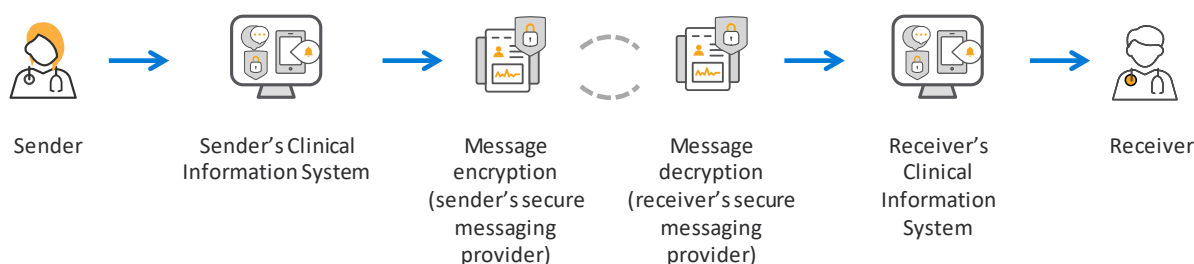
## WHAT IS SECURE MESSAGING?

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/or 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 which is distributed by Services Australia.

## HOW DOES SECURE MESSAGING WORK?

For an organisation to send and receive secure messages, the organisation will need to have installed a conformant clinical information system and registered with one or more secure messaging providers. The process and diagram 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 from within 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 lack the ability to integrate secure messages into a clinical information system (without manual effort). Your secure message provider can provide additional details.

## WHY WOULDN'T I 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; and
- email is vulnerable to interception.

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

## WHAT ARE THE BENEFITS OF SECURE MESSAGING?<sup>1</sup>



### 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, and
- a more streamlined patient experience.



### Specialists

#### 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, and
- improved traceability and tracking of information for audit purposes.



### Practice Managers

#### may benefit through:

- a single channel through which referrals and correspondence are received,
- reduced overheads and more cost-effective delivery of service from reduced use of paper correspondence and postage costs,
- improved coordination of care and service integration,
- reduction in clerical error rates through reduced manual data collection, and
- 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 little to no security measures and leave healthcare providers exposed to breaches in privacy and security. It is also inefficient to be receiving 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.<sup>2</sup> 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 has estimated the gross economic benefit of secure messaging could be around \$2 billion over four years and more than \$9 billion over 10 years.<sup>3</sup>

## 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 send and receive messages with another secure message 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 exact specifics of what documentation you can receive through secure messaging will be dependent 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 of setting up secure messaging involves choosing an appropriate secure messaging provider compatible with your conformant clinical information system.<sup>4</sup> 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 DO NOT USE A CLINICAL INFORMATION SYSTEM?

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

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

## IS SECURE MESSAGING EXPENSIVE TO IMPLEMENT?

Typically, there is a one-off installation fee and ongoing subscription costs associated with using secure messaging services. However, fees vary between secure messaging providers and further information should be sought from the provider that takes the specific practice environment into account. Also, some vendors include secure messaging as a default within clinical information system, so no additional subscription or set-up costs are charged. It should be noted that secure messaging is cost effective compared to other methods of sending (e.g. postage costs).

## DO I NEED A RELIABLE INTERNET CONNECTION?

A fast and reliable internet connection will support you 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 the instance of internet outages.

## WHAT EQUIPMENT DO I NEED TO USE SECURE MESSAGING?

Secure messaging systems are designed to work alongside existing clinical information systems, meaning additional equipment or software should not be required beyond that supplied by your secure messaging provider and an 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 (CA). 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 to enable secure messaging. PKI certificates are a digital certificate used to securely access online services, for example, secure messaging, My Health Record, and the HI service). The NASH certificate is issued by [Services Australia](#) to eligible healthcare organisations who are registered in the Healthcare Identifiers 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 to continue to be able 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, you should 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 enable searching these directories to identify the appropriate recipient for their 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 acknowledgment associated with sending messages. Your clinical information system will have functionality that enables you to check whether a message has been successfully delivered i.e. acknowledgment has been received.

## HOW DO I SUPPORT OTHER HEALTHCARE ORGANISATIONS TO USE SECURE MESSAGING?

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

---

Copyright notice:

- Works published on [www.servicesaustralia.gov.au](http://www.servicesaustralia.gov.au) are provided under [Creative Commons licence 3.0](#).

<sup>1</sup> ADHA, 'Secure Message Delivery For Allied Health Providers', n.d., accessed 10 September 2020.

<sup>2</sup> ReferralNet, 'An introduction to secure messaging', 2018, accessed 10 September 2020.

<sup>3</sup> ADHA, 'Secure Messaging', n.d., accessed 10 September 2020.

<sup>4</sup> ADHA, 'Conformant clinical software products', 2020, accessed 10 September 2020.