Practice Assist
Strengthening general practice in WA

Fact Sheet
V1 / April 2022

Secure Messaging
Getting Started - Guide and Checklist

The following guide provides an overview of the steps to implement secure messaging in your practice, including:

- choosing your secure messaging provider
- checking and implementing security certificates as required
- sharing your secure messaging contact details
- training staff and preparing your practice
- supporting adoption of secure messaging

Together, these steps will support you in implementing secure messaging successfully in your practice, ensuring you are able to safely send and receive clinical information.

Implementation Checklist	
Step 1	Choose your secure messaging provider
Step 2	Healthcare provider registration and security certificates
Step 3	Publish your details and message type configuration
Step 4	Prepare your practice
Step 5	Support the use of secure messaging
Step 6	Additional resources

Secure messaging implementation checklist

Implementation Steps	
☐	Select secure messaging provider
☐	Ensure your organisation has a Healthcare Provider Identifier (HPI-O)
☐	Obtain your National Authentication Service for Health Certificate (NASH)
☐	Share secure messaging contact details and promote use
☐	Create or update templates for secure messaging
☐	Train Staff
☐	Update address books with provider's secure messaging contacts

Step 1:
Choose your secure messaging provider

There are a range of practical considerations to discuss with software vendors when selecting a secure messaging provider, as outlined below. Healthcare providers may register with more than one provider.

Secure messaging provider selection criteria	
☐	**Compliance with relevant standards** Does the secure messaging provider's system meet the Australian Secure Message Delivery (SMD) Standard?
☐	**Compatible hardware** Will the secure messaging provider's system work on the hardware used in your practice (e.g. PC or Mac)?
☐	**Compatible clinical software** Will the secure messaging provider's system work with the clinical information system used for patient record keeping in your practice?
☐	**Fees and charges** Are there any fees and charges? (e.g. per user, setup, subscription, per message)
☐	**Vendor training and support** What documentation, training and ongoing support is available from the vendor? Are there costs associated with this support?
☐	**Linked organisations** Which system(s) do your regular contacts use? (e.g. WA Health CRS use HealthLink)
☐	**Other practice specific requirements** Are there additional requirements based on the specific needs of your practice?

Note: Further information on the range of secure messaging vendors may be found in the Digital Health Toolkit

Step 2:
Healthcare provider registration and security certificates

Ensure your practice has a healthcare provider identifier

Practitioners will need a Healthcare Provider Identifier - Individual (HPI-I) and the organisation will need a Healthcare Provider IdentifierOrganisation (HPI-O). Ensure your practice has an HPI-O recorded in the clinical information system (CIS) and is connected to the Healthcare Identifiers (HI) Service.

For details on obtaining these identifiers, see the Digital Health Toolkit

Obtain your NASH PKI Certificate

The National Authentication Service for Health (NASH) PKI certificate is used by healthcare providers to securely access and share health information. A guide to obtaining a NASH certificate can be found on the Digital Health Toolkit

Note: If your organisation uses My Health Record then you already have the required identifiers and certificates

Step 3:
Publish your details and message type configuration

Publish your details to help others find you

Use of secure messaging requires accurate information about your practice and practitioners including identifiers such as HPI-O, HPI-I and Medicare provider number. This allows other organisations to communicate with you. Your secure messaging provider will help you publish your details in their directory.

Advise your secure messaging provider what message types you wish to receive

Your secure messaging provider will need to publish the message types that your organisation's clinical software is able to process via secure messaging. In most cases, this will be done automatically as part of the product installation. However, if your organisation does not wish to receive all the message types that your clinical software can receive, let your provider know this during set-up.

Step 4:
Prepare your practice

The following tasks will help you get the most out of the secure messaging system and promote adoption in your practice:

Update clinical workflows.

Update your workflows and processes to include secure messaging as the preferred communication channel.

Update the clinical information system address book.

Most secure messaging providers will update your practice address book as part of the setup process. To support the consistent use of secure messages, you may wish to create a list of favourite or commonly used contacts. Refer to your clinical software providers support for further details.

Update templates.

Templates can be used when sending secure messages to pre-populate information such as patient details, practice details, and clinical information. This can save time and improve consistency. Many organisations provide referral templates which can be added to your clinical system and will be able to provide these to you

Note: WA Health Central Referral Service have referral templates for a wide range of clinical software systems

Update practice documents and website.

Advertise your secure messaging ID on external communication documents such as letterheads, website, reports and referrals. You may wish to indicate your preference for secure messaging by removing fax details from these documents.

Step 5:
Support the use of secure messaging

To embed the use of secure messaging and promote adoption in your practice:

- **Train staff** on how to use secure messaging. Your secure messaging provider should be able to provide resources to support training. Your clinical information system provider may also be able to provide guidance.
- Talk to the organisations you commonly refer to see if they have secure messaging capability.