Implementation Guide

Secure messaging

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.

Australian Government
Australian Digital Health Agency

Secure messaging implementation checklist

Implementation step	Status
Ensure your clinical software is compatible	□
Select secure messaging provider	□
Ensure your organisation has a Healthcare Provider Identifier (HPI-O)	□
Obtain your National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) certificate via Health Professional Online Services (HPOS)	□
Share secure messaging contact details and promote use	□
Create or update templates for secure messaging	□
Train staff	□
Update address books with providers' secure messaging contacts	□

Australian Government
Australian Digital Health Agency

Step 1: Choose your secure messaging provider

Secure messaging provider selection criteria

There are a range of practical considerations when selecting a secure messaging provider, as outlined below. Practitioners are often registered with more than one provider. However, work driven by the Australian Digital Health Agency to develop standardised message formats and interoperability is reducing the need for this.

✓ **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**

What are the set-up costs? Are there any other fees and charges (e.g. fee per user, annual fee, per message fee)?

✓ **Vendor training and support**

What documentation, training and ongoing support is available from the vendor? Are there costs associated with this support?

✓ **Other practice specific requirements**

Are there additional requirements based on the specific needs of your practice?

Allied Health Professions Australia (AHPA) has published a Connection Guide for Secure Messaging that provides additional information on secure messaging software providers.

Important note:

Secure messaging providers may also offer other secure messaging models such as web-based options for message creation and receipt.

These options cannot integrate secure messages into clinical information system patient records (without manual effort). Your secure message provider can provide additional details.

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 Identifier-Organisation (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.

If your practice does not have an HPI-O, you can view the Agency's website for guidelines and further information about registering your organisation.

Important note:

If your practice is connected to the My Health Record system, then you have already completed this step.

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. For secure messaging, a NASH PKI certificate (preferred) or a secure messaging provider issued commercial PKI certificate is required.

Healthcare organisations need to request a NASH PKI certificate using the Health Professional Online Services (HPOS) portal. HPOS can be accessed here.

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 particular message types (e.g. eReferral) 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 is capable of receiving, 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 a communication channel.
- **Update the clinical information system address book**. Efforts to locate a provider's secure message identifier can be a barrier to adoption. Check that the contact details in your clinical information system address book are correct for frequently used contacts. HealthVitalIT has a useful article on secure messaging and electronic clinical referrals that provides examples using several commonly used clinical information systems.
- **Update templates**. Many clinical information systems have a template function that can be used when sending secure messages. Templates can pre-populate information such as patient details, practice details, and standard text. This can save time and improve consistency. HealthVitalIT has a useful article on templates that provides an overview of template management using several commonly used clinical information systems.
- **Update practice documents and website**. Advertise your secure messaging ID on external communication documents such as letterheads, website, reports and referrals. You can 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 frequent referrers**. Review correspondence from other clinicians and contact those who are not using secure messaging to see if they have secure messaging capability.

Additional resources

- Connection Guide for Secure Messaging | AHPA
- Example Secure Message Delivery (SMD) Policy | Australian Digital Health Agency
- Help Centre | Australian Digital Health Agency
- Secure Messaging Fact Sheet | Australian Digital Health Agency
- Secure Messaging Frequently Asked Questions | Australian Digital Health Agency
- Secure Messaging User Guide | Australian Digital Health Agency