Practice Assist
Strengthening general practice in WA

Fact Sheet
V1 / April 2022

Secure Messaging Frequently Asked Questions

What is secure messaging?

Secure messages provide an alternative method for healthcare providers to communicate with each other and minimises the risk associated with sending sensitive information

What can secure messaging be used for?

The specifics of what documentation you can receive through secure messaging depends on your clinical information system.
Most clinical information systems allow you to receive:

- Specialist reports
- Pathology results
- Digital Imaging results
- Hospital discharge summaries
- Allied health consultation reports
- Ad-hoc communication from other healthcare providers

In addition, secure messaging can be used to send:

- Referrals to connected providers such as WA Health's Central Referral Service
- Ad-hoc communication (where agreed between providers)

Can I use secure messaging to communicate with patients?

No. Secure messages are currently only available for communication between healthcare providers. When sending sensitive information to patients, consider using encrypted email, password protected attachments via email or uploading an event summary to the patient's My Health Record

How secure are secure messages really?

Secure messages sent by systems meeting the Australian Secure Message Delivery Standard are securely encrypted so that they can only be viewed by the sender and recipient. The use of a directory ensures that messages are sent directly to the recipient's inbox and, unlike post, fax or email, are not subject to human error when addressing messages.

What are the benefits of secure messaging?

What are the risks associate with sending clinical information via post/fax/email?

Sending sensitive information via post, fax, or email, leaves healthcare providers subject to breaches in privacy and security which may result in clinical information inadvertently being exposed. Such data breaches must be reported to the individual(s) and the Australian Information Commissioner and risk attracting substantial fines for both the organisation and individual involved.

What are the benefits for clinicians?

In addition to improved security, secure messaging can:

- Reduce or eliminate the time spent re-entering demographic and clinical information already captured in the clinical system
- Reduce the need to re-write or provide supplementary information by using referral templates
- Provide near real time updates on the successful receipt of referrals
- Support the identification of a wide range of suitable providers for referrals
- Provide an accurate audit trail for investigation purposes
- Integrate with the clinical system, allowing for important clinical information to be stored in the patient record

What are the benefits for organisations?

In addition to improved security, secure messaging can:

- Drastically reduce the administrative burden associated with printing, scanning, sending and receiving clinical information
- Minimise printing, fax and postage costs
- Allow for timely access to information
- Minimise the risk of documents being attached to an incorrect record
- Reduces requirement to manually attach documents to a patient record
- Improves visibility of the organisation to other healthcare providers

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 are the requirements for using secure messaging?

What do I need to prepare for secure messaging?

If you are using My Health Record and/or ePrescribing, you are well prepared to use secure messaging. The requirements are:

- An organisation HPI-O
- An active, current NASH certificate
- HPI-Is for each clinician

There is no need to obtain any new copies of the above if already setup

What secure messaging system should I use?

Organisations are free to use their own choice of secure messaging provider. However it is suggested that the following considerations are taken into account

- 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?
- Will the secure messaging provider's system work with the clinical information system used for patient record keeping in your practice?
- Are there any fees and charges? (e.g. per user, setup, subscription, per message)
- What documentation, training and ongoing support is available from the vendor? Are there costs associated with this support?
- Which system(s) do your regular contacts use? (e.g. WA Health CRS use HealthLink)

For further information, see the Digital Health Toolkit

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.

Can I use secure messaging without a conformant clinical information system?

Many secure messaging providers offer a standalone system, allowing messages to be sent and received without a conformant clinical information system. Check with your provider to see if this is available.

Is secure messaging expensive to implement?

Each secure messaging provider has their own price model which may vary depending on provider type. Some providers do not charge General Practice for using their system. When considering the cost of implementing and using a secure messaging system, it is important to balance any cost against the cost associated with other communications such as postage, printing and administrative time.

Using Secure Messaging

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).

Is every healthcare provider contactable via secure messaging?

All healthcare providers make their own decisions around the use of secure messaging, therefore not all organisations are contactable via secure messaging. Despite this, the value of secure messaging is such that the majority of providers are capable of receiving secure messages.

It is important to note that not all secure messaging systems can communicate with each other, so before deciding on a provider it's worth viewing their directory to ensure it can connect you to commonly used providers.

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.

You may also wish to speak with organisations you commonly refer to to encourage them to start using secure messaging if not already doing so