Capital Health Network
ACT's primary health network

Information sheet

Secure messaging – Allied Health

Secure messaging is a secure and reliable way to exchange confidential patient health information electronically. The use of email to communicate patient health information is not recommended as it is insecure and has none of the safeguards offered by secure messaging. Secure messaging:

- enables the secure sending and receipt of clinical documents between healthcare professionals
- uses an intermediary and the national provider directory to send and receive messages
- uses PKI NASH certificates to encrypt the message

Encryption allows you to know:

- who sent (or uploaded) the information – authentication
- the information content has not been altered between sending and receiving – integrity
- the sender cannot at some time in the future dispute they created and sent the information – non-repudiation the only person/practice the information is directed to can open it – confidentiality (NEHTA 2013).

NASH certificates are needed to secure (sign and encrypt) patient health information messages/and correspondence between yourself and other health professionals and to access the My Health Record system. NASH certificates are issued by the National Authentication Service for Health managed by the Department of Human Services.

Note: the NASH PKI certificate is additional to the PKI certificate you use to do eBusiness with the Department of Human Services – Medicare.

To find out more about secure message delivery see the Australian Digital Health Agency for the following: http://www.digitalhealth.gov.au/get-started-with-digital-health/what-is-digital-health/secure-messaging

Secure messaging products

There are a number of secure messaging products using the national digital health infrastructure available for you to choose from. Some of the providers are listed below. You can find additional secure messaging products by searching the internet.

Telstra Health – Argus

Argus is a secure, simple and reliable electronic message service. Argus enables secure transmission of clinical documents such as referrals letters, discharge summaries and requests for diagnostic services. Argus uses national infrastructure and is compliant with Australian digital health and privacy standards:

- national health services directory
- NASH public key encryption
- HL7 and CDA message and document formats

There are several clinical software applications that have interfaces with Argus. If you do not have clinical software and write your correspondence using MS Word.

http://healthconnex.com.au/solution/argus

HealthLink – HL Connect

HealthLink has a web portal that enables you to send and receive patient-related documents securely from any device. If you use a clinical application for your patient records HealthLink is integrated with most of the products on the market.

http://www.healthlink.net/en_AU/support/knowledge-base/hlconnect/

Medical Objects Australia

Secure messaging enables allied health practices to send patient letters and download patient referrals and receive hospital discharge summaries. If you write your reports in MS Word and wish to send them securely and electronically to the referring practitioner you can do this using Medical Objects Word plug-in. Medical Objects has integrated with the major Allied Health clinical software providers. For more information see:
https://www.medical-objects.com.au/allied-health/secure-messaging/

coreplus

coreplus provides a secure messaging hub that sends and receives messages to both HealthLink and Argus messaging systems.

http://coreplus.com.au/integrated-secure-message-delivery-smd-service/

Capital Health Network

For more information or assistance with secure messaging set up please contact Elizabeth Moss, eHealth Consultant on 02 6287 8039 or email e.moss@chnact.org.au