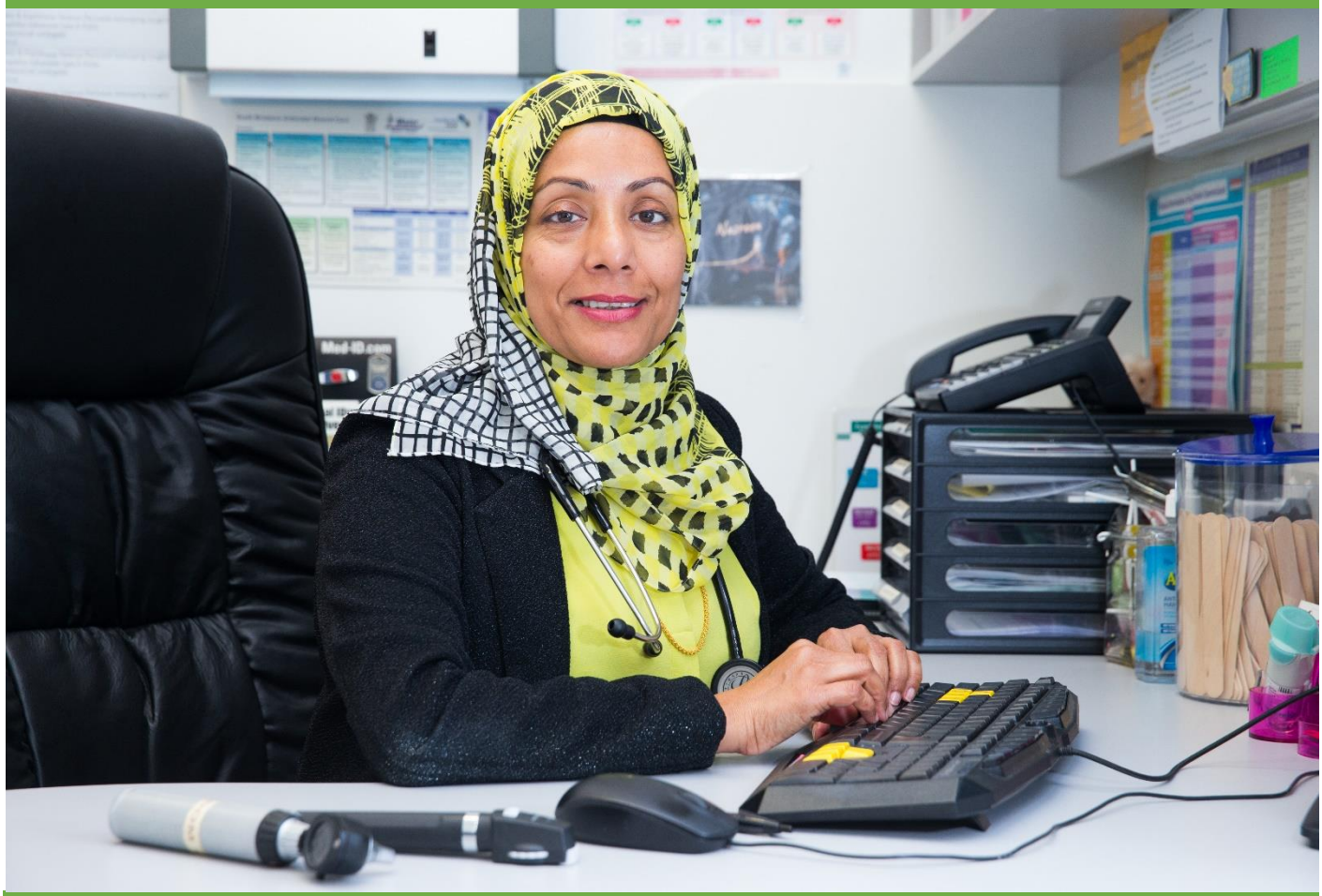
Secure Message Delivery Information Pack

General Practice



phn BRISBANE SOUTH

An Australian Government Initiative

BETTER SYSTEM, BETTER HEALTH

Contents

Secure Message Delivery

This information pack has been designed to provide general practices with relevant information on and to support them in the uptake of secure message delivery (SMD).

What is Secure Message Delivery?

Secure message delivery is a set of technologies that enables:

- the encryption (by sender) and decryption (by receiver) of messages
- secure point-to-point delivery of messages
- storage on a secured network server
- delivery to a single, known intended receiving entity.

The Australian Digital Health Agency (ADHA) identifies three basic tenets of SMD as:

1. prevents the unauthorised interception of the message content
2. provides verification that the message has not been altered since it was sent
3. provides system notification of successful delivery.

What are the Benefits of Secure Message Delivery?

The benefits of SMD to general practice include:

- secure exchange of clinical information and documents such as referrals and discharge summaries, preventing unauthorised interception of the message
- reducing the use of paper correspondence – cost saving
- reducing the time taken to send and follow up paper correspondence
- confidential patient correspondence is only seen by intended recipient/treating clinicians
- system notification of successful message delivery
- potential to improve the timeliness of receipt of clinical information, and therefore the efficiency and quality of care provided.

In a healthcare setting, SMD can be used for:

- clinician to clinician communication management (e.g. referral, discharge summary, event summary, lab/radiology, prescription/dispense messaging)
- patient services/ clinical operations management.

Limitations to SMD

SMD applications developed by different vendors result in interoperability issues. This means that messages cannot be seamlessly exchanged between different vendors. However the ADHA is currently collaborating with the industry to co-design a Proof of Concept Project to address interoperability issues. For information about the progress of the Proof of Concept Project, visit the Australian Digital Health Agency website.

Public Key Infrastructure certificates– What are they?

A Public Key Infrastructure certificate, or PKI, is a certificate used to securely access online services. Some of these services include Health Professionals Online Service (HPOS), Provider Digital Access (PRODA), My Health Record and Secure Messaging. PKI certificates use a technology called a Secure Hash Algorithm (SHA) to access/use these online services. This allows the system to authenticate users to ensure that only authorised people (usually clinicians) and organisations are sending and receiving the correct information. The Department of Human Services issues the PKI certificates to individual health care providers and health care organisations who are registered and authorised to access confidential information and public health care portals. There are a number of different PKI certificates that are used for different tasks.

PKI certificates are not permanent and will expire after a certain period – usually two or five years depending on the certificate type.

What PKI is Required for SMD?

The PKI certificate required for SMD is commonly known as an Organisational NASH PKI certificate. NASH stands for National Authentication Service for Health. The same certificate is also used to access the My Health Record System.

What do You Need to Know about a NASH PKI Certificate?

The NASH PKI certificate is sent to the practice in a secure, downloadable file which needs to be installed into the clinical software. A Personal Identification Code (PIC) code is also sent separately from the Department of Human Services. Both the NASH PKI CD and the PIC code are required for successful installation. The NASH PKI certificate expires every two years.

The Department of Human Services will automatically issue the practice with a new certificate and PIC code when renewal is approaching. The new NASH PKI CD and PIC code will need to be installed into the clinical system (if the clinical system is compatible) and the expired certificate will need to be removed. To apply for an organisational NASH PKI certificate, a Provider Digital Access (PRODA) account is required - here.

Helpful Information about PKI Certificates

Document or Webpage title	Link
HPOS, PRODA and PKI Certificates	View here
Public Key Infrastructure Information (Department of Human Services)	View here

Setting up SMD

Pre-requisites

The table below outlines the pre-requisites required to successfully set up SMD within a practice[1].

Pre-requisites	
Step 1	The organisation must have registered with the Healthcare Identifiers (HI) Service, and received their Health Provider Identifier –Organisation (HPI-O) number(s) from the Department of Human Services.
Step 2	The organisation should have linked their existing Human Services Public Key Infrastructure (PKI) Site Certificate to the HI Service (as part of the Seed Application), or applied for and installed a new one.
Step 3	The organisation should have applied for and installed their National Authentication Service for Health (NASH) PKI Certificate(s) for Healthcare Provider Organisations.
Step 4	The Organisation Maintenance Officer (OMO) and/or Responsible Officer (RO) should have established access to Health Professional Online Services (HPOS), by setting up their HI Service Individual PKI Certificate(s).
Step 5	Providers should have published their HPI-O details in the Healthcare Provider Directory (HPD).
Step 6	It is also recommended that the Health Provider Identifier –Individuals (HPI-I) publish their details in the HPD, and these are linked to the organisation's HPI-O by the OMO. This is optional, but is highly recommended if individual providers in an organisation receive correspondence addressed to them by name. This will make it easier for senders to find them and address correspondence to them electronically.

Checklist of pre-requisites:

The checklist below outlines the required infrastructure to start using SMD.

	Pre-requisites	Complete
1	Nominate the organisation's Responsible Officer (RO) and Organisational Maintenance Officer/s (OMO)	☐
2	Apply for an organisational HPO-I number (here)	☐
3	Linked the Human Services PKI Site certificate to the HI service	☐
4	Apply for a NASH certificate (here)	☐
5	RO and OMO/s have established access the HPOS (recommended through PRODA) (here)	☐
6	Organisation's HPI-O details are registered in the HPD, this can be done through HPOS (details here)	☐
7	Organisations HPI-I details are published in the HPD	☐
8	Install the NASH PKI certificate into the clinical software	☐

Getting Connected:

The table below outlines the next steps to take to ensure a practice can use SMD.

Setting up SMD	
Step 1	SMD requires the use of an Endpoint Location Service (ELS) which allows other organisations to discover each other's SMD details in order to communicate. The SMD provider will provide the necessary details of its ELS Instance and will advise or assist in publishing ELS details in the HPD through HPOS.
Step 2	Authorise the SMD Provider as a Contracted Service Provider (conditional). This is a conditional step dependent on the SMD provider. If the SMD provider informs a practice that it needs to make them a Contracted Service Provider (CSP), the SMD provider must provide the CSP number and the practice will need to authorise them to act as a CSP for the organisation. The HPI-O number will need to be linked to their CSP Number in the HI Service. The CSP linkage can be done using HPOS by the Responsible Officer (RO) or Organisational Maintenance Officer (OMO). See the HPOS CSP Linking Quick Reference Guide for guidance. Alternatively, individuals can call the HI Service enquiry line on 1300 361 457.
Step 3	Advise the SMD provider of the message types the practice wishes to receive via SMD. The SMD provider will need to publish the particular message types (e.g. eReferral) that the organisation wishes to receive (and that the clinical software also has the ability to process) via SMD. In most cases, this will be done automatically as part of the product installation, however if the organisation does not wish to receive all the message types that the clinical software is capable of receiving, they will need to inform the SMD provider of this during set-up.

Checklist for getting connected:

The check list below will help track progress towards being able to use SMD in the practice.

	Setting up SMD	Complete
1	Publish the End Point Location Service (ELS) details in the Healthcare Provider Directory (HPD)	☐
2	Authorise the SMD Provider as a Contracted service Provider (conditional)	☐
3	Advise the SMD provider of the message types the practice wishes to receive via SMD	☐

SMD vendors

There are a number of SMD vendors available for practitioners to review and decide on one, or more, that is appropriate to their practice. Below is a table with links to their respective website.

SMD Vendor	Link
Argus	General Information
Healthlink	General Information
Medical Objects	General Information
ReferralNet	General Information

What next

When a practice has secure messaging installed and configured, it is time to start using the new system. Below is a table of information to guide practices to ensure they are getting the most out of SMD.

Activity	Complete
Provide training to staff on how their role can use SMD (through your SMD vendor)	☐
Update referral templates to the latest versions. Templates being created with the support of Brisbane South PHN will have auto-populated fields and the receiver's STS address already embedded; this makes sending referrals via SMD simple and quick	☐
Talk to the practice's frequent referees and see if they have SMD too. Start sending to them to quickly see an improvement in workflow	☐
Make sure to install the latest version of Metro South Health's Refer Your Patient template and start referring to the Central Referral Hub using SMD. This means a prompt notification that the referral has been received.	☐
Read Metro South Health's 'Refer your patient to Metro South Health using Secure Messaging' flyer.	☐

Support

For support, further information or general questions about SMD, please contact Brisbane South PHN Digital Health Enablement team on 07 3864 7555 or ehealth@bsphn.org.au.

Reference list

1. Australian Digital Health Agency. Secure Messaging [internet]. Canberra (ACT): Australian Digital Health Agency; 2016 [citied 2018 March 21]. Available from: https://www.digitalhealth.gov.au/get-started-with-digital-health/what-is-digital-health/secure-messaging

This service has been made possible through funding provided by the Australian Government under the PHN Program.

First floor, Building 20, Garden City Office Park, 2404 Logan Road, Eight Mile Plains QLD 4113
PO Box 6435, Upper Mt Gravatt QLD 4122 T: 3864 7555 or 1300 467 265 F: 3864 7599
www.bsphn.org.au