nehta

Secure Messaging

Commissioning Requirements for Secure Message Delivery

3 June 2016

National E-Health Transition Authority

National E-Health Transition Authority Ltd
Level 25
56 Pitt Street
Sydney, NSW, 2000
Australia.
www.nehta.gov.au

First published: 3 June 2016

Table of contents

1 Introduction

1.1 Purpose and audience

This document defines the commissioning requirements for installation, configuration and operation of SMD products for the purpose of the Secure Messaging requirement of the Practice Incentives Program (PIP) eHealth Incentive.

The document has two main sections, each with a different audience and purpose.

- Section 2 is intended for general practices. It is intended to help a practice verify that their secure messaging product has been installed and configured as required for the PIP eHealth Incentive requirement 2. This does not require detailed knowledge of the Secure Message Delivery (SMD) specification.[1]
- Section 3 is intended for commissioning agents – the parties who will install and configure an SMD product for use by a general practice.

  It is expected that the commissioning agent is familiar with the technical issues related to installation and configuration of SMD products. This role would typically be fulfilled by the SMD product or Secure Messaging Service Provider. However other parties may have the technical knowledge and skill needed to carry out the work, such as a contracted IT support specialist or Medicare Local providing similar services. General practices with the necessary in-house IT support may wish to undertake the work themselves.

1.2 Scope

This document addresses only those aspects of SMD implementation that relate to:

- access and use of the national infrastructure services
- achieving interoperability between implementations by different vendors
- security and reliability of implementations.

It defines what an implementation must do; it is not a technical guide on how to do it.

1.3 Assumptions

It is assumed that the practice's desktop clinical system complies with the PIP eHealth Incentive requirement 1 regarding integrating healthcare identifiers into electronic practice records.

1.4 Updates

This document may be updated from time to time based on feedback from stakeholders. Practices, software vendors or commissioning agents can provide feedback to help@nehta.gov.au

[1] ATS 5822-2010 E-Health secure message delivery is referred to in this document as the SMD specification.

2 For general practices

2.1 Introduction

This section is intended for a practice principal or manager in a general practice who is responsible for ensuring PIP eHealth Incentive compliance.

It is intended to help you verify that your secure messaging product has been installed and configured as required for the PIP eHealth Incentive requirement 2.

2.2 Recommended reading

It is recommended that clinicians and staff at your general practice are familiar with these documents:

Implementation Overview – Secure Messaging Capability

http://www.nehta.gov.au/get-started-with-digital-health/pip-ehealth-incentive

Clinician's User Guide

http://www.nehta.gov.au/using-the-my-health-record-system/digital-health-training-resources/guides/519-clinicians-user-guide

2.3 Getting ready

There are a few things that your practice must do before installing and configuring your SMD product. These are described in the **Implementation Overview – Secure Messaging Capability** and the **Clinician's User Guide**, and summarised below:

- Obtain a Healthcare Provider Identifier(s) – Organisation (HPI-O) from the HI Service. This can be done by using the eHealth Online Forms application tool.

  While most general practices require only one HPI-O and all incoming messages for the practice will be encrypted using the secure key associated with that one HPI-O, other practices may have more complex structures. If this is the case, you should review and consider the information related to organisation identifiers presented in the *eHealth Clinician's Desktop User Guide* and the *Healthcare Identifiers Implementation User Guide*.

- Select an SMD product from the *Digital Health Incentive Product Register for Secure Messaging* at https://digitalhealthincentive.nehta.gov.au/product-register/registers/secure-message-delivery. (See 2.4 below.)

- Obtain a NASH PKI Certificate for Healthcare Provider Organisations (if you do not already have a DHS eHealth Record Organisation PKI Certificate).

  Note: The DHS eHealth Record Organisation PKI Certificate has now been replaced by the NASH PKI Certificate for Healthcare Provider Organisations.

  A NASH PKI Certificate can be obtained using the eHealth Online Forms application tool

  Additional information is provided on the Department of Human Services (DHS) website www.humanservices.gov.au/pki. Note the certificate required for point-to-point secure messaging is the same certificate that is used to access the My Health Record system.

You will also need to develop a written policy to encourage the use of standards-compliant secure messaging within your practice.

2.4 Selecting an SMD product

All products listed on the *Digital Health Incentive Product Register for Secure Messaging* conform to the required technical specifications and have the ability to send and receive messages to other standards-compliant products. However, products may differ in how they do this. Some products may enable practices to use the services of an intermediary party (such as a secure messaging service provider). Others may enable the practice to send and receive messages without the use of an intermediary party. SMD products may also differ in their need for specialist IT security expertise and whether that expertise is needed in house or is provided externally via a support contract.

It is ***strongly recommended*** that you ask your preferred SMD product supplier about the options provided by the product and seek advice regarding the configuration that best suits your practice, ***before you commit to a particular product***.

In most cases, the SMD capability will be provided by a separate product from your desktop clinical system (however, there will be some exceptions to this). Therefore, it is ***strongly recommended*** that, when you choose your SMD product, you consider whether and how the product will integrate with your desktop clinical system. You should seek advice from both your desktop clinical system supplier and your preferred SMD product supplier regarding product compatibility and integration.

2.5 Verifying that your SMD product is ready for use

It is an eligibility requirement for the PIP eHealth Incentive that you verify that your SMD product(s) have been "installed and configured so as to be interoperable with other standards-compliant products"[2].

Installing and configuring an SMD product at a practice involves a number of technical steps that require specialist skills and knowledge. You need to decide whether you are equipped to do this work yourself or whether you require technical assistance. Typically this work will be done by a representative of the SMD product supplier, since it requires detailed technical knowledge of the SMD product being installed and configured.

Whoever installs and configures the SMD product is referred to as a "commissioning agent" for the purpose of this document. Section 3 describes what needs to be done by the commissioning agent. It is expected that the tasks can be performed without the commissioning agent needing to visit your practice.

Even if you engage a commissioning agent to undertake the technical work of installing and configuring the SMD product, some tasks require the involvement of practice staff. The commissioning agent will need to prompt or guide you about when and how to complete the following tasks, and may provide tools to automate some of them:

- Publish and link your HPI-O and HPI-Is in the Healthcare Provider Directory (HPD) (and any other public healthcare directories approved by the practice).
- Enter details for an Endpoint Location Service in any HPI-O records for your practice which you publish in the HPD. This will allow other parties to locate you in order to send you messages.

[2] Quote from *Practice Incentives Program eHealth Incentive guidelines*, February 2013, Department of Human Services.

- Install either your NASH PKI Certificate for Healthcare Provider Organisations or your DHS eHealth Record Organisation PKI Certificate.
- If you outsource the operations of your IT systems, you may need to register in the HI Service that your practice has authorised a particular Contracted Service Provider to act on your behalf when interacting with the HI service. This can be done via Health Professionals Online Services (HPOS), humanservices.gov.au/hpos.
- The last task is to ensure that you have a completed and signed copy of the Commissioning Requirements Checklist in Appendix A. Retain this as evidence that your SMD product has been properly installed and configured for operation in accordance with the PIP eHealth Incentive requirements.

2.6 Timeline to meet PIP eHealth Incentive requirements 1 and 2

Sections 2.3, 2.4, and 2.5 describe tasks required to fully satisfy the PIP eHealth Incentive secure messaging capability requirements. The tables below give the critical dates related to these tasks and the tasks required for PIP eHealth Incentive requirement 1.

PIP eHealth Incentive requirement 1: Integrating Healthcare Identifiers into Electronic Practice Records

Activity	Critical date
Your practice has applied for or obtained an HPI-O.	1 February 2013
Your practice has selected a desktop clinical system from the *PIP eHealth Product Register for Healthcare Identifiers.*	1 February 2013
Your HPI-O is recorded in your desktop clinical system.	1 February 2013 or when obtained
Each general practitioner's HPI-I is recorded in your desktop clinical system.	1 February 2013

PIP eHealth Incentive requirement 2: Secure Messaging Capability

Activity	Critical date
Your practice has applied for a NASH PKI Certificate for Healthcare Provider Organisations (if you do not have a DHS eHealth Record Organisation PKI Certificate).	1 February 2013 or within 2 weeks of receiving HPI-O
Your practice has either: • a standards-compliant product that is listed on the *PIP eHealth Product Register for Secure Messaging* (nehta.gov.au/pip); or • written advice from one of the vendors listed on the *PIP eHealth Product Register for Secure Messaging* that their listed product will be available to the practice in order to meet the last compliance point below.	1 February 2013 or within 4 weeks of receiving your NASH PKI Certificate for Healthcare Provider Organisations
Your practice has a written policy to encourage the use of standards-compliant secure messaging.	1 February 2013
Your practice must be able to verify that your compliant SMD product has been installed and configured in accordance with this document.	1 August 2013

3 For commissioning agents

3.1 Introduction

A commissioning agent is the person responsible for installing and configuring an SMD product for use by a general practice in the context of the PIP eHealth Incentive.

This role may be fulfilled by any party who has the technical knowledge and skill to carry out the tasks, but typically would be one of the following: SMD product supplier, secure messaging service provider, Endpoint Location Service operator, systems integrator.

3.2 Recommended reading

It is recommended that commissioning agents are familiar with the following documents:

- E-Health Secure Message Delivery Technical Overview, Version 1.0, 28 September 2009

  https://www.nehta.gov.au/implementation-resources/ehealth-foundations/EP-1880-2014/NEHTA-1000-2009

- ATS 5822 – E-Health secure message delivery

  infostore.saiglobal.com/store/details.aspx?ProductID=1391035

- Endpoint Location Service Technical Service Specification, Version 1.3, 15 November 2010

  https://www.nehta.gov.au/implementation-resources/ehealth-foundations/EP-1880-2014/NEHTA-1157-2010

- Healthcare Identifiers Service User Guide for Practice Managers, Version 1.0, 14 December 2012

  https://www.nehta.gov.au/implementation-resources/national-infrastructure/EP-1826-2014/NEHTA-1164-2012

- Clarification on Messaging and CDA Packaging

  https://www.nehta.gov.au/implementation-resources/clinical-documents/EP-2241-2016/NEHTA-1270-2013

3.3 Obligations and requirements

As a commissioning agent assisting a general practice in implementing secure message delivery, you are responsible for ensuring that the chosen SMD product and its implementation meet and comply with the requirements outlined in this document.

Most requirements will be met by you directly or by the products and services provided by your organisation or other parties.

Some requirements will need the general practice to carry out certain tasks. As a commissioning agent, you will need to guide the practice regarding when and how to complete these tasks.

Section 4 expands on each requirement in the SMD Commissioning Requirements Checklist in Appendix A, with a guideline for how the requirement is to be met.

As a commissioning agent, you are required to complete and sign the SMD Commissioning Requirements Checklist in Appendix A for the general practice.

4 Requirements and guidelines

4.1 Product configuration

4.1.1 Requirement

The product is installed in a configuration which suits the requirements and capabilities of the general practice regarding the secure operation of web services.

4.1.2 Guideline

As commissioning agent, compliance with this requirement can be met as follows:

- **Determine the product configuration that suits the practice's technical capability regarding the secure operation of web services.**

  Some SMD product configurations require the healthcare organisation to operate web service endpoints that accept requests over the internet from external systems. Other SMD product configurations simply require the healthcare organisation to operate systems that only ever call out to external systems (either to send messages or to retrieve messages and transport responses from an intermediary).

- **Ensure the product is installed in a configuration which meets the practice's preferences regarding the operation of web services.**

  If the practice has elected a configuration that requires software installed within the healthcare organisation's local network to connect with externally operated intermediaries, you will need to install and configure the product to be able to access those intermediaries.

4.2 Send and receive capability

4.2.1 Requirement

The product is configured to send and receive messages using the Sender and Receiver roles as defined in the SMD specification.

4.2.2 Guideline

The capability to send and receive messages using the Sender and Receiver roles is a mandatory requirement for the product to be listed on the *PIP eHealth Product Register for Secure Messaging*.

As commissioning agent, you must ensure that the product as installed is configured to deliver both capabilities.

4.3 Use SMD where feasible

4.3.1 Requirement

The product is configured to use SMD as the general practice's default method of sending secure messages to other healthcare organisations, where feasible.

4.3.2 Guideline

A product which is listed on the *Digital Health Incentive Product Register for Secure Messaging* is expected to carry out the obligations and functions required of the role(s) when it is deployed. The SMD specification does not define the interface between the clinical systems and the SMD roles of Sender or Receiver. If the product is a Sender or Receiver, it will therefore be able to use whatever method (HL7 file transfer, Application Programming Interface (API), or other protocol) best suited to interface to the desktop clinical system. However, when the message is sent or received from the practice, the transaction must be in accordance with the SMD specification, if this is technically feasible.

The practice may have other proprietary products for electronic communication which operate concurrently with its SMD product. However, the system(s) used for electronic communication by a practice should be configured to attempt to first send a message using an SMD Sender, before failing over to an alternative method(s).

As commissioning agent, you will need to ensure that the product (Sender role) is configured to operate as follows:

- It must attempt to first establish a connection to an SMD endpoint to send each message to the healthcare organisation that is identified as the intended recipient of the message.
- It may fail-over to an alternative mechanism ***if and only if*** the target healthcare organisation does not have a designated SMD endpoint for that type of message or the Sender fails to connect to the designated SMD endpoint. If an alternative mechanism is not available or not successful, the Sender must escalate to human intervention.
- The Sender can determine whether a particular healthcare organisation has SMD capability by attempting to look-up the HPD and/or other public service directories to find the Uniform Resource Identifier (URI) for the Endpoint Location Service (ELS) used by the organisation.

  If:

  - the HPI-O is not in the HPD or other directories (see Section 4.10); or
  - the HPI-O record does not have a URI for an ELS (see Section 4.12); or
  - an interaction record matching the HPI-O and service category corresponding to the payload scheme for the message cannot be found (see Section 4.5),

  Then:

  - the Sender may conclude that the healthcare organisation does not have a capability to receive this type of message using SMD, in which case it may use an alternative, proprietary mechanism for electronic communication or escalate to human intervention, e.g. an email notification. The method of escalation is not defined in the SMD specification.

4.4 Services directory

4.4.1 Requirement

The product is configured to identify, locate and access the Endpoint Location Service designated by the healthcare organisation which is the target recipient of each message for any function or purpose defined in the SMD specification which requires the use of a services directory.

4.4.2 Guideline

This requirement may be met in a number of ways. For example, one or more directories and local address books may be used to locate the appropriate ELS instance for a specified receiver organisation. The approach used may impact the ability of the practice to send messages to other healthcare organisations and hence their ability to “use SMD where feasible”.

Regardless of which approach is used, the product is expected to respect the role of the HPD as the “single point of truth” for the relationship between an HPI-O and an ELS instance. Other directories and local address books may cache these relationships, but must refresh their caches when appropriate to re-synchronise with the HPD. The following failure conditions indicate that a cache may no longer be in synchronisation with the HPD and can be expected to trigger a cache refresh and a delivery re-try (if the receiver endpoint changes as a result of a cache refresh):

- Failure to contact a target ELS instance.
- Failure to locate a suitable ELS interaction record in a target ELS instance.
- Failure to receive a final transport acknowledgement before the expiry time nominated in the original message metadata.

As commissioning agent, you will need to ensure that the product is configured to identify, locate and look up the ELS used by the target recipient of each message, regardless of which party operates the ELS.

4.5 Interaction records

4.5.1 Requirement

The ELS instance used by the practice contains an interaction record for each service category published on ns.electronichealth.net.au/ that the practice’s desktop clinical system can receive.

4.5.2 Guideline

Interaction records are the records which are managed by an ELS instance.

Interaction records can be entered in an ELS instance by messaging software using the publish interface of the ELS instance or directly by the ELS instance operator using an alternative mechanism. The method used for a particular ELS instance will be determined by the ELS instance operator. In most cases, the ELS interaction records will be created automatically as part of the product installation.

Each interaction record in the ELS instance nominated by the practice must consist of the following:

- *target*: a fully-qualified identifier containing the HPI-O for the practice. The HPI-O should be the same as the HPI-O published in the HPD.
- *serviceCategory*: URI representing the payload scheme for the message. There must be a service category for each payload scheme that the practice's clinical information system is able to receive and process.

  Note: As commissioning agent, you should explain to the practice how the SMD product can be reconfigured at a later point, if necessary, to reflect changes in the ability of the desktop clinical system to receive and process messages of a new type or format (such as discharge summaries, specialist letters, referrals, event summaries as specified by NEHTA) at any time after the interaction records are first created.
- *serviceInterface*: URI representing the technical service (e.g. corresponding to the security mechanism for the service. In the case of SMD endpoints, this is always TLS).
- *serviceEndpoint*: URL for the operation on the instance of the web service used by the practice for receipt of the specified message type.
- *serviceProvider*: Identifier of the organisation that is hosting the web service endpoint designated in *serviceEndpoint*. The identifier must be one of:
  - an HPI-O which is the same as the HPI-O for the target (if the practice is hosting its own web service endpoints);
    or
  - an HPI-O which is in the same HPI-O network structure as the HPI-O for the target (if the practice is hosting its own web service endpoints);
    or
  - a CSP number which has been linked in the HI Service to the HPI-O for the target (if the web service endpoint is hosted by a party that manages the practice's clinical information under a CSP arrangement).
- *certRef*: zero or more elements indicating a certificate reference and certificate use for the PKI certificate associated with the particular instance of the web service designated in *serviceEndpoint*. The certificate reference must refer to a NASH PKI Certificate for Healthcare Provider Organisations.

A list of service categories for any payload scheme defined by NEHTA is available at: ns.electronichealth.net.au/browse-service-category.html.

As commissioning agent, you should work with the ELS instance operator to ensure that:

- There is an interaction record in the ELS instance nominated by the practice for each payload scheme the practice's clinical information system is able to receive and process.
- Each interaction record contains the correct information in each element as described above.
- There is an appropriate contractual arrangement in place to create and maintain interaction records in the ELS instance nominated by the practice (if applicable).

The interaction records are expected to be entered into the appropriate ELS instance messaging software as part of the installation process.

4.6 PKI certificates

4.6.1 Requirement

The product is configured to use either a NASH PKI Certificate for Healthcare Provider Organisations or a DHS eHealth Record Organisation PKI Certificate to assert the identity of SMD Senders and Receivers.

4.6.2 Guideline

A NASH PKI Certificate can be obtained by using the eHealth Online Forms application tool. Additional information about obtaining the NASH PKI Certificate for Healthcare Provider Organisations is available on the DHS website www.humanservices.gov.au/pki

Note that the NASH PKI Certificate for Healthcare Provider Organisations and the DHS eHealth Record Organisation PKI Certificate are the same certificates used to access the My Health Record system.

4.7 End-to-end security

4.7.1 Requirement

The product is configured to operate in a manner that ensures the payload is secured between the origin of the clinical information and the intended recipient.

4.7.2 Guideline

A key feature of the SMD specification is the mechanism to provide payload security separately from any transport level security. This is designed to ensure the clinical content is secured “end-to-end” irrespective of whether one or more intermediaries are involved in the transport of the payload. It is important therefore to ensure that, when the product is installed, it is configured to operate in a way which is consistent with this intention.

As commissioning agent, you must ensure that the product is configured as follows:

- The SMD payload is signed using the signing certificate for the organisation which is the origin of the payload contents, i.e. the location where the content is stored/created.
- The SMD payload is encrypted for the target healthcare organisation (or its designated agent) before it leaves the location where the payload contents are stored/created.

The origin of the payload contents is the clinical information system that creates and stores the clinical records used to construct the payload. This may be in a very different location from where the Sender role is installed (especially if the Sender is operated by an agent/contracted service provider.)

In most cases, where the practice is both the originator of the clinical records and the operator of the SMD Sender role, this requirement is straightforward. The product must be configured to sign and encrypt the payload at the practice before transmitting the message to the recipient.

However, in cases where the practice has outsourced the management of its clinical information to a contracted service provider who stores the clinical records at a location external to the practice and has engaged a secure messaging service provider to operate its SMD services, care must be taken to ensure that the payload containing the clinical record is encrypted for the recipient before it leaves the location where the clinical content is stored.

As commissioning agent, you must ensure that the product is installed and configured such that the payload is encrypted or decrypted ***only in a secure environment***. A secure environment is one where applications and data can be protected from unauthorised access, in particular by applications or persons external to the practice. It would be inappropriate to install the product so that it encrypts or decrypts messages in a location which is external to the practice's inner firewall (such as in a DMZ).

4.8 Product is operational

4.8.1 Requirement

The product is operational with the ability to send and receive messages using the capabilities of the infrastructure services that have been configured for its use.

4.8.2 Guideline

This requirement can be met by undertaking a loopback test. This involves sending and receiving one or more test SMD message using the same HPI-O for both the sending and receiving organisations. This tests that requisite information is correctly defined in the HPD and ELS and demonstrates that the deployment of the SMD product can send a message to itself (with the aid of the infrastructure services needed to support the messaging process).

Performance of the loopback test requires that:

- An HPI-O record for the practice is published in the HPD and such other healthcare directories approved by the practice.
- Reference to an ELS instance has been entered into the ELS elements in the HPI-O record.
- Appropriate PKI certificates have been installed and configured for use by the product.
- A suitable interaction record with a service category for the test message is entered into the ELS instance.
- Test messages are sent in 'deferred mode'.

The commissioning agent shall confirm the success or failure of the loopback test by ensuring that a final transport response is received in response to each test message sent.

4.9 Integration with clinical information systems

4.9.1 Requirement

The product is integrated with the clinical information system(s) used by the general practice.

4.9.2 Guideline

In the context of the PIP eHealth Incentive, the messaging product is required to integrate with the desktop clinical system used by the practice for the purpose of ensuring the "use where feasible" requirement.

The SMD specification does not define the manner by which a message is transferred between the desktop clinical system and a separate messaging product.

Regardless of how the integration is achieved, the practice's systems (desktop clinical system and SMD product) should be able to perform the following functions automatically:

- Take a message produced by the desktop clinical system and transmit it via SMD.
- Receive a message via SMD and make it accessible to the desktop clinical system.
- Inform the user or desktop clinical system of the outcome of sending each message.
- If necessary, encapsulate the CDA package within the Medical Document Management (MDM) HL7 v2 specification, as described in the *Clarification on Messaging and CDA Packaging*.

Some products may simply maintain a record of messages sent and their status, leaving it to the user to periodically "check the logs" or run a report. Other products may provide a feature whereby the user is automatically notified of the outcome (especially if message delivery has failed). Confirm with the practice that the method provided by the product is acceptable to them, taking into consideration the criticality of reliable message delivery to their operation.

The commissioning agent should ensure that the practice understands the options available and help implement the desired level of integration.

4.10 Audit trails

4.10.1 Requirement

If the product provides the capability to maintain an audit trail of messages sent/received, this capability is activated for the practice.

4.10.2 Guideline

A general practice which is receiving payments under the PIP eHealth Incentive may need to provide evidence of messages sent and received if requested by DHS. If the product does provide an audit trail, the commissioning agent should ensure that this function is activated.

4.11 Healthcare directories

4.11.1 Requirement

The practice has published the HPI-O record(s) it wishes to be identified as the recipient(s) of messages in the Healthcare Provider Directory and any other public healthcare directories approved by the practice.

4.11.2 Guideline

The Healthcare Provider Directory (HPD) is operated by DHS as part of the HI Service.

The HPD is a listing of healthcare providers (individuals and organisations) registered with the HI Service and it underpins an effective secure messaging system. In particular, the HPD is a means by which other healthcare organisations can find the relevant HPI-Is and HPI-O for a practice in order to send clinical information in the form of messages (such as referrals, test results, discharge summaries) to the practice.

Publication in the HPD of the HPI-O for the SMD Receiver(s) for a practice is mandatory and the entry must include the details of the ELS instance that contains ELS interaction records for that HPI-O. It is ***strongly recommended*** that the practice's HPI-Is are also listed in the HPD and are linked to the appropriate HPI-O(s) that will act as the SMD receiver for those healthcare provider individuals.

While other healthcare directories exist in addition to the HPD, the latter is the authoritative source for the ELS instances used by a healthcare provider organisation and is accessible only to authorised users.

Publication in the HPD can be completed by the general practice using DHS Health Professional Online Services (HPOS). Guidance regarding the HPD is available in the *Healthcare Identifiers Implementation User Guide*.

As commissioning agent, you may need to provide a tool to automate the publication, or help the practice manually publish to the HPD.

4.12 Endpoint Location Service

4.12.1 Requirement

The practice has access to and the use of an Endpoint Location Service which implements the *Endpoint Location Service Technical Service Specification v1.3*.

4.12.2 Guideline

The Endpoint Location Service (ELS) is a fundamental component that supports secure messaging between healthcare organisations without requiring those organisations to have previous knowledge of each other.

In order for the SMD product to work correctly, the practice needs to obtain the use of an ELS instance. This ELS instance may be operated by the party that will operate the web service endpoint(s) for the practice (e.g. the practice itself or a secure messaging service provider) or by an independent source, such as the ELS instance provided by the NHSD.

As commissioning agent, you should do the following:

- Confirm that the ELS instance provided for use by the practice is an implementation of the Endpoint Location Service Technical Service Specification v1.3.
- Guide the practice's representative, or provide a tool, to enter the information to identify the ELS instance into each HPI-O record that the practice has consented to publish in the HPD and any other public healthcare directories approved by the practice.

The following information required to complete this task will need to be obtained from the ELS instance operator:

- Service Identity: a URI representing an identifier for the organisation which is operating the ELS instance
- Service Address: a URI representing the URL for the ELS instance.

4.13 Contracted service provider

4.13.1 Requirement

The practice has registered its association with its contracted service provider in the Healthcare Identifiers Service (if applicable).

4.13.2 Guideline

Some product offerings enable another party (such as a secure messaging service provider) to operate the web services used for sending and receiving messages on behalf of the practice. In some cases, this arrangement will require that party to have access to the HI Service. If this applies to the SMD product chosen by the practice, the web service operator will need to register with the HI Service Operator as a contracted service provider (CSP). In addition, the practice will need to authorise the CSP to act on its behalf with the HI Service Operator.

The practice must establish a link between the CSP organisation and the HPI-O for the practice in the HI Service. This must be done by the responsible officer who registered the practice with the HI Service.

As commissioning agent, you will need to determine whether this task is applicable and, if so, help the responsible officer for the practice to carry out this task (either manually or by providing a tool). Establishing a link can be done via Health Professionals Online Services (HPOS), humanservices.gov.au/hpos.

Appendix A SMD Commissioning Requirements Checklist

This checklist is to be completed and signed by the SMD commissioning agent.

General practice for which the SMD product is installed: _____

*__Note__: If "Yes" is the only option, this requirement is necessary to achieve compliance.

The product is installed in a configuration which suits the requirements and capabilities of the general practice regarding the secure operation of web services.	Yes ☐
The product is configured to send and receive messages using the Sender and Receiver roles as defined in the SMD specification.	Yes ☐
The product is configured to use SMD as the general practice's default method of sending secure messages to other healthcare organisations, where feasible.	Yes ☐
The product is configured to identify, locate and access the Endpoint Location Service designated by the healthcare organisation which is the target recipient of each message for any function or purpose defined in the SMD specification which requires the use of a Services Directory.	Yes ☐
The ELS instance used by the practice contains an interaction record for each service category published on ns.electronichealth.net.au that the practice's desktop clinical system can receive.	Yes ☐
The product is configured to use either a NASH PKI Certificate for Healthcare Provider Organisations or a DHS eHealth Record Organisation PKI Certificate to assert the identity of SMD Senders and Receivers.	Yes ☐
The product is configured to operate in a manner that ensures the payload is secured between the origin of the clinical information and the intended recipient.	Yes ☐
The product is operational with the ability to send and receive messages using the capabilities of the infrastructure services that have been configured for its use.	Yes ☐
The product is integrated with the desktop clinical system(s) used by the general practice.	Yes ☐
If the product provides the capability to maintain an audit trail of messages sent/received, this capability is activated for the practice.	Yes ☐ N/A ☐
The following steps are typically performed by a tool included with the SMD product that is executed from within the GP's local IT network.	
The practice has published the HPI-O record(s) it wishes to be identified as the recipient(s) of messages in the Healthcare Provider Directory and any other public healthcare directories approved by the practice.	Yes ☐
The practice has access to and the use of an Endpoint Location Service which implements the *Endpoint Location Service v1.3 Technical Service Specification*	Yes ☐
The practice has registered its association with its contracted service provider in the Healthcare Identifiers Service (if applicable).	Yes ☐ N/A ☐

Signature of commissioning agent _____

Full name of commissioning agent _____

Name of commissioning agent's organisation _____

Name of product supplier _____

Name and version of SMD product installed _____

Date _____