eHealth Clinician's User Guide

For Medical Practices (GPs and Private Specialists)

nehta | eHealth

National E-Health Transition Authority Ltd

Level 25
56 Pitt Street
Sydney, NSW, 2000
Australia.

www.nehta.gov.au

Contributing Author

Jeff Parker, JP Consulting (Aust) Pty Ltd

www.jpconsulting.com.au

Disclaimer

The National E-Health Transition Authority Ltd (NEHTA) makes the information and other material (‘Information’) in this document available in good faith but without any representation or warranty as to its accuracy or completeness. NEHTA cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control

This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

TABLE OF CONTENTS

This page intentionally blank

1 Introduction

This is Release 2 of the eHealth[1] Clinicians User Guide (User Guide)[2]. If your practice has already implemented Healthcare Identifiers (either through following the guidance in Release 1 or by other means), then you may find it beneficial to skip ahead to Chapter **2**[3], which includes a roadmap of recommended actions for the effective implementation, verification and beneficial use of eHealth in a medical practice.

1.1 Intended Audience

This User Guide is intended primarily for Medical Practices, i.e. general practices and those of private specialists, especially:

- Practice principals/owners, practice managers (including managers for quality and governance) and staff of medical practices who plan to upgrade their Desktop Software to a version that supports new eHealth functionality[4] as it is released; and
- Medicare Locals (and where relevant Divisions of General Practice), Colleges and other organisations that provide support to medical practices in the implementation and use of eHealth.

The User Guide includes material that is relevant to both general practices and private specialist practices, and also material that is specific to each. In the interests of providing relevant and useful information for practices implementing eHealth, examples and evidence for topics and recommendations are included that are generally applicable for both types of medical practices.

Practices of other healthcare professionals, e.g. allied health and in aged and community care, may also find this guide useful in increasing their understanding and in planning, implementing and using eHealth.

[1] eHealth is defined by the World Health Organisation as being the "combined use of electronic communications and information technology in the health sector".

[2] For clarity, the previous Release was called the eHealth Clinician's Desktop User Guide.

[3] Note that in addition to the internet website addresses included in this PDF document, the cross references to chapters and sections within it can also be clicked on to be taken to the referenced location. These links are displayed in **bold blue**. In addition the entries in the Table of Contents may be clicked on as an additional aid to navigation in the document.

[4] The eHealth functionality referred to is as outlined in the Australian Government's eHealth Program. See **http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/theme-ehealth** for details.

1.2 Purpose

This guide is intended to assist you and your practice to:

- Understand the national eHealth system[5] and related eHealth features that have become available in recent updates to your Desktop Software, and how the features could be beneficial;
- Identify the work process, organisational and governance changes that may be necessary in your practice so that you can benefit from the use of eHealth, and to plan and implement these;
- Understand the prerequisites for the implementation and use of the eHealth features, and undertake the necessary once-off pre-implementation set up steps;
- Plan and implement the eHealth features included in the updated version of your Desktop Software;
- Verify that your implementation of the eHealth features operates correctly; and
- Gain initial and ongoing value from eHealth through guidance on its effective use, quick reference checklists and access to education and support resources.

1.3 Scope and Environment of this User Guide

Desktop Software Needs to Conform with National eHealth Specifications

The National E-Health Transition Authority (NEHTA[6]) has contracted with Desktop Software vendors to incorporate a number of key national eHealth specifications[7] into software products commonly used by medical practices. Other vendors are also updating their products to be conformant with the specifications and hence enable users of their products to participate in the national eHealth system.

Conformance to those national eHealth specifications is required for software products to interact electronically with the national eHealth system. The process for this is explained later in Section **6.1**.

[5] The words "national eHealth system" are used in this User Guide to describe all of the functionality that is being implemented to enable enhanced electronic exchange and sharing of healthcare information across the Australian healthcare system, i.e. including the eHealth record system and other functionality, e.g. secure message delivery – Chapter **3** provides an overview of the components of the national eHealth system.

[6] See **http://www.nehta.gov.au**.

[7] One of NEHTA's roles is to develop specifications and standards (through working with industry and standards bodies) for eHealth that are to be implemented in the Australian healthcare system. This requires modifications to software used by healthcare providers.

The list of conformant software products is available at:
https://epipregister.nehta.gov.au/[8]

If your Desktop Software vendor's product is not listed in the above Register, you should contact them to see if they are including the eHealth features into their products and to understand the extent of their planned conformance with the specifications.

It is important that you realise that it is *necessary* for your practice to use software and services that are conformant to these specifications, but that this is not *sufficient*. You need to assess the fit of the software and services to your practice's business needs, as some may have features or limitations that won't suit the way your practice wishes to participate in the national eHealth system, e.g. by not being able to accommodate multiple organisational identifiers and/or multiple organisational digital (or PKI) certificates (both explained later).

Current and Future eHealth Features

This version of the User Guide provides guidance on the currently available eHealth functionality that is built into conformant Desktop Software. The national eHealth system will continue to evolve to provide, in summary:

- The national personally controlled electronic health record (PCEHR) system, including the creation and use of Shared Health Summaries, Event Summaries and other related features;
- Healthcare Identifiers;
- National Authentication Service for Health (NASH) and related PKI certificates (for security);
- Clinical Terminology/Coding;
- Secure Message Delivery (SMD), with improved security, including eSignatures;
- eReferrals, eDischarge Summaries, and eSpecialist Letters;
- eMedication Management, including Electronic Transfer of Prescriptions (ETP) and improvements to ePrescribing; and
- eDiagnostic Services, including eRequesting and eReporting for pathology and diagnostic imaging.

Section **3.1** (and those that follow it) describes these eHealth features in greater detail.

[8] This website lists products in the ePIP categories (see Section **4.5**) that have passed conformance testing.

Further versions of the User Guide will be developed to align with future releases of nationally specified eHealth functionality, and for other community-based healthcare professionals, e.g. allied health professionals and those working in aged care.

Practice Incentives Program for eHealth (ePIP)

In May 2012 the Federal Health Minister announced an update to the Practice Incentives Program for eHealth designed to encourage the uptake of eHealth in general practices. The updated ePIP became effective in February 2013 and is discussed in Section **4.5**.

The ePIP payments are accessible to accredited general practices that use conformant Desktop Software against a number of eHealth related requirements. Vendors of these products (and non-conformant products) are motivated to ensure their products enable their customer practices to meet the ePIP requirements and hence access the available payments.

It is anticipated that vendors will increasingly include eHealth functionality in their products and seek to be registered as being conformant. As a number of these Desktop Software products are used also by private specialists, it is envisaged that specialist practices will increasingly be able to participate in the national eHealth system over time.

Stay Up To Date with eHealth Developments

You can be kept up to date with national eHealth program developments by subscribing to receive update emails at:

http://www.yourhealth.gov.au/subscribe

You may also find it beneficial to register on NEHTA’s website to obtain access to useful resources and to receive updates when things change:

https://www.nehta.gov.au

1.4 Structure

The User Guide has six main components, which align with the chapters that follow:

1. **eHealth Implementation Roadmap** – a summary of the key steps that are required and recommended for medical practices to undertake to effectively participate in the national eHealth system;

2. **User Guide Context** – overviews the eHealth system and its features, and explains why your practice might undertake to use them;

3. **The Benefits to Your Practice** – describes the benefits you should reasonably expect from using the national eHealth system;

4. **Planning and Implementation** – outlines what you need to do to implement the eHealth features – the goal being to achieve meaningful use from eHealth

for those clinical transactions conducted by your practice that the features support;

5. **Verification** – outlines steps you could undertake to verify the correct implementation and operation of the eHealth features; and
6. **Effective Use** – outlines ideas and guidance about things to do so your practice might benefit from eHealth. Includes quick reference checklists for clinicians and staff on the efficient use of the eHealth features, and links to further information and who to contact if you need advice or assistance.

1.5 Important Information and Disclaimer

This guide does not replace the advice, guidance and support provided by your software vendor. As the guide is generic (i.e. applicable to all upgraded Desktop Software products) there will be instances where additional important information will be provided by your vendor.

The national eHealth system includes the ability for your practice to share clinical patient data electronically (inbound and outbound), possibly for the first time. As with the use of all eHealth functionality, including electronic records, there are risks of unintended consequences if not implemented and operated correctly. This risk should be lower than at present as Healthcare Identifiers (discussed later) act as a key to correctly match patient, practitioner and practice data, and the security and privacy measures implemented in the system are designed to minimise unlawful and unauthorised access to healthcare information.

As the eHealth features require your practice's computer systems to access external online services via the Internet, if not done already, you should also:

- Review the IT security arrangements in your practice and take action to address any shortcomings or areas of risk[9]. Note also that practices are required to have written policies in a number of areas (including for security and user account management) for participation in the eHealth record system, which is discussed later; and

- Review the reliability and performance of your practice's Internet connection and consider upgrading if warranted.

It is recommended that you seek advice and support from your Software Vendor or other organisations that provide you with IT and/or eHealth support. Your Medicare Local or College may also be able to provide advice, assistance or services to support planning and implementing eHealth in your practice.

[9] See Section **3.2.3** for information about eHealth security. The RACGP provides very useful information and guidance for medical practices on computer and information security. For information on its Computer and Information Security Standards (CISS) and the National eHealth Security and Access Framework (NESAF) see **http://www.racgp.org.au/your-practice/e-health/cis/**.

This User Guide should be read in conjunction with your software vendor's release notes, and implementation and user guides, which will provide relevant product-specific information. This documentation should be included with the software update kit provided by your vendor, or available from their website.

See Chapter **8** for links to websites and other useful information related to obtaining advice and support.

Disclaimer

This User Guide is provided to assist you to plan and implement eHealth in your practice. In recognising that many different structures and business and service models exist in medical practices, it cannot and does not provide guidance specific to your practice. The guide is not an exhaustive list of all the actions your practice may need to undertake and you should take your own steps to ensure your obligations are met and your practice is prepared and able to participate effectively in the national eHealth system.

In addition, requirements, timeframes, processes, forms and other instruments referenced in the guide are subject to change, so you should check the currency and accuracy of information contained herein before relying upon it.

1.6 Key Learning and Information Resources

The following is a list of information resources that you may find useful for introductory or other reference purposes on eHealth generally and on the national eHealth system specifically. It is not essential that you read through all of these at this point in time, as many are referred to later in the guide itself.

Key eHealth-related Websites

Australian Government websites, which have information, including brochures and learning modules on eHealth, and the ability to subscribe for updates and notification of key events:

http://www.ehealth.gov.au and **http://publiclearning.ehealth.gov.au/hcp**

http://yourhealth.gov.au/ehealth

http://www.health.gov.au/ehealth

http://www.youtube.com/user/eHealthAus

http://www.nehta.gov.au

Professional and Peak Body eHealth websites:

http://www.racgp.org.au/ehealth

https://ama.com.au/policy/ehealth

http://www.aapm.org.au/resources/ehealth.aspx

http://www.amlalliance.com.au/medicare-local-support/ehealth

Section **3.5** lists the legislation relevant to eHealth.

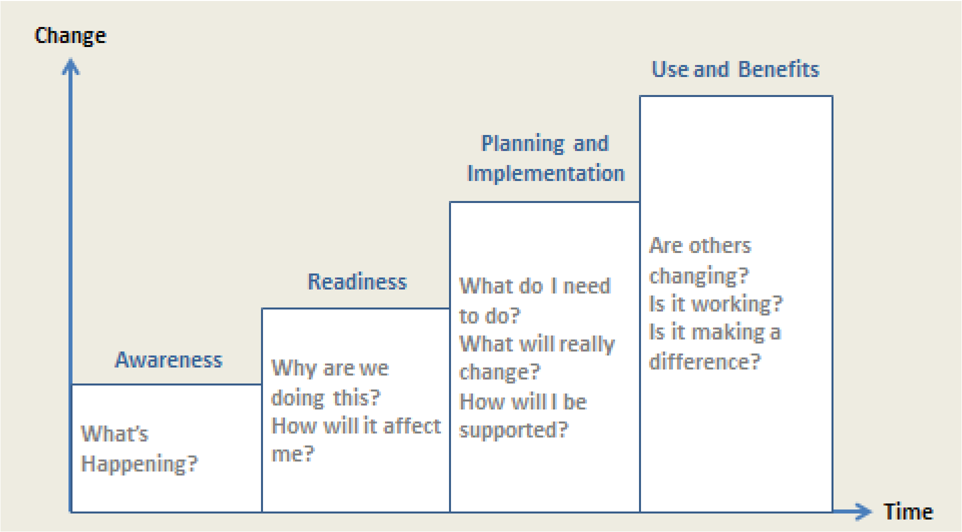
This page intentionally blank

2 eHealth Implementation Roadmap for Medical Practices

Adopting new technologies, including eHealth innovations, is never as straight-forward as it seems. For the eHealth system, consumers and healthcare professionals are being asked not only to adapt existing processes of healthcare, but also to adopt and use technology to perform new activities (including the use of shared patients' eHealth records).

A national approach is therefore needed to foster adoption of the eHealth system.

The following diagram shows the phases that consumers and healthcare professionals may go through before using the eHealth system in a meaningful way to support their healthcare interactions.


Change
Use and Benefits
Planning and Implementation
Readiness
Awareness
What's Happening?
Why are we doing this? How will it affect me?
What do I need to do? What will really change? How will I be supported?
Are others changing? Is it working? Is it making a difference?
Time

The national approach includes an active role for Medicare Locals in providing advice, support and education, along with important roles for Colleges, the Australian Government Department of Human Services (Human Services) and NEHTA. Many software suppliers (including of the commonly used Desktop Software systems) have also been active participants in the development of the national eHealth system. These vendors provide information, training and support that practices would also find beneficial.

To assist medical practices navigate a pathway to implement eHealth and gain the expected benefits, the roadmap below summarises the key steps necessary and includes links to sections in this User Guide that contain more relevant detail. These section references can be clicked on to take you directly to the relevant place in the document, should you wish.

If you have already partly implemented or have a good understanding of eHealth, you may find it useful to use the roadmap below as a check-list and to go directly to the sections that are relevant to the particular sub-set of activities needed for your practice. Otherwise it would be prudent to read the whole User Guide and follow it in detail.

1. Increase Your Practice's eHealth Awareness and Understanding

1. Read the sections in this User Guide about eHealth and its benefits – Chapters **3** and **4**
2. Selectively read from the available eHealth learning and reference resources – Section **1.6**
3. Subscribe to receive email updates on the national eHealth system – Section **1.3**
4. Engage with your Medicare Local's eHealth Team and participate in its activities – Chapter **8**
5. Read what your College has to say about eHealth and engage in their programs – their website
6. Read the AMA's Guide to the eHealth Record System – Section **1.6**
7. Read your Desktop Software vendor's eHealth information – their website and manuals
8. Discuss and promote the introduction of eHealth in your practice with clinicians and staff
9. Encourage all clinicians and staff to register for their own eHealth record – **my.gov.au**

2. Get Your Practice Ready for eHealth

1. Establish/Review Clinical Governance in your Practice and connect it with the Clinical Governance model used by your Medicare Local – Section **5.1**
2. Review your PC and network (including Internet) security and performance, and update/upgrade if necessary, inc. implement the RACGP's CISS – Section **3.2.3**
3. For general practices, review requirements for the updated ePIP program – Section **4.5**
4. Check that your Desktop Software is conformant with at least the requirements of the HI Service – Section **3.2.1** (It will also need to be conformant for other eHealth functions – discussed below)
5. Record eHealth details, e.g. of PKI certificates held in the Practice along with other key security and access control related information, in a register as part of your Quality System – Section **5.3**
6. Organise a visit from your Medicare Local's eHealth Team to your practice to review status and assist in eHealth planning and education
7. Contact your Medical Defence Organisation (MDO) about coverage for eHealth at both practice and practitioner levels

3. Plan and Implement the Essential Prerequisites for eHealth

1. Undertake data quality improvement activities, including using a CDSA Tool – Section **5.2**
2. Educate clinicians and other Desktop Software users to not use free-text fields to enter key patient data and to always select from drop-down lists and check boxes – Section **3.2.4**
3. Check if the simple model of a single HPI-O can apply to your practice – Section **5.4.3**, otherwise determine the preferred HPI-O structure – Section **5.4**
4. Understand the formal Roles required for HI and PCEHR (e.g. RO, OMO) and allocate staff to them – Section **5.4.4**
5. Identify any additional PKI certificates required in your practice – Section **3.2.3**
6. Identify the relevant Human Services forms (for the HI Service, Roles and PKI certificates), complete and submit them (most can be done online with HPOS) – Section **5.6.1**
7. Plan and implement the HI Service in your practice, including installation of the relevant update of your Desktop Software – Section **5.6.2**
8. Ensure practice, clinician and authorised staff information is correctly listed in your Desktop Software and, where appropriate, in the HPD (and marked for publication), and any other relevant directories – Section **3.2.1**
9. Verify that the HI Service operates correctly with your Desktop Software – Section **6.2**
10. Decide on an approach to download IHIs for active patients and where necessary update patient data in your Desktop Software – Section **5.7.1**
11. Decide on the approach and timing to implement further eHealth functions, as below

4. Plan and Implement the eHealth Record System in Your Practice

1. Check that your Desktop Software is or is capable of being conformant for the eHealth record system – Section **3.3.3**
2. Familiarise yourself and your practice with the legislative framework for the eHealth record system – Section **5.5.1**
3. Familiarise yourself (the Practice Principal, at least) with the PCEHR Participation Agreement – Section **5.5.1**
4. Develop and implement written policies as required by the PCEHR Rules – Section **5.5.1**
5. Identify requirements for formal Roles and assign to appropriate staff – Section **5.5.1**
6. Review appropriateness of your HPI-O structure and if necessary decide on use of Access Flags – Section **5.3**
7. Obtain necessary NASH PKI certificate(s) and record details in your practice's register – **Step 2** in Section **5.6.1**
8. Decide if your practice needs a list of authorised healthcare provider individuals for access to the Provider Portal and if so set it up – Section **5.7.2.1**
9. Register your practice (if not already done), including have each legal entity sign the Participation Agreement, and submitting any other required forms – Section **5.6.1**
10. Install update to Desktop Software that includes eHealth Record access and configure it correctly – Section **5.6.2**
11. Verify installation and operation of eHealth Record access functionality (and optionally Provider Portal access) – Section **6.3**

5. Plan and Implement SMD, ETP and Other eHealth Functions

1. Check that your Desktop Software is or is capable of being conformant for SMD, ETP and other required functions – Sections **3.2.2** and **3.3.2**
2. If not already done for PCEHR usage in your practice, obtain NASH PKI (Organisation) certificate (for use by SMD) and record details in your practice's register – **Step 2** in Section **5.6.1**
3. For SMD, ensure your HPI-O is loaded into the ELS directory provider to be used by your practice – Section **5.5.3**
4. If your SMD vendor(s) request it, authorise them to act as a CSP on behalf of your practice – section **5.5.3**
5. For ETP, choose and enter into a commercial arrangement with a PES – Section **5.5.4**
6. Install update to Desktop Software that includes required eHealth functionality and configure it correctly – Section **5.6.2**
7. Verify installation and operation of Desktop Software update/upgrade and implemented eHealth functionality – Sections **6.5** and **6.6**

6. Use eHealth Effectively in Your Practice

1. Handout the eHealth Usage Check Lists to clinicians and staff in your Practice – Chapter **7**
2. Identify patients who may benefit from having an eHealth Record, talk with them about it and assist with having it set up where appropriate – Section **7.1**
3. Keep your Desktop Software and IT environment up to date and fit for purpose
4. Maintain the training of your clinicians and staff in eHealth
5. Maintain awareness and compliance by your clinicians and staff of the written policies required for the eHealth record system, and update the policies as required
6. Continue your Practice's Clinical Governance and Quality Improvement activities
7. Keep data about your practice up to date in the HPD, HPOS and any other relevant directories and encourage your practice's clinicians and relevant staff to do the same – Section **3.2.1**
8. Keep key eHealth information in your Quality System up to date – Section **5.3**
9. Monitor usage and report eHealth-related Clinical Incidents – Section **7.3**

3 User Guide Context and eHealth System Overview

This version of the User Guide (Release 2) builds on the previous release[10] that encouraged practices to carefully plan and then implement an update to their Desktop Software that included the following eHealth functionality:

- Healthcare Identifiers; and
- Clinical Document (CDA[11]) Viewing

Implementing Healthcare Identifiers in your practice is an **essential prerequisite** for the implementation of other eHealth functionality, including the use of the national eHealth record system. This release of the User Guide now also incorporates the national eHealth record system[12] as well as other eHealth features that may be included in the latest version of your Desktop Software[13]. The User Guide will continue to be updated, including via an online web version, to incorporate additional and updated eHealth features relevant to medical practices as they are released.

This chapter describes the eHealth functionality that the latest version of your Desktop Software may include and other eHealth functions that you should expect in later versions. The chapters that follow outline the benefits your practice should reasonably expect from their implementation, the important steps required to successfully implement the latest version, and other things you may consider doing to verify the correct operation of the eHealth features and achieve the expected benefits.

3.1 Development and Availability of eHealth Features

Vendors of Desktop Software and messaging products, Human Services, NEHTA, oH and their eHealth delivery partners have worked together to make the components of the national eHealth system available for use by medical practices

[10] Release 2 of this User Guide replaces Release 1 (the previous version), which was made available in July 2012. There is no need to read Release 1 in order to follow the guidance offered in this version.

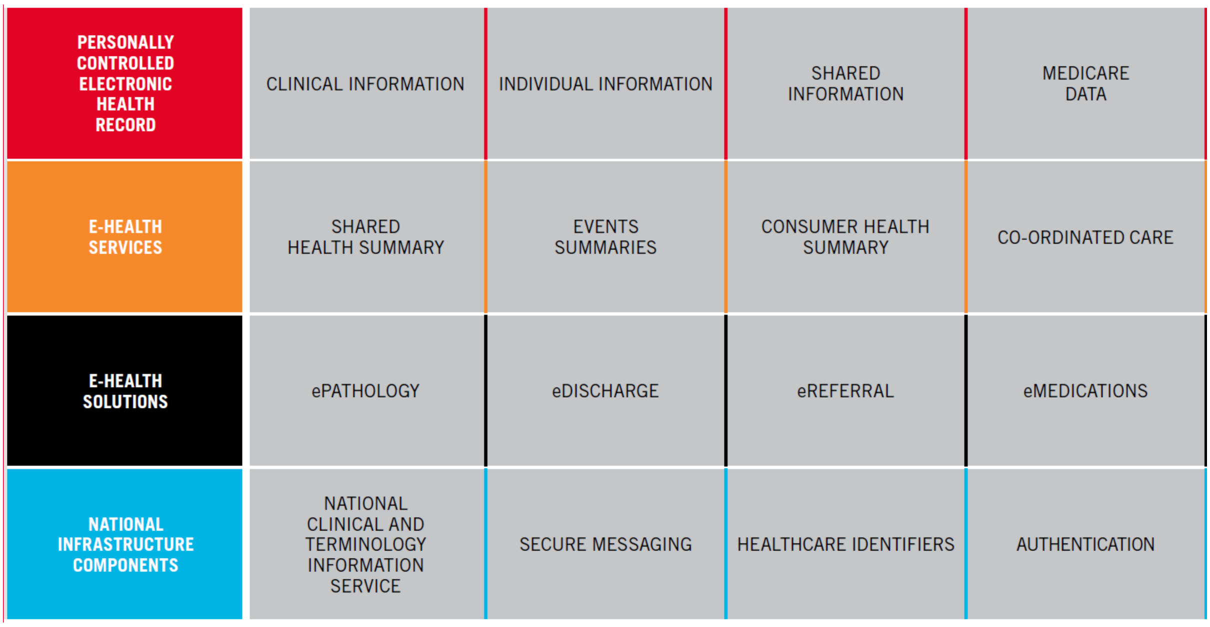
[11] CDA stands for Clinical Document Architecture, which is a standard for defining electronic versions of documents such as referrals, discharge summaries, etc. – see Section **3.2.5** for further information.

[12] For the sake of clarity, the national eHealth *record* system is a part of the national eHealth system, which was described earlier in Section **1.2**.

[13] See Section **1.3** for a link to a website where you can check what eHealth features are included in the version of the Desktop Software your practice is using. Note too that some software vendors may include additional eHealth-related functionality in their updated products, and also enhancements and bug fixes to the product itself. Please check the release notes that came with the software update.

and other healthcare provider organisations. Different parts of the national eHealth system are being released at different stages depending on development and deployment cycles, and legislative and regulatory processes.

The diagram below illustrates the major elements of the national eHealth system and shows that the elements build piece by piece to add functionality to the national eHealth record system. Over time eHealth functionality will become richer thus making the system increasingly more useful and beneficial to healthcare providers and patients.



PERSONALLY CONTROLLED ELECTRONIC HEALTH RECORD	CLINICAL INFORMATION	INDIVIDUAL INFORMATION	SHARED INFORMATION	MEDICARE DATA
E-HEALTH SERVICES	SHARED HEALTH SUMMARY	EVENTS SUMMARIES	CONSUMER HEALTH SUMMARY	CO-ORDINATED CARE
E-HEALTH SOLUTIONS	ePATHOLOGY	eDISCHARGE	eREFERRAL	eMEDICATIONS
NATIONAL INFRASTRUCTURE COMPONENTS	NATIONAL CLINICAL AND TERMINOLOGY INFORMATION SERVICE	SECURE MESSAGING	HEALTHCARE IDENTIFIERS	AUTHENTICATION

This release of the User Guide describes the following eHealth components:

eHealth Features Described in this User Guide	
Foundation (also known as Infrastructure) Components	**Services and Solutions**
• Healthcare Identifiers • Secure Message Delivery (SMD) • NASH PKI certificates and other authentication and security-related mechanisms • Data Recording and Clinical Terminology/Coding	• Clinical Communications: eReferral, Specialist Letters and eDischarge • Electronic Transfer of Prescriptions (ETP), which is a part of eMedication Management • The national eHealth record system, including use of Shared Health Summaries and Event Summaries

In addition, Clinical Document (CDA) Viewing is also described, which is the capability in your Desktop Software that allows you to view electronic standards-based versions of clinical documents such as referrals, specialist letters, discharge summaries and event summaries.

The above eHealth features can be used in your practice progressively as they are included in updates to your Desktop Software vendor's product. Implementing the updates as they are released will make it easier for you to stay up to date with eHealth developments. You should find this approach better than attempting to implement the features all in one step at a later time.

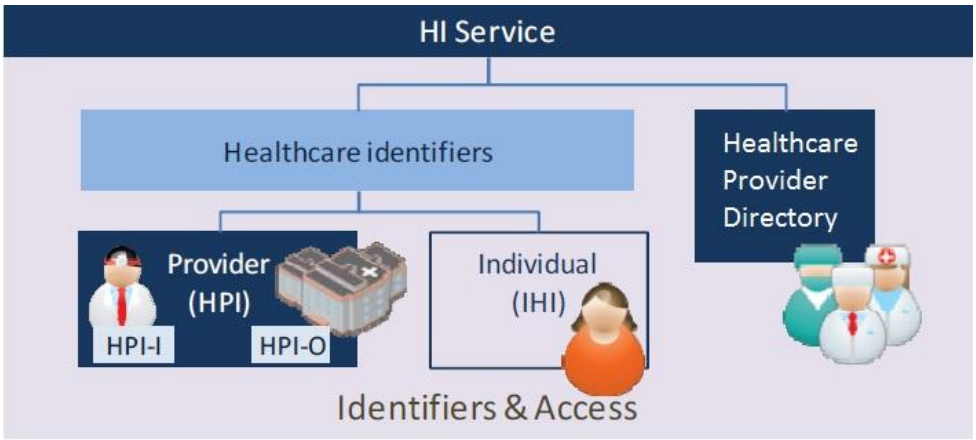
3.2 eHealth Foundations

Each of the eHealth Foundation components introduced above is briefly explained in the sub-sections that follow. In some cases further information is provided in Appendices.

These eHealth foundations when implemented, on their own, won't provide your practice with much additional clinical utility. They are necessary for the subsequent implementation of the eHealth services and solutions, which do enhance clinical processes. However, in implementing the foundations as outlined in this User Guide, especially Healthcare Identifiers, your practice will undertake a range of activities that are considered good practice, e.g. improving the quality of data stored in your Desktop Software and how user login accounts are managed.

3.2.1 Healthcare Identifiers

The Healthcare Identifiers (HI) Service is a national system for uniquely identifying healthcare professionals, organisations and individual consumers of healthcare services. The service is operated by Human Services. Healthcare Identifiers help ensure individuals and healthcare professionals can have confidence that the right information is associated with the right individual at the point of care.

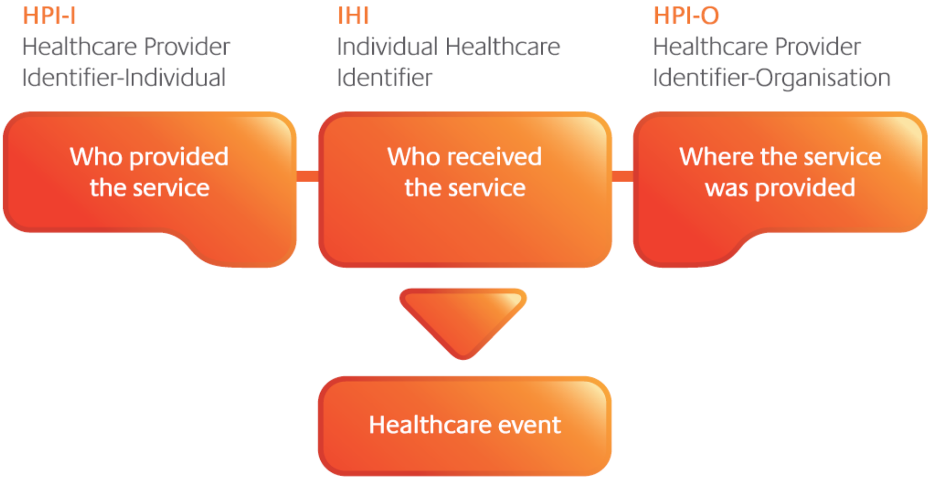


As illustrated in the above diagram, the HI Service allocates and manages the following types of healthcare identifiers:

- **Healthcare Provider Identifier – Individual (HPI-I)** – for individual healthcare professionals involved in providing patient care;
- **Healthcare Provider Identifier – Organisation (HPI-O)** – for organisations that deliver healthcare (such as medical and allied health practices, or hospitals); and

- **Individual Healthcare Identifier (IHI)** – for individuals receiving healthcare services[14].

The diagram below illustrates how these identifier types work together in the context of a healthcare event.


HPI-I
Healthcare Provider Identifier-Individual
IHI
Individual Healthcare Identifier
HPI-O
Healthcare Provider Identifier-Organisation
Who provided the service
Who received the service
Where the service was provided
Healthcare event

Healthcare Identifiers can only be used for the purposes described in the Healthcare Identifiers Act 2010 and Healthcare Identifiers Regulations 2010 (see Section **3.5** for links), including, for example, for electronic referrals, discharge summaries and medication management.

Accessing the HI Service requires registration and digital credentials, namely PKI certificates (discussed later in Section **3.2.3)**, to authenticate the identity of the organisation and individual accessing the Service.

Contracted Service Providers (CSP)

Some healthcare organisations may choose to use a third party service provider to deliver health software as a service (SaaS[15]) and facilitate access to the HI Service, and/or Secure Message Delivery (SMD – discussed in the next section), and/or the eHealth record system on their behalf. These service providers are referred to as Contracted Service Providers (CSP). A CSP is an entity that provides information technology services under contract with a Healthcare Provider Organisation relating to the communication of health information or health information management and is registered with the HI Service.

An example of a CSP might include a vendor that offers web (or cloud) based general practice or aged care software via a hosted model. In addition to the above identifiers, for these organisations there is the Contracted Service Provider Registration Number. [16]

[14] Note that all Australians have already been assigned an IHI. IHIs do not replace Medicare or DVA numbers and they do not affect the way medical benefits are claimed.

[15] See **http://en.wikipedia.org/wiki/Software_as_a_service**.

[16] A Contracted Service Provider (CSP) does not receive a healthcare identifier but a registration number. A CSP must be authorised by a healthcare organisation to transact with the HI Service on their behalf.

Information on CSPs in relation to the HI Service is available at:

http://www.humanservices.gov.au/hiservice

The need for a CSP is likely to only be relevant to your practice if needed by your Desktop Software to connect to the HI Service, eHealth record system or to use SMD. In which case, the prospective CSP will provide your practice with relevant information and assistance. Consequently this User Guide does not cover CSP in detail.

If you are considering a CSP arrangement for your practice, then you should ensure that any organisational implications of CSP arrangements, e.g. in relation to taxation and indemnity cover, are also understood.

The Healthcare Provider Directory (HPD)

An important component of the HI Service is the Healthcare Provider Directory (HPD), which is an opt-in listing of healthcare providers (individuals and organisations) registered with the HI Service.

Once a healthcare provider (organisation and individual) is registered with the HI Service, they can choose to be listed in the HPD. The HPD is not a public directory and is only available to healthcare providers and authorised users (explained later in Section **5.4.4**) of organisations registered with the HI Service.

It is extremely important for your practice and clinicians to be listed and linked in the HPD[17] so that key identifying information can be available, e.g. in searches performed by other healthcare providers. This will enable your practice and clinicians to be selected to receive referrals and other forms of secure electronic communications.

Clinicians are encouraged to consent to their information, including their HPI-I, being visible in the HPD and also for it to be linked to your practice's HPI-O. This linking can be managed on the Human Services HPOS website, which is discussed later, by an Organisation Maintenance Officer (OMO, also discussed later) of the practice. Practice and clinician information held in the HI Service and HPD should also be kept accurate and up to date.

The HPD and Other Directories

When your practice's HPI-O is listed in the HPD information about your practice's Endpoint Location Service (ELS) can be associated with it in the HPD. An ELS is necessary for Secure Message Delivery (SMD), i.e. for your practice to send and receive clinical documents electronically, e.g. referrals. The secure messaging vendor chosen for your practice will advise on how to set up your practice's ELS information. These things are discussed in greater detail in the following section, and are mentioned briefly here because of the HPD's role in secure messaging.

[17] It is a recommendation of this User Guide that clinicians have their HPI-I published in the HPD. In addition to the reasons above (and discussed further later), some Desktop Software requires this in order for it to upload a Shared Health Summary (SHS) to the eHealth record system on behalf of the clinician.

In addition to the HPD, there are a number of other directories that you may find it important to maintain accurate practice and practitioner data in and potentially utilise.

One of these is the National Health Services Directory (NHSD)[18], which is a publically accessible directory of healthcare services, including of general practices, pharmacies, hospitals and emergency departments. The NHSD contains location, opening hours and telephone numbers and, with government endorsement and support, is emerging to have a key role in eHealth. Importantly all the State and Territory Health Departments and Medicare Locals in Australia are committed to ensuring that all health service information the NHSD contains is accurate and up to date. The NHSD is mentioned here because it is currently an important part of the overall health directory landscape that is being positioned to play an important role also in electronic clinical communications.

In addition to the HPD and NHSD, there are other directories that may be relevant to your practice. These include those that are included in your Desktop Software and available as part of the secure messaging service your practice may use. Further directories have been set up by State Health Departments, Local Health Networks, and Medicare Locals, which you may also currently use. In the majority of cases, these are in the process of being integrated into the NHSD.

A listing and description of the key eHealth related directories is included in Appendix **B.1.**

Uses of Your Practice's HPI-O(s)

Your practice will need to decide on a structure of HPI-O(s) based on a range of considerations, which are discussed in detail in Section **5.4** below and the sections that follow. In summary, a HPI-O will have different uses when interacting with:

- The HI Service;
- The eHealth record system;
- A SMD-compliant secure messaging service; and
- When published in the HPD and other directories.

It is important to understand the requirements and options related to HPI-Os, the dependent interactions between the above eHealth services and then design a HPI-O structure that is best for your practice, clinicians and staff, and importantly for your patients.[19]

This guide recommends simplicity in this area of HPI-O structuring as it can be quite complex.

[18] The NHSD is managed by Healthdirect Australia on behalf of all Australian governments and operates as a not-for-profit community resource. See **http://www.nhsd.com.au**.

[19] Note also, for general practices registered for PIP that your PIP entity needs to have a HPI-O.

Your Desktop Software Needs to be Conformant

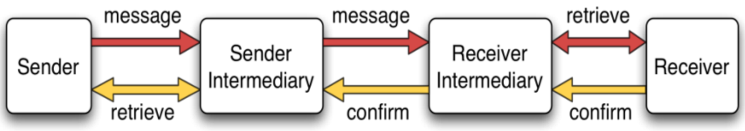
You can check the register of HI Service conformant products at the URL below to see if your Desktop Software can permit your practice to participate in the eHealth system.

https://epipregister.nehta.gov.au/registers/healthcare-identifiers

3.2.2 Secure Message Delivery (SMD)

Secure Message Delivery (SMD) is a set of specifications developed collaboratively by the eHealth community including NEHTA, Standards Australia, Desktop Software vendors and secure messaging service providers. This set of specifications defines an approach to eHealth communication using widely supported IT industry standards for Web Services.[20]

The SMD specification focuses on the secure delivery of messages, which contain clinical documents and/or information, between healthcare organisations, either directly or indirectly using one or more intermediaries. A typical example, from a number of possible configurations, is shown in the diagram below.



Your practice may currently be using one or a number of messaging service providers that are not currently SMD compliant to send and receive some types of clinical documents electronically. A limitation of the non SMD compliant services is that messages may only be exchanged between practice organisations and clinicians who use the same messaging service provider. This limitation often causes medical practitioners to have to use multiple messaging services in order to send and/or receive messages with as broad a network of participating practitioners and other healthcare providers as possible.

This situation is similar to a scenario for example where Optus mobile phone customers can communicate only with other Optus customers, i.e. and not also with Telstra customers, for example. In addition, directories and phone books for each provider would be limited to only listing customers of that provider.

These limitations, the added burden of maintaining contact information in multiple places and the complexity from using different systems for different purposes can be avoided through using SMD compliant Desktop Software products (or equivalent, e.g. clinical software for a hospital) in conjunction with SMD compliant secure messaging service providers.

[20] A Web service is a method of communication between two electronic devices over the World Wide Web. The W3C defines a Web Service as "a software system designed to support interoperable machine-to-machine interaction over a network”. For further information, see **http://en.wikipedia.org/wiki/Web_services**.

Healthcare organisations that implement products and services compliant with the SMD specifications, either directly or indirectly via an intermediary, will be able to connect to and exchange a broad range of message types, securely and reliably, with any other healthcare organisation that also uses software compliant with the specification. Parties will also be able to communicate even where the sender and receiver use different intermediaries to route messages provided that those intermediaries have established commercial interconnect agreements.

The SMD specification itself does not result in complete “interoperability”, because it does not define the content, format and meaning of messages nor the rules of exchange. However, it enables technical connectivity between all messaging endpoints, which is a significant foundation upon which to build future capability. Standards do exist for the content of secure messages and these are discussed in the relevant sections that follow, e.g. **3.3.1** for electronic referrals, specialist letters and discharge summaries.

For secure messaging to work and provide the assurances your practice should expect relating to reliability, authentication, security, etc., a number of components need to be configured correctly in your practice and interoperate as designed. This is discussed in greater detail later in Section **5.5.3**, and for introductory purposes includes:

- That the HI Service is correctly set up for your practice, importantly including that information about your practice and its clinicians is published in the HPD;
- That your practice uses an Endpoint Location Service (ELS), which is explained below, and that your HPI-O is correctly linked to it in the HI Service; and
- That your practice has the NASH PKI certificate for Healthcare Provider Organisations configured for use in your Desktop Software.[21]

If your practice is not using a SMD-compliant Desktop Software product and SMD-compliant messaging service providers, you should contact these suppliers and check what their plans are to become compliant.

You should be aware that most (but not all) of the SMD-compliant providers have designed their service in such a way that it requires their practice customers to establish a CSP link to them (see Section **3.2.1** above) to access the HI Service on your practice’s behalf. Hence, depending on the provider you use, you may be required to link their CSP registration number to the HPI-O your practice uses for SMD. The CSP should assist you with this.

You can check the register of SMD conformant products at:

https://epipregister.nehta.gov.au/registers/secure-message-delivery

Endpoint Location Service (ELS)

SMD and the HI Service work together with the ELS your practice uses to ensure secure messages are sent from and received by your practice correctly. Associated

[21] The same PKI certificate that is used for access to the eHealth record system is required for SMD – see the following section.

with the HPI-O you specify to use for SMD is a pointer (like an electronic location) to the ELS your practice uses. This association is recorded in the HPD.

The ELS itself then contains, in its record for your practice's HPI-O, all the information necessary, such as the electronic address and the associated PKI certificate, for your Desktop Software (via a SMD-compliant messaging service) to transmit and receive secure messages for your practice.

Healthcare organisations using SMD need to use an ELS provider. In many cases for medical practices this will also be their SMD service provider. Larger organisations, for example such as State Health departments, may set themselves up to be their own ELS provider.

3.2.3 NASH PKI, NESAF and other Security-related Mechanisms

In order to safely share and manage access to information, it is essential to be able to authenticate users, i.e. organisations and people, in the healthcare system. In the national eHealth system this is achieved through the use of digital certificates that are conformant to the Australian Government endorsed PKI standard.[22]

In addition a number of other measures, including access control, are required to provide a comprehensive approach to the security of shared electronic healthcare information, whether it is stored on computers in your practice, in the eHealth record system, or exchanged in other ways in the national eHealth system.

NASH plays a critical role in authenticating healthcare organisations and people who use the national eHealth services and solutions, and it also importantly plays a role in protecting the clinical information that is exchanged through data encryption. This means that should a message be intercepted by a party not involved in the exchange (i.e. not the sender or receiver) then that party will not be able to read the message's contents. The technology used to achieve this is relatively complex and it is not essential that you're aware of the details in order to use it.

In order to ensure the technology protects you and your patients' information, you should not give your PKI certificates (organisational or individual) to any other person or organisation for their use. You will need though, when installing and configuring your Desktop Software, to provide it with access to the organisational level PKI certificates so that the software can properly interact with the eHealth services and solutions that it needs to for you to perform the necessary related functions for your practice.

[22] PKI stands for Public Key Infrastructure, which is a set of procedures and technology that provides security and confidentiality for electronic business. PKI is relatively complex and you don't really need to know in detail how it works to use it effectively.
See **http://www.humanservices.gov.au/pki** for information about the use of PKI published by Human Services. Gatekeeper is the Australian Government's strategy for the use of PKI as a key enabler for the delivery of online government services. See **http://www.gatekeeper.gov.au/**.
For detailed information and links on PKI see **http://en.wikipedia.org/wiki/Public_key_infrastructure**.

The concepts and mechanisms relevant to the national eHealth system are further discussed below.

Authentication using PKI Certificates

In electronic transactions, where there is no face-to-face interaction, identity is *asserted* using credentials such as user names and passwords, smartcards, PICs, etc.

The potential damage resulting from an inability to authenticate an individual, organisation or device accessing information, such as pathology or radiology, held in clinical information systems can be substantial. Password-based only authentication is considered inadequate for many purposes – with governments at local, federal and state levels directing that security of access to sensitive information be upgraded to use PKI certificates.

PKI enables users to know:

- Who sent (or uploaded) the information – **authentication**;
- That the information content has not been altered in any way between sending (or uploading) and receiving (or downloading) – **integrity**;
- That the sender (or uploader) cannot at some later stage dispute they created and sent (or uploaded) the information – **non-repudiation**; and
- That only the person the information is directed to can open it – **confidentiality**.

It is probable that your practice is already using PKI certificates for your electronic interactions with Human Services for claiming and other business and commerce related functions. These certificates will continue to be required for those purposes.[23]

Your practice may also be currently using PKI certificates for some eHealth functionality, e.g. for the HI Service, the eHealth record system and for Secure Message Delivery (SMD). These certificates may include:

- The Human Services Site PKI certificates held in your practice that you utilised to become HI-enabled so that your Desktop Software and staff could access the HI Service; and
- The NASH PKI certificates (also previously called eHealth record PKI certificates) for your practice organisation to access the eHealth record system.

The table below (and the Notes that follow) outlines the types of PKI certificates that are necessary for the different requirements in your practice.

[23] The following website may be used to search for the existence of PKI certificates for your practice, other healthcare organisations and clinicians: **http://www.certificates-australia.com.au/general/cert_search_health.shtml**.

PKI Certificate Type	Human Services Medicare Services [i]	eHealth Services		
		HI Service	eHealth Record System	Secure Message Delivery (SMD)
Site (also known as Location) or Organisation [ii]	Provided on a CD for installation on your PC or Local Network.	Existing Human Services Site PKI certificates can be enabled for use with the HI Service, or a PKI Site certificate can be requested. [iii]	A NASH PKI certificate for Healthcare Organisations (also previously known as an eHealth Record Organisation PKI Certificate) needs to be requested and installed or enabled for use if you already have one. [iii]	The same NASH PKI certificate described in the cell to the left (i.e. for the eHealth Record System) can be used for SMD.
Individual [iv]	Provided on a USB Token or Smartcard with a Smartcard Reader.	Existing Human Services Individual PKI certificates can be enabled for use with the HI Service, or an Individual PKI certificate can be requested. [v]	A NASH PKI certificate for Individual Healthcare Providers (previously known as an eHealth Record Individual PKI Certificate) needs to be requested and installed or enabled for use if you already have one. [vi]	Individual PKI certificates are not needed for SMD.

Notes:

[i] For the use of Medicare Online, e.g. for claiming, and other services provided by Human Services that require a PKI certificate, including HPOS. These certificates will continue to be required for these purposes.

[ii] This PKI certificate type can be installed and used on multiple PCs for the specific organisation or site.

[iii] This PKI certificate type is for use with a conformant Desktop Software product.

[iv] This PKI certificate type requires a PIC to be entered to be used. It is necessary for individual clinicians and practice staff who require access to the service in certain circumstances – discussed later in the sections relevant to the eHealth services and solutions, i.e. in Section **3.3**.

[v] A variant of this PKI certificate is available for Organisation Maintenance Officers (OMO – discussed later) that permits a range of additional functions for this role.

[vi] Individual healthcare providers who you wish to access the Provider Portal of the eHealth record system on behalf of your practice will need one of these PKI certificates, and their HPI-I needs to be linked to your practice's HPI-O(s) in the eHealth record system. This is discussed later.

The PKI certificate requirements for the current implementation of ETP are determined by the vendors. This is explained later in Sections **3.3.2** and **5.5.4**.

The following recent news article from Human Services explains NASH PKI certificates and their use in eHealth:

http://hpnews.medicareaustralia.gov.au/2013/04/nash-pki-certificates-and-their-use-in-ehealth/

Please visit **http://www.humanservices.gov.au/pki** for the latest information on PKI certificates.

Security and Access Control

For organisations and individuals in the healthcare system, robust security practices are required to both meet legal obligations and protect personal health information. Greater collaboration and exchange of health information also creates an emerging set of business risks that need to be considered and addressed.

All organisations involved in the provision of healthcare whether they have many staff or operate as a sole practitioner, need to carefully manage the security of information systems and allow information to be available to the right person, at the right time and in the right form regardless of its origin, all the while supporting traceable provenance and control.

There are two important and related initiatives for security and access control that are relevant to medical practices for their participation in the national eHealth system[24]. These are:

- The National eHealth Security and Access Framework (NESAF)[25]; and
- The RACGP's Computer and Information Security Standards (CISS)[26].

The RACGP has developed the CISS to work concurrently with the NESAF, as it adheres to the same outcome of implementing safe security measures to protect patient information held and transmitted by electronic healthcare records. While the NESAF covers the whole of electronic infrastructure across Australia's healthcare network, the CISS has been designed specifically for medical practices.

The CISS and accompanying templates (in the form of a workbook) explain the security and safety controls in an accessible and easy to understand format, with measures that can be immediately implemented into medical practices.

If Australian medical practices comply with the CISS they can be confident that their processes and policies also comply with the higher level requirements of the NESAF.[27]

The CISS and templates[28], which medical practices are advised to implement, are available at:

http://www.racgp.org.au/your-practice/standards/ciss/[29]

[24] Note too that participation in the national eHealth record system requires practices to have written policies related to security and access control. This is discussed below in Section **3.3.3**.

[25] See Appendix **B.2** for further information on NESAF, and **http://www.nehta.gov.au/our-work/security**.

[26] See **http://www.racgp.org.au/your-practice/e-health/cis/**.

[27] The RACGP makes this statement for general practices, but it also applies generally to medical practices. See **http://www.racgp.org.au/download/documents/e-health/2012nesaf_information.pdf**.

[28] The RACGP recently published (June 2013) the second edition of their CISS, which incorporates specific guidance to enable practices to also comply with the legislative requirements for the eHealth record system and the Healthcare Identifiers Service. These requirements are discussed later.

3.2.4 Data Recording and Clinical Terminology/Coding

A clinical terminology is a structured vocabulary used in clinical practice to accurately describe the care and treatment of patients. Clinical terminology covers complex concepts such as diseases, operations, treatments and medicines, and relies upon the consistent use of standardised coding systems.

Healthcare providers need to describe and record this type of information about their patients to provide a history of care for their own purposes and to share with other providers. Consistent and accurate articulation and interpretation of this information is critical to the process of safe information exchange. For example, errors in recording the name of a medicine or in transcribing it from one place to another can lead to serious consequences for the patient and risks to the practice and clinicians involved.

Information will only be shared if there is confidence in its quality. For example, clinical software will only 'read' a patient as having diabetes, coronary heart disease or any other condition if this information is entered correctly and consistently.

In conjunction with Desktop Software products that can intelligently interpret the clinical information being input by a user, a consistent clinical terminology (or language) will significantly reduce errors and deliver more accurate and improved recording and checking of information. In order for these information systems to be interoperable and act intelligently they must be able to record, read and interpret clinical information that is exchanged between systems, e.g. drug names, diagnoses, pathology test results and the like.

For further information on clinical terminology systems used in Australia for medical practices, please see Appendix **B.3**.

What does Clinical Terminology mean for Your Practice?

As far as your practice is concerned, much of what happens with clinical terminology in the use of your Desktop Software and its communications with the national eHealth system and software used by other healthcare providers should be largely invisible. Some Desktop Software products do make the codes visible, for example when you select a diagnosis, but it really operates mostly in the background, and you shouldn't need to worry about the actual code that is used.

However, the benefits to your practice and other healthcare providers from the use of standardised clinical terms will only come if clinicians in your practice only select options, e.g. for diagnoses, treatments, medicines, etc. from drop-down or check-box lists. If text is typed into a free text data entry field in your Desktop Software, that data is not coded and hence cannot be reliably interpreted elsewhere in the eHealth system.

[29] In addition, the Australian Government provides information about protecting 'endpoints' such as desktop computers and what you should do if you see something wrong, at the Stay Smart Online website at **http://www.staysmartonline.gov.au**.

Hence, for your practice to participate effectively in the eHealth system, you will need to educate your clinicians to use the drop-down and check-box type selection features in your Desktop Software for key patient data and to not use free text data fields.

3.2.5 Clinical Document (CDA) Viewing and Creation

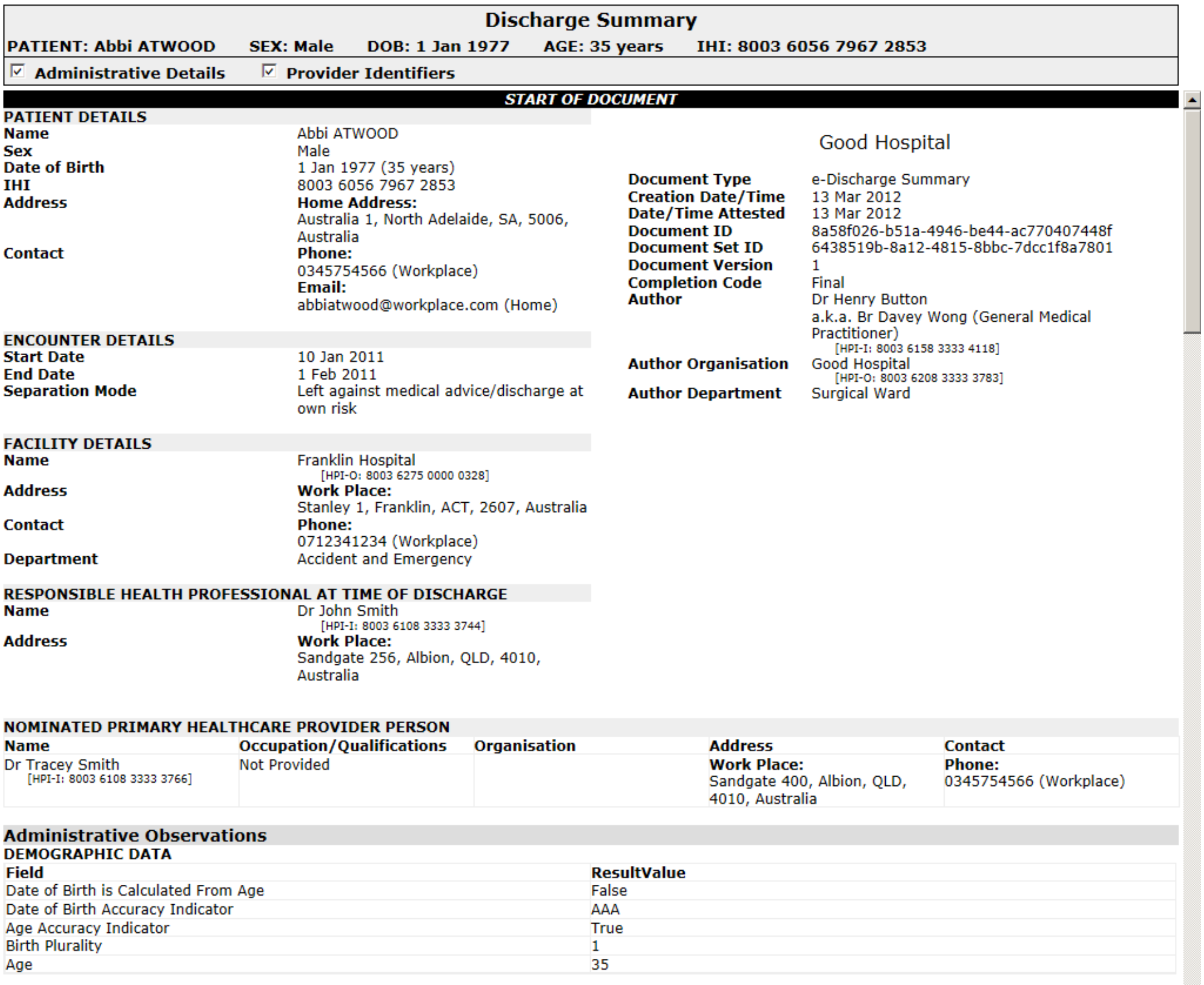
The Clinical Document Architecture is a HL7[30] standard for the representation and machine processing of clinical documents in a way that makes the documents both human readable and machine processable. CDA is a document mark-up standard that specifies the structure and semantics of clinical documents for the purpose of exchange between healthcare providers and with patients.

A CDA document can contain any type of clinical content – typical CDA documents would be a Discharge Summary, Diagnostic Report, Referral, Specialist Letter and more. The most popular use is for inter-enterprise information exchange, as implemented in Australia's national eHealth system and similarly in many other countries.

The national eHealth record system requires all documents that are to be stored in it to be in the CDA format. Conformant Desktop Software for medical practices and the software used by other participating healthcare organisations (e.g. hospitals, pathology laboratories, etc.) are all required to create CDA compliant clinical documents. The ability to display CDA compliant documents is a minimum functional requirement for conformant Desktop Software.

The top part of an example CDA compliant eDischarge Summary (using test data) is shown in the following image.

[30] Health Level Seven International (HL7) is the global authority on standards for interoperability of health information technology with members in over 55 countries – see **http://www.hl7.org**, and for CDA specifically: **http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7**.



Discharge Summary

PATIENT: Abbi ATWOOD **SEX: Male** **DOB: 1 Jan 1977** **AGE: 35 years** **IHI: 8003 6056 7967 2853**

☑ **Administrative Details** ☑ **Provider Identifiers**

START OF DOCUMENT

PATIENT DETAILS	
Name	Abbi ATWOOD
Sex	Male
Date of Birth	1 Jan 1977 (35 years)
IHI	8003 6056 7967 2853
Address	**Home Address:** Australia 1, North Adelaide, SA, 5006, Australia
Contact	**Phone:** 0345754566 (Workplace) **Email:** abbiatwood@workplace.com (Home)
ENCOUNTER DETAILS	
Start Date	10 Jan 2011
End Date	1 Feb 2011
Separation Mode	Left against medical advice/discharge at own risk
FACILITY DETAILS	
Name	Franklin Hospital [HPI-O: 8003 6275 0000 0328]
Address	**Work Place:** Stanley 1, Franklin, ACT, 2607, Australia
Contact	**Phone:** 0712341234 (Workplace)
Department	Accident and Emergency
RESPONSIBLE HEALTH PROFESSIONAL AT TIME OF DISCHARGE	
Name	Dr John Smith [HPI-I: 8003 6108 3333 3744]
Address	**Work Place:** Sandgate 256, Albion, QLD, 4010, Australia

Good Hospital

Document Type	e-Discharge Summary
Creation Date/Time	13 Mar 2012
Date/Time Attested	13 Mar 2012
Document ID	8a58f026-b51a-4946-be44-ac770407448f
Document Set ID	6438519b-8a12-4815-8bbc-7dcc1f8a7801
Document Version	1
Completion Code	Final
Author	Dr Henry Button a.k.a. Br Davey Wong (General Medical Practitioner) [HPI-I: 8003 6158 3333 4118]
Author Organisation	Good Hospital [HPI-O: 8003 6208 3333 3783]
Author Department	Surgical Ward

NOMINATED PRIMARY HEALTHCARE PROVIDER PERSON

Name	**Occupation/Qualifications**	**Organisation**	**Address**	**Contact**
Dr Tracey Smith [HPI-I: 8003 6108 3333 3766]	Not Provided		**Work Place:** Sandgate 400, Albion, QLD, 4010, Australia	**Phone:** 0345754566 (Workplace)

Administrative Observations

DEMOGRAPHIC DATA

Field	**ResultValue**
Date of Birth is Calculated From Age	False
Date of Birth Accuracy Indicator	AAA
Age Accuracy Indicator	True
Birth Plurality	1
Age	35

The above example is included to highlight some of the standard mandatory information that CDA conformant documents include in order to improve consistency between healthcare providers. The layout and how the information is presented when viewed (or printed) are determined by a style sheet, which is provided by the vendor of the clinical software being used. In addition, vendors may include other functionality, such as “sort”, “go to” or “find” to aid in navigating the information in CDA documents when displayed.

Clinical Software vendors and messaging service providers are increasingly upgrading their offerings to be conformant with the standards required for their customer’s practices to participate in the national eHealth system. Amongst others these standards include CDA and those for SMD. There are some vendors and service providers whose non-conformant products do support the exchange of clinical documents, e.g. discharge summaries, referrals and specialist letters (i.e. that are not CDA compliant), so you will need to be aware if your practice uses any such products or services as part of your practice’s eHealth planning.

For the eHealth record system, Shared Health Summaries (SHS) and Event Summaries (ES) require conformity to a higher level of CDA specification[31] than other document types. Conformant Desktop Software products are capable of doing this.

[31] The level required for SHS and ES is called 3A. It is not essential for you to know about these levels, suffice that they are 1A, 1B, 2, 3A and 3B, with increasing rigour and scope of conformance as the level numbers increase.

As healthcare organisations gain the ability to create and send CDA documents (e.g. hospital discharge summaries) they will need to work with their community of healthcare providers (e.g. GPs, specialists, etc.) to ensure that these are implemented safely and correctly.

Please consult your software vendor's documentation for advice on how to use this feature.

3.3 eHealth Services and Solutions

The eHealth foundations described in the above sections work together largely behind the scenes to enable you and your practice to perform the types of clinically orientated eHealth services and solutions outlined in the sections that follow.

As introduced in Section **1.3** above, the exchange of clinical documents in the national eHealth system requires that the software products and services used by healthcare organisations comply with national eHealth specifications[32]. This applies to both the following situations:

- When documents are sent and received by your Desktop Software through a messaging service provider, i.e. point-to-point; and
- When documents are stored and then later accessed by your Desktop Software from the national eHealth record system.[33]

At the time of writing not all document types are able to be exchanged via both the methods listed above, although it is expected over time that more will.

Adding to the foundation eHealth components introduced in Section **3.2** above, the following eHealth services and solutions are introduced in the sub-sections that follow[34]:

- Clinical Communications, including for Referrals, Specialist Letters and Discharge Summaries;
- Electronic Transfer of Prescriptions (ETP), which is a part of eMedication Management; and
- The national eHealth record system.

3.3.1 Clinical Communications

Electronic communication in healthcare is expanding – starting with electronic versions of existing clinical document types commonly exchanged between health-

[32] Your conformant Desktop Software and that of other healthcare organisations will produce CDA compliant clinical documents for use in the national eHealth system.

[33] When your Desktop Software interacts with the national eHealth record system it is sometimes called B2B.

[34] See the diagram in Section **3.1** for context.

care providers, e.g. discharge summaries, pathology reports, referrals and specialist letters – to a new set of document types designed for use in the national eHealth record system, such as the Shared Health Summary (SHS) and Event Summary (ES).

This expansion is:

- From the *point-to-point* form of document exchange, i.e. from a clinician to another specific clinician via secure messaging, in support of a named shared patient's continuity of care,
- To a *point-to-share* form where a patient's key clinical information is uploaded and stored for access by *any* authorised clinician to use in the care of the patient.

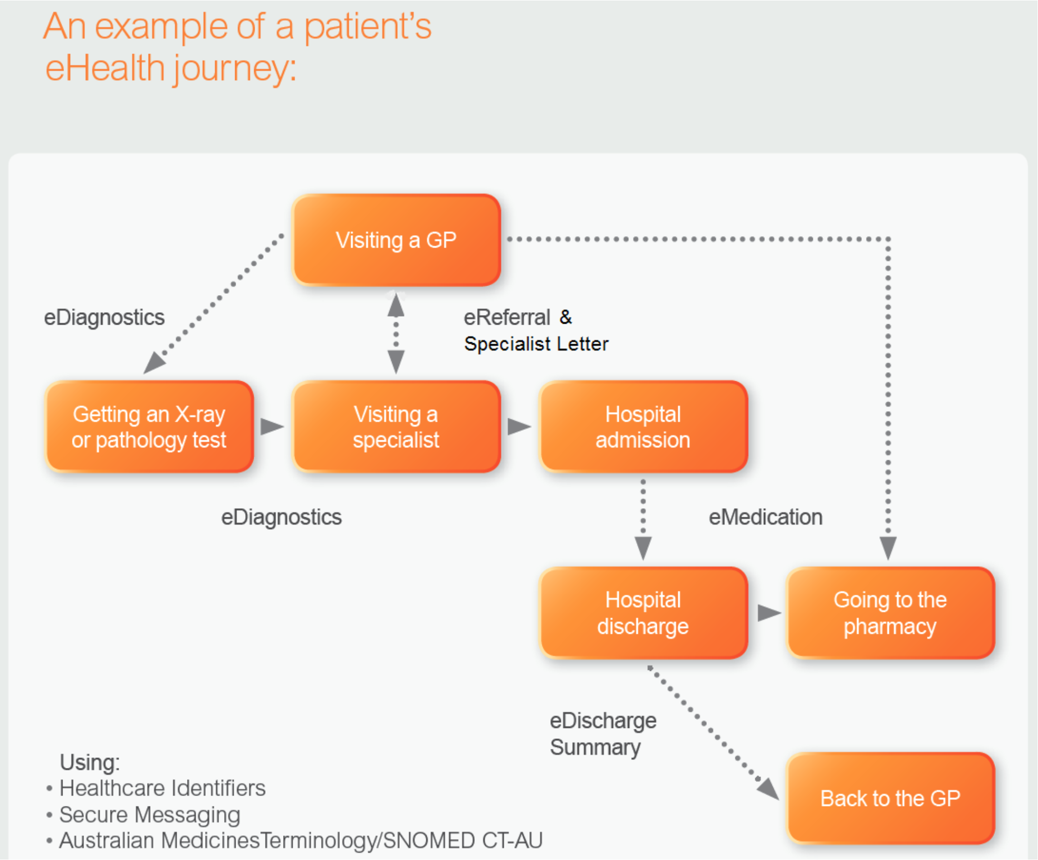
Through the use of standards and a system of conformance for software products and services, the national eHealth system caters for both of these forms of communication.

At the time of writing CDA compliant Referrals and Discharge Summaries can be exchanged via secure messaging (see Section **3.2.2** above). In some regions, Discharge Summaries are being uploaded into a patient's eHealth record, but it is not yet common. The ability to upload Referrals and the specifications for CDA compliant Specialist Letters were still in development at the time of writing, and are expected to be available in Desktop Software in mid-2013.

The intention over time is that all clinical document types could be stored in the eHealth record system, and all, except the SHS and ES (as they are designed solely for use in the eHealth record system[35]), could also be exchanged by SMD. It is important to remember that the eHealth record system does not replace the need for point to point communication between healthcare professionals, or the obligation to keep up to date local clinical records.

The types of point-to-point exchanges of clinical documents discussed above, along with some others, are illustrated in the diagram below.

[35] Note that other eHealth record system specific document types may be introduced in the future.



Pathologists and radiologists have been sending a very high proportion of their reports to medical practitioners electronically for many years. More recently referrals from GPs, discharge summaries from hospitals and letters from specialists have been increasingly sent electronically, although not as significantly as diagnostic reports.

Your practice is likely to currently use some form of electronic exchange of some, if not all, of these types of clinical documents using features in your Desktop Software that may not presently be compliant with the national eHealth specifications. Vendors of these products and the providers of messaging services are working to be compliant so that your practice can receive the benefits that SMD and the national eHealth system can provide.

At the time of writing this level of compliance is increasing but not universally available, so you may find it necessary to continue using the non-compliant methods until your vendor(s) update their products to be compliant. Vendors anticipate that transitioning to the compliant method should be relatively straight-forward for practices.

3.3.2 Electronic Transfer of Prescriptions (ETP)

ETP is a subset of eMedication Management and involves your Desktop Software being able to create and send electronic prescription information – essentially a copy of the script. These electronic copies will be sent to a Prescription Exchange Service (PES) where they are stored and can be retrieved later by a dispenser at the time of dispensing.

It is likely that Desktop Software vendors will design this functionality into their products differently, so you should follow the guidelines from your vendor about how you can send prescription information electronically.

Until full electronic transfer of prescriptions is implemented (including with electronic signatures), prescribers will still be required to provide patients with a signed paper prescription when sending an electronic copy to a PES. The paper prescription with the handwritten signature will remain the legal document for the time being until regulations that currently require this are changed. The paper record generated by the prescriber and provided to the patient contains a bar code to enable retrieval of prescriptions from the PES for dispensing by a pharmacy, for example.

In order to send copies of prescriptions electronically to a PES, your practice should have an agreement with a PES. The PES providers may have different terms and conditions and it is important that your practice understands and accepts those terms and conditions.

Some PES providers currently exist and most Desktop Software vendors have updated their products to send copies of prescriptions to a PES. You should check if your Desktop Software can do this by checking the register for ETP conformance at:

https://epipregister.nehta.gov.au/registers/electronic-transfer-of-prescriptions

Further information about ETP and the broader context and developments in eMedication Management can be found in Appendix **B.4**.

3.3.3 The eHealth Record System

The Australian Government has introduced a personally controlled electronic health record system, commonly called the PCEHR system (and officially known as the "eHealth record system") as the core component of the national eHealth system.[36]

The key principles for the design of the eHealth record system include:

- Participation is voluntary (opt-in) for both consumers and healthcare providers;
- Healthcare provider organisation access to a consumer's record is under the consumer's control, except in situations where the treating healthcare professional's clinical judgement is that access is required and patient consent is not possible, in which case they can "break glass" to gain emergency access;[37]

[36] This section provides an overview of the eHealth record system. Detailed information is available at **http://www.ehealth.gov.au**.

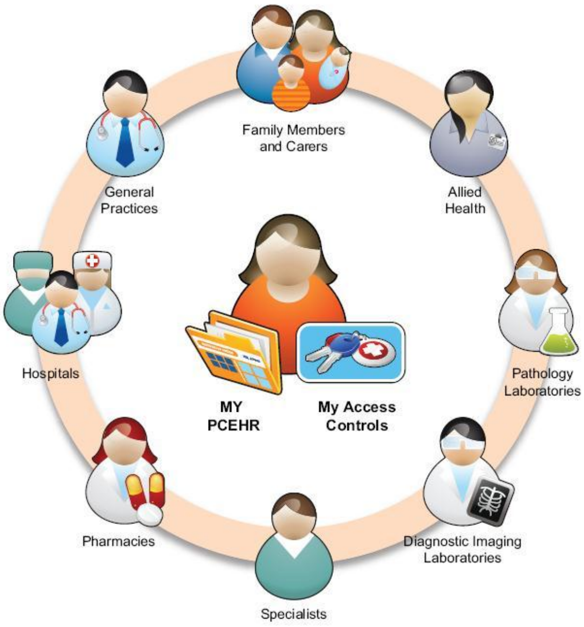
[37] Note that this approach is consistent with privacy laws. Use of this emergency function is recorded in the consumer's eHealth record's audit log and may be notified to the patient if they requested notifications.

- The eHealth record is not a replacement for organisational or practitioner clinical records, i.e. the “source of truth” remains where it is today – in local clinical records, and is not a replacement for current point to point sharing of health information;

- The eHealth record includes two components – clinical and personal (or consumer-entered) – and the clinical component contains copies, not originals, of healthcare-related information;

- Consumers may themselves enter two types of data into their eHealth record – one set that is only viewable to themselves (personal health notes) and the other that can be viewed by healthcare providers (personal health summary);

- Only healthcare professionals authorised by their healthcare organisation and providing healthcare to the consumer can enter information into the consumer’s eHealth record; and



- Consumers may remove information from view on their eHealth record and request that particular information not be uploaded. As there will be no indication to a healthcare professional who views the patient’s eHealth record of how the patient may have modified their record, healthcare professionals need to exercise their normal clinical judgement as in other situations where information may be absent or not complete.

The diagram above illustrates the important role of the eHealth record in sharing key patient health information across healthcare providers, and the centrality of the consumer’s control of access to their record.

The Priority Groups of Consumers

The Australian Government has identified the following groups as key priorities for participation in the national eHealth record system:

- People with chronic and complex conditions;

- Older Australians;

- Aboriginal and Torres Strait Islander peoples;

- Mothers and newborns;

- People with mental health conditions; and

- People in regional, rural and remote communities.

While participation is not restricted, i.e. any Australian consumer may register for an eHealth record, it is believed that greatest benefit will be provided to the above groups, and if they participate earliest and to the largest extent that the healthcare system will derive greater benefits overall.

What an eHealth Record Contains

The eHealth record system is designed to have the following document types and information uploaded, entered, downloaded and viewed (depending upon the mode of use, e.g. from within conformant Desktop Software or via an Internet browser):

Shared Health Summaries

- This may include information about a patient's medical history, including medications they are currently taking, allergies and adverse reactions they may have, or immunisations they have received. It will not include clinical notes. The structure of a patient's shared health summary is underpinned by the RACGP's template for a GP health summary, and represents the patient's status at a point in time.

- The shared health summary is prepared and uploaded by a patient's nominated healthcare provider (discussed below) who can be a medical practitioner, registered nurse or Aboriginal and Torres Strait Islander health practitioner.
- The healthcare provider authoring a Shared Health Summary is likely to be involved in ongoing care for the patient, or may be responsible for coordinating care across multiple healthcare providers.
- To create a Shared Health Summary, the healthcare provider will need to obtain the patient's agreement that:

  the healthcare provider is to be the individual's Nominated Healthcare Provider;

  the healthcare provider is to create the Shared Health Summary for the patient;

- The most recently uploaded shared health summary in a consumer's eHealth record is likely to be the first document accessed by any other healthcare professional viewing a patient's eHealth record.
- A patient has only one Shared Health Summary at a time – each time a new one is uploaded it replaces the previous summary.
- Shared Health Summaries can only be uploaded to and retrieved from the eHealth record system, i.e. they cannot be exchanged via secure messaging.

Event Summaries

- This is a summary of a clinically significant event that may contain allergies and adverse reactions, medicines, diagnoses, interventions, immunisations and diagnostic investigations.

- It can be uploaded by a healthcare professional at any participating healthcare organisation that is authorised to use the eHealth record system – such as an after-hours GP clinic, hospital or an allied health professional.

- Event Summaries can only be uploaded to and retrieved/viewed from the eHealth record system, i.e. they cannot be exchanged via secure messaging.

eReferrals, Specialist Letters and eDischarge Summaries

- These clinical document types are discussed above in Section **3.3.1**, and may, depending on the context and software used, be both exchanged by secure messaging (see Section **3.2.2** above), and uploaded to and retrieved/viewed from the eHealth record system when the functionality supports this.

Medicare Records

- When registering for their eHealth record, consumers can choose to have data held by Medicare about them included in their record. This can include past[38] and future MBS and PBS (and RPBS) transaction information, their organ donor status (sourced from the Australian Organ Donor Register (AODR)) and, if relevant, details from their Australian Childhood Immunisation Register (ACIR) records.

- These records may be viewed individually or in summary via the consumer's Medicare Overview.

- This data is visible to healthcare providers authorised to access the record.

Consumer Entered Data

- Personal Health Summary – consumers can enter information about allergies and adverse reactions, and current medications into their eHealth record. This data can be viewed by healthcare providers authorised to access the patient's record.

- Advance Care Directive (ACD) Custodian – consumers can enter contact information of a person or organisation who is the holder of their advance care directive (or "living will"). This information can be viewed by healthcare providers authorised to access the patient's record.[39]

[38] The system is configured to include up to two years of prior transactions, which are each stored in the eHealth record system as discrete documents.

[39] Work is underway to enable consumers to have their actual ACD stored in their eHealth record. See: **http://www.pulseitmagazine.com.au/index.php?option=com_content&view=article&id=1422**.

- Emergency Contact Details – consumers can create a list of important emergency contacts in their eHealth record, which is viewable by healthcare providers authorised to access the patient's record.
- Personal Health Notes – consumers can enter information to help them keep track of their health, i.e. like a health journal. These notes are dated by the system and include an entered title and the text of the personal note. These notes are **not** viewable by healthcare providers.

Child Development

- This section of an eHealth record provides parents with the ability to record results of regular health checks, childhood development and other useful information. The objective is to provide an integrated view of a child's health status for the parents/guardian and healthcare providers involved in the child's care.
- The Child eHealth Record (CeHR) initially contains: an Achievement Diary, Personal Observations, Immunisations, Child Health Check Schedule, Child Growth Charts and Information for Parents.
- This data is visible to healthcare providers authorised to access the record.

Medicines Information

Information about medicines for consumers is included in a number of places in their eHealth record:

- The shared health summary will, and other clinical documents (e.g. event and discharge summaries) may contain medicines data based on the current medications list from the clinical system of the healthcare provider;
- The Prescription and Dispense View contains details of medicines prescribed and dispensed that are stored in the National Prescription and Dispense Repository (NPDR – discussed below), which is part of the eHealth record system;
- Information on medicines supplied via PBS (and RPBS) is viewable in the Medicare Records section (see above); and
- Consumers themselves may enter medicines information (see above).

The National Prescription and Dispense Repository (NPDR) stores and links prescription and dispense information for consumers as part of their eHealth record. The data in it is sourced from Prescription Exchange Services (PES – see Section **3.3.2** above)[40] and is expected grow as ETP is increasingly used by prescribers and dispensers – see Appendix **B.4** for further information.

[40] Information on medicines dispensed by hospitals and via private scripts will also be stored in the NPDR.

Ongoing Development of the System

Note that not all of the above types of data are fully available at this stage of the eHealth record system's implementation, and that use of some features will also depend on your Desktop Software product vendor incorporating the specific functionality into their product. If access is via the Provider Portal (discussed below), then all document and information types that have been inserted in the consumer's eHealth record can be viewed by authorised healthcare providers, subject to the access settings established by the consumer.

In addition, the eHealth record system will continue to evolve to include other document types and services over time to match the needs and priorities of the healthcare system.

Registered Repositories

The eHealth record system has a design feature that is supported through its legislative framework to include what are called Registered Repositories.

An existing example of such a repository is the collection of Medicare data (introduced above), where a patient's MBS and other transaction or status data (that they specify) is stored in a database that is effectively part of the eHealth record system. This Human Services repository was the first of a number that are envisaged and planned for the system.

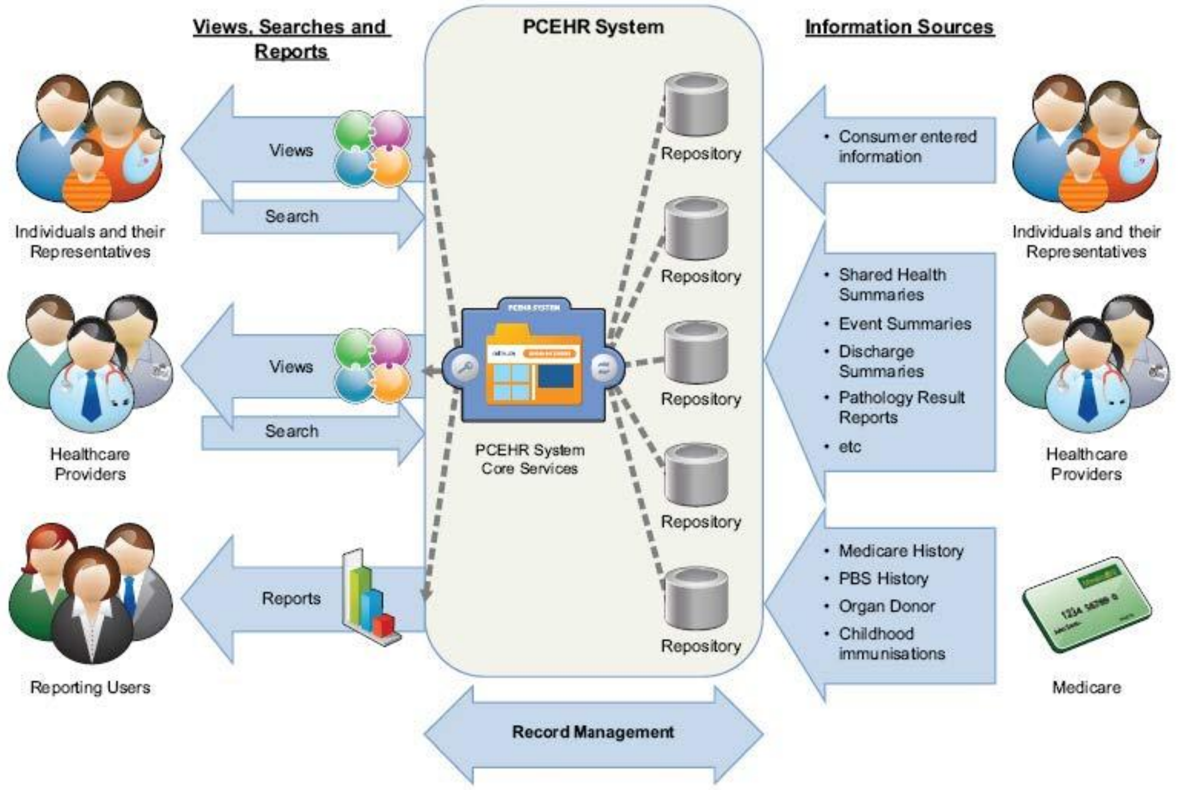
A further example is the repository for medicines prescription and dispensing data, i.e. via the NPDR introduced above. Other repositories may also be considered – for example it is possible that pathology and radiology results may be the subject of a future repository.[41]

The diagram in the section below illustrates that the eHealth record system is designed to incorporate a number of different types of repositories.

[41] See **http://www.pulseitmagazine.com.au/index.php?option=com_content&view=article&id=1507**.

How the eHealth Record System is Designed to Work

The diagram below highlights the key participants and the roles and actions intended for the national eHealth record system.



Access by individual consumers and their representatives[42] to the eHealth record system is via an Internet browser, and for healthcare providers via a conformant clinical information system (e.g. your practice's Desktop Software) or with an Internet browser to the Provider Portal, which currently provides read-only access[43].

To assess and manage the reliability and performance (including uptake) of the eHealth record system, it is essential that it produces reports that the System Operator can use to support the operation of the system. This is indicated by the Reporting Users role in the above diagram.

The eHealth record system includes a feature called Access Flags, which are set by healthcare organisations to control access to patients' eHealth records within their organisational structure. Access Flags are explained in Appendix **C.2**.

[42] Parents are able to set up eHealth records for their children and consumers are able to establish access to their record for Authorised Representatives and Nominated Representatives. These roles are defined in detail at **http://www.ehealth.gov.au**. The eHealth record system itself can also be accessed at **http://my.gov.au**, which is the website that the Australian Government prefers people to use for registration and access.

[43] It is anticipated that future updates to the Provider Portal may introduce the ability for an authorised healthcare provider to write information to a consumer's eHealth record.

Your Desktop Software needs to be Conformant

You can check if your Desktop Software complies with the specifications required for your practice to use the national eHealth record system at the URL below:

https://epipregister.nehta.gov.au/registers/personally-controlled-electronic-health-records

Provider Portal Access

The eHealth record system includes a portal that enables authorised healthcare professionals on behalf of registered organisations to access consumers' eHealth records. The provider portal is currently a read only service[44] and can be accessed through:

https://portal.ehealth.gov.au/

It is essential that clinicians who wish to use this portal have their HPI-I linked to your practice's HPI-O within the eHealth record system. Clinicians also need to have an Individual NASH PKI certificate before they can utilise the provider portal. The process to do this is explained later.

A Fact Sheet on the Provider Portal is available at the following web address:

http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/resources-hcp

Patient registration for an eHealth Record

There are a number of ways in which consumers can register for their eHealth record. These currently include:

- Online at **http://my.gov.au**[45];
- Call centre on 1800 PCEHR1 (1800 723 471);
- At a Medicare Shopfront;
- Via posted mail; and
- Assisted Registration at a healthcare organisation (described below).

A method called Assisted Registration is available that enables healthcare organisations to help their patients register for an eHealth record at the point of care.

Your practice could assist patients to register by asserting the patient's identity and then submitting their details to the eHealth record system using the feature in your Desktop Software or, if that is not provided, with a purpose-built software tool that is available for this purpose. If successful, the patient will be registered almost immediately and your practice could upload clinical information to their record

[44] It is anticipated that future updates to the Provider Portal may introduce the ability for an authorised healthcare provider to write information to a consumer's eHealth record.

[45] Note that the eHealth record system is also accessible from **ehealth.gov.au**, however the Australian Government prefers that people use the **my.gov.au** website listed above.

straight away. You may find this process more beneficial than sending your patient away to register themselves and then come back later, with the chance that they haven't.

Practices should consider what resources (e.g. staff and time) might be involved in assisting patients to register before committing to providing this as a service and also the benefits that might be achieved. The process to set your practice up for Assisted Registration is outlined later in Section **5.7.2.2**. Further information is available at:

http://ehealth.gov.au/internet/ehealth/publishing.nsf/content/assistedregguide

Consider Encouraging Your Clinicians and Staff to Register

You may find it very useful for clinicians and staff in your practice to register for their own eHealth record, i.e. as healthcare consumers themselves. This will provide your practice with knowledge and experience that will be invaluable when talking with your patients about the system.

The process for registering is described above and is available for all Australians. An added benefit for those clinicians and staff, who are also patients of the practice, is that their eHealth record could be accessed as soon as your Desktop Software is configured to use the system.

It is an individual decision to opt-in to the eHealth record system, i.e. the practice cannot force its clinicians and staff to register, but it would be a positive move to encourage them to participate for their own benefit as healthcare consumers. If they do register, then the practice may also benefit from their participation.

How Consumers control access to their eHealth Record

The default access control settings are that all healthcare professionals involved in a consumer's care will be able to:

- Access the consumer's eHealth record during, or in regard to, a consultation or clinical event involving the consumer; and
- View all documents in the eHealth record and upload documents to the eHealth record, unless the consumer specifically requests the healthcare professional not to.

This is because when a consumer registers for an eHealth record, they effectively give "standing consent" to all registered healthcare provider organisations to upload to the eHealth record system any record that includes health information about the consumer.

A consumer also has a number of mechanisms available to them to manage the content of and to control access to their and/or their dependent's eHealth record(s). These include:

- Limiting access to the *whole of their record* and having a Record Code (RC)[46] that needs to be provided to healthcare providers who they wish to have access;
- Limiting access to *specific documents* in their eHealth record, and having a Document Code (DC)[47] to provide to healthcare providers for them to gain access to the set of documents the consumer has specifically selected to have restricted access[48];
- The consumer can see a list of healthcare organisations that have accessed their record and should they wish can change the level of access[49] they wish particular healthcare organisations to have, including revoking access (except in the case of an emergency, as discussed earlier);
- By expressly informing a healthcare provider that they do not wish particular information to be uploaded to their eHealth record during a consultation, upon which the healthcare provider must comply; and
- The ability to "effectively remove" documents for viewing from their eHealth record (via their consumer portal) that were previously uploaded. When this is done these documents will not be available to the consumer or healthcare providers, including in an emergency (see the "break glass" provision discussed at the beginning of this section)[50].

When registering, consumers are made aware of the implications and risks of limiting the access of healthcare providers to their eHealth record, i.e. as it relates to affecting the quality of advice and decision making about their care. This type of facility is, in effect, not dissimilar to the current situation where patients may choose to withhold and/or unfortunately provide inaccurate information to their care providers.

The value of an eHealth record for a patient's medical care will largely depend on the information it contains about the patient's health status and the care they've received. As the patient's healthcare provider you could explain how the patient might set access controls in a way that is beneficial to them given their clinical situation. You could also explain the clinical implications of excluding particular

[46] Previously known as Record Access Code (RAC) or the Provider Access Consent Code (PACC).

[47] Previously known as Limited Document Access Code (LDAC) or Provider Access Consent Code Extended (PACCX).

[48] Note that once a consumer provides the RC or DC to a healthcare provider, their HPI-O is added to the list of healthcare providers that are authorised to access the consumer's whole record or the restricted documents, as the case may be. This access is on an ongoing basis, until the consumer revokes access, which they can do from their eHealth record portal. These access codes are for a single use only and it is not permitted for healthcare providers to keep or record the codes.

[49] The consumer can set levels for Read and Write access for particular healthcare organisations to particular types of clinical documents. These options are explained in **http://www.ehealth.gov.au**.

[50] These documents remain stored in the eHealth record system for audit and legal purposes, but are not viewable in normal use of the system.

information and limiting access to certain types of providers who may need to access the record from time to time to facilitate their care of the patient in the future.

Healthcare providers are encouraged to talk with their patients as discussed above, for example, and to use normal clinical judgement in situations where information may be absent or incomplete.[51]

The Role of Nominated Healthcare Provider and the Consent Process

A consumer's nominated healthcare provider can be a medical practitioner, registered nurse or an Aboriginal and Torres Strait Islander health practitioner. It is expected that, for the majority of people seeking healthcare in Australia, the nominated healthcare provider will be the patient's regular GP, although in some situations it may be appropriate for a private specialist to have this role.

The healthcare provider authoring a Shared Health Summary is likely to be involved in ongoing care for the patient, or may be responsible for coordinating care across multiple healthcare providers.

To create a Shared Health Summary, the healthcare provider will need to obtain the patient's agreement that:

- the healthcare provider is to be the individual's Nominated Healthcare Provider;
- the healthcare provider is to create and upload the Share Health Summary for the patient;

It is a good idea for the healthcare provider to have a conversation with the patient about the type of information the provider will include in the Shared Health Summary. There is no requirement for the patient to review the Shared Health Summary before it is uploaded to their eHealth record.

When creating the Shared Health Summary, the Nominated Healthcare Provider needs to ensure that all aspects of it have been completed and take reasonable steps to verify the accuracy of the information it contains. In assessing its content, the Nominated Healthcare Provider should take into account other relevant information on the patient's eHealth record.

When they register for an eHealth record, the patient provides a standing consent for their health information to be uploaded to the PCEHR. Provided that the patient has agreed for the healthcare provider to create their Shared Health Summary, further consent is not essential given the standing consent that has already been provided.

If a nominated healthcare provider wishes to change the information in their patient's shared health summary, e.g. the medications listed, they will need to upload a new shared health summary with the updated information. Note that there is no additional responsibility for a nominated healthcare provider to update a shared health summary outside of a consultation with the patient[52]. Sections 4.5.3 and 5.4 of the

[51] See the AMA PCEHR Guidelines for further related information: **https://ama.com.au/ama-guide-using-pcehr**.

[52] In addition, see **http://www.mbsonline.gov.au/** for information on item numbers relevant to actions related to patients' eHealth records, which can be found by searching for "PCEHR" on the website.

AMA's Guide to Using the PCEHR (discussed below) provide guidance to medical practices in these and related areas.

There can only be one nominated healthcare provider at one time. If a patient wishes to appoint a new nominated healthcare provider, they can ask another registered and authorised healthcare professional to author and upload their shared health summary. By doing this that healthcare provider automatically becomes the patient's nominated healthcare provider.

A patient is not required to have a Nominated Healthcare Provider. However, if a patient has never had a Nominated Healthcare Provider, the patient's PCEHR will not contain a Shared Health Summary.

What's involved in your Practice participating

In addition to considering the topics above, to participate in the eHealth record system your practice will also need to undertake a range of other actions, which are described in detail later in this guide. In summary, these include:

- Be registered with the HI Service and assigned a HPI-O that is linked to your practice's current Human Services Site PKI Certificate (or request one in your application to register);
- Ensure your Desktop Software is working with the HI Service. This is an **essential prerequisite** for the eHealth record system and other eHealth services and solutions;
- Request a NASH PKI Certificate for Healthcare Organisations for your practice and, where necessary, Human Services Individual PKI certificates for clinicians and authorised staff who require one for their roles;
- Review the PCEHR Participation Agreement and the PCEHR Rules and implement the necessary pre-registration requirements. This importantly includes the requirement to have written policies in place regarding security and access control, and also the establishment of formal roles and, if necessary, the design of Access Flags for eHealth record access; and
- Register your practice for the eHealth record system. This involves completing a form (online in HPOS or in paper) and for the PCEHR Participation Agreement to be signed by each legal entity in your practice organisation.

You are also encouraged to investigate the position of your Medical Defence Organisation (MDO) with respect to covering your practice for potential eHealth record liability issues. Many MDOs are supportive of the system and provide cover, but you should check that this is also at the practice level and not just at the individual practitioner level, as the Participation Agreement is signed by your practice as a legal entity and not by individuals.

The AMA has published a document titled ***AMA Guide to Medical Practitioners on the use of the Personally Controlled Electronic Health Record System***, which provides very useful advice and guidance for medical practices regarding these and other aspects of the eHealth record system. The AMA provides the following websites related to the eHealth record system:

https://ama.com.au/ama-guide-using-pcehr; and

https://ama.com.au/getting-ready-pip-ehealth-incentive-and-pcehr

In addition, the RACGP and NEHTA have websites dedicated to the eHealth record system respectively at:

http://www.racgp.org.au/your-practice/e-health/ehealthrecords/

http://www.nehta.gov.au/registration-support

Online Learning Resources for the eHealth Record System

The Learning Centre (available at **http://publiclearning.ehealth.gov.au**) contains education and training modules that will help you better understand the eHealth record system and how to use it. These modules include:

- eHealth record introduction
- eHealth record evolution
- Understanding privacy and security
- Clinical information systems and eHealth records
- Getting your practice ready (including data quality and roles and responsibilities)
- Provider registration
- Clinical scenarios
- Potential uses
- How to use the provider portal

For further information, you can also call the helpline on 1800 PCEHR1 (1800 723 471).

In addition, the RACGP hosts webinars on the eHealth record system and offers a suite of online educational modules about eHealth that can be accessed respectively at:

http://www.racgp.org.au/your-practice/e-health/ehealthrecords/pcehr/webinar-resources/

http://thinkgp.com.au/education/content/15016

What to do if something goes wrong

While the eHealth record system has many safe-guards and cross-checks it is possible that errors may occur in the data it holds and clinical incidents may unfortunately result.

NEHTA and The Department of Health have established a process for the reporting, monitoring and analysis of incidents. This is described in Section **7.3** and the

process will be updated from time to time. A discussion on clinical safety and eHealth is included
in Section **3.6** below.

3.4 Protection of Health Information

Medical practices and other healthcare providers understand the need for patient privacy and confidentiality, and already have many processes, policies and procedures in place to maintain this. However with the rollout of eHealth initiatives, additional security controls may be needed. Implementing these controls increases the level of protection of health information for both patients and healthcare providers and helps prevent potential unauthorised access. These technology-related aspects are discussed above in Section **3.2.3**.

In addition, health information is protected by specific privacy laws in Australia, including Commonwealth (Cth), State and Territory Legislation:

- The Privacy Act 1988 (Cth) is the key piece of legislation in Australia and regulates how organisations collect, use, disclose and secure personal information and provides individuals with rights of access and correction.
  All healthcare organisations are expected to comply with the Privacy Act;
- The PCEHR legislation provides further assurances by setting out civil penalties for unauthorised use, collection, disclosure of information held in a patient's eHealth record, as does the Healthcare Identifiers Act for the unauthorised use and disclosure of healthcare identifiers, including possible imprisonment for years for an individual; and
- In addition to legal obligations, professional and ethical codes and standards also apply to healthcare providers in order to ensure that the confidentiality of individuals' health information
  is protected in the health sector.

Links to the key pieces of legislation and other regulatory instruments relevant to eHealth are included in the following section.

In addition, the Office of the Australian Information Commissioner provides the following websites for privacy information relevant to healthcare identifiers and the eHealth record system:

http://www.oaic.gov.au/privacy/privacy-act/healthcare-identifiers

http://www.oaic.gov.au/privacy/privacy-act/e-health-records

http://www.oaic.gov.au/privacy/applying-privacy-law/legally-binding-privacy-guidelines-and-rules/pcehr-information-commissioner-enforcement-powers-guidelines-2013

3.5 eHealth-related Legislation

eHealth is enabled through a set of legislative instruments that are designed to guide, and in many respects control organisations and people involved in eHealth, e.g. government agencies, healthcare providers, eHealth product and service suppliers, and consumers. The legislation also provides protections in many cases and penalties for breaches.

The following list of legislation, current at the time of writing, is provided for reference.

Healthcare Identifiers Act 2010 (as amended):

http://www.comlaw.gov.au/Details/C2012C00590

Healthcare Identifiers (Consequential Amendments) Act 2010:

http://www.comlaw.gov.au/Details/C2010A00073

Healthcare Identifiers Regulations 2010:

http://www.comlaw.gov.au/Details/F2013C00700

Personally Controlled Electronic Health Records Act 2012 (as amended):

http://www.comlaw.gov.au/Details/C2013C00295

Personally Controlled Electronic Health Records Regulation 2012:

http://www.comlaw.gov.au/Details/F2012L01399

PCEHR Rules 2012:

http://www.comlaw.gov.au/Details/F2012L01703

PCEHR (Assisted Registration) Rules 2012:

http://www.comlaw.gov.au/Details/F2013C00314

PCEHR (Information Commissioner Enforcement Powers) Guidelines 2013:

http://www.comlaw.gov.au/Details/F2013L01085

PCEHR (Participation Agreements) Rules 2012:

http://www.comlaw.gov.au/Details/F2012L01704

PCEHR Participation Agreements and FAQs:

http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/providerregistration_participationagreement

3.6 Clinical Safety and eHealth

It has become increasingly recognized internationally that deployment of health information systems can improve healthcare's effectiveness and safety. However, there is a growing awareness that information technologies such as the electronic health record and related systems can also introduce new types of errors if not designed and deployed carefully.[53]

There is a range of potential causes of clinical safety issues and risks related to eHealth. The above paragraph mentions design and deployment, which are crucially important, and deal with topics such as useability, process (or workflow) design, education, training and support.

In addition, the quality of the data in clinical systems is vitally important as that data is used to inform decision making and determine actions that may create risk or unfortunately cause harm. Having high quality data in your practice's computer systems is essential to participate effectively in the national eHealth system and more importantly to improve patient safety. This is because your practice's data will be shared and possibly relied upon by other healthcare providers, and vice versa. Improving data quality is dealt with in detail later in this User Guide.

There is a vast amount of literature available on clinical safety and eHealth (or Health IT, as it is also called). One key text is titled "Health IT and Patient Safety: Building Safer Systems for Better Care" [54], which amongst many important topics and concepts, discusses the notion of a Sociotechnical System – "The sociotechnical perspective takes the approach that the system is more than just the technology delivered to the user. The overall system—the sociotechnical system—consists of many components whose interaction with each other produces or accounts for the system's behaviour".

The diagram at the right illustrates the components of a sociotechnical system.

Each of these components requires developing an approach to clinical safety for healthcare organisations, both individually and how they interact with each other and as a whole. Clinical safety is a critical responsibility of clinical governance, which is discussed later in this User Guide in the context of eHealth.

In recognition of the increasingly important and dependent role of eHealth in

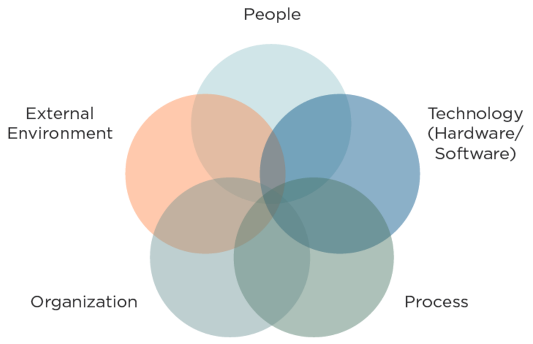


FIGURE 3-1
Sociotechnical system underlying health IT–related adverse events.

SOURCE: Adapted from Harrington et al. (2010), Sittig and Singh (2010), and Walker et al. (2008).

[53] Quoted from the following paper that provides a thorough analysis of safety and health IT systems: A.W. Kushniruk, et al., National efforts to improve health information system safety in Canada, the United States of America and England, Int. J. Med. Inform. (2013), **http://dx.doi.org/10.1016/j.ijmedinf.2012.12.006**.

[54] National Research Council. *Health IT and Patient Safety: Building Safer Systems for Better Care*. Washington, DC: The National Academies Press, 2012, available from **http://www.nap.edu/catalog.php?record_id=13269**.

healthcare, the organisations that set standards accredit and provide guidance for healthcare provider organisations and individual healthcare professionals all include eHealth in the scope of their roles and processes. It is accepted that information is a critical resource (and/or an asset) that needs to be managed and protected as its use becomes more wide-spread and shared both electronically and by other means, and depended upon.

The Australian Commission on Safety and Quality in Healthcare (ACSQHC), as the peak body for clinical safety and standards, has a significant focus on the role of eHealth and actively integrates it into the portfolio of standards and guidance that it provides and regulates.[55]

[55] As an example, see **http://www.safetyandquality.gov.au/our-work/safety-in-e-health/**.

4 Benefits to Your Practice

There is a broad range of potential benefits to be achieved from the effective use and progressive uptake of eHealth. The key areas of benefits include:

- Improving your practice's ability to comply with practice standards and requirements for patient safety, risk minimisation and quality improvement (e.g. for accreditation);
- Providing an opportunity for your practice to strengthen its clinical governance arrangements and interact more effectively with other healthcare organisations and practitioners involved in the care of your patients; and
- Creating considerable efficiencies and cost savings for your practice when eHealth is implemented competently, including when business processes are designed to take optimal advantage of the new and evolving eHealth functionality.

Achieving benefits from the use of eHealth in your practice is progressive in nature, i.e. it starts off slow and grows as you and other healthcare providers use more and more of its features and as increasing numbers of healthcare providers participate in the national eHealth system.

The benefits also won't just occur on their own, e.g. from simply installing and configuring conformant software. It is likely that changes in work practices and other organisational and business aspects will be required in order to achieve what you should reasonably expect. This aspect of planning and implementation is discussed in the chapter that follows.

By implementing eHealth as outlined in this User Guide, you in effect start and progress your practice on the eHealth journey. The approach, starting with implementing Healthcare Identifiers, provides an opportunity to establish accurate patient, practitioner and practice identification information in your computer systems. This is an imperative for data quality and integrity, which is essential for quality improvement activities and improved practice performance. The implementation of Healthcare Identifiers in your practice is also an essential prerequisite for the implementation of all other eHealth features.

The information that follows outlines the types of benefits that you should reasonably expect from the implementation of eHealth over time.

4.1 Broad Benefits from Participating in eHealth

The Australian Government's eHealth program aims to provide you and your practice with the following:

- More timely access to accurate and more comprehensive information about your patients, including their medical history and treatment. The eHealth record system supports and enhances examination and questioning during consultations;
- Quick and efficient sharing of patient information between clinical colleagues, for example between a GP and a specialist, in the case of shared patients;
- More time treating patients, less time spent tracking down records and test results, through faster access to relevant information – helping you make better clinical decisions and spend more time on patient care;
- Access to potentially life-saving patient information in an emergency situation;
- Patients have online access to their eHealth records and tools designed to help them to better manage their health, especially those with chronic and complex conditions; and
- Synergies and a critical mass of participating healthcare organisations to create a more connected healthcare system, which will ensure better continuity and coordination of care.

4.2 Meeting Practice and Governance Requirements

To the maximum extent possible, this User Guide aligns with and aims to support your practice's use of eHealth in meeting the relevant requirements of organisations such as the Australian Commission on Safety and Quality in Healthcare (ACSQHC), specialist medical Colleges and the Royal Australian College of General Practitioners (RACGP)[56]. This includes in the areas of:

1. **Governance for Safety and Quality** in healthcare services, through integrated systems of governance to actively manage patient safety and quality risks;
2. **Patient Identification**, including improving data quality, e.g., matching demographic data with that held in the HI Service, etc.;
3. **Clinical Handover**, including referrals, handling discharge summaries, etc.;

[56] See RACGP Standards for General Practices 4th edition **http://www.racgp.org.au/your-practice/standards/standards4thedition/**, and particularly Appendix B - Clinical Governance: **http://www.racgp.org.au/standards/appendixb**.

4. **Quality Improvement** using practice data, including increasing focus on the clinical safety, risk management and quality improvement aspects of Clinical Governance;

5. **Supporting Preventative Care** through improved management of patient information, including standardised coding of conditions and use of Shared Health Summaries, etc.; and

6. **Secure and consistent electronic communication** and the move to less paper, including addressing privacy, security and confidentiality concerns.

This User Guide supports all of these objectives. The introduction of Healthcare Identifiers is fundamental to supporting patient identification requirements (in reference to item 2 above, and for example as outlined in RACGP Standard 3.1, Criterion 3.1.4[57]), and is a critical first step in introducing eHealth in Australia and into your practice.

Conformant Desktop Software is now available that can provide your practice with access to a rich set of eHealth functionality in support of the above requirements. Subsequent releases of the software with additional eHealth functionality will further enable your practice to more comprehensively address the requirements discussed above, and achieve the expected benefits over time.

4.3 Patient, Practitioner and Practice Benefits

Through their support of technical and practice standards, the eHealth features in your Desktop Software, when implemented and used effectively, should provide your practice and patients with a range of benefits. In broad terms these include:

Shared Health Summaries, Event Summaries and the eHealth Record System

- Improved decision making through access to patient clinical history that is shared for clinicians providing ongoing care for a patient, with access being under the patient’s control;

- Ability to validate rather than recapture a patient’s medical history (thus avoiding full reliance on the patient’s memory), and improved delivery of multi-disciplinary care for patients with complex needs, i.e. supporting a team based system of healthcare delivery;

- Particular advantages for updating relevant clinical information for Aboriginal and Torres Strait Islander peoples, mobile populations and for patients who do not have a regular healthcare provider; and

[57] Amongst other important things, this standard states “Correct patient identification is vital for patient safety and the maintenance of patient confidentiality”.

- Significant benefits for gaining information about un-referred patients who often get lost in the system and for whom information about clinical events is sometimes not captured.

eMedication Management, including Electronic Transfer of Prescriptions (ETP) and improved ePrescribing

- Reduced potential for errors of transcription and/or interpretation, leading to improved health outcomes through lower dispensing error rates;
- Electronic prescriptions will allow more flexibility and convenience for the consumer (e.g. the existing need for consumers to re-visit their prescriber to have lost prescriptions re-issued can be avoided in many instances) [58];
- Prescribers can avoid hand-signing prescriptions through the use of electronic signatures, and thus obtain savings in the use of paper, printing and the time involved; and
- Build a technical foundation for improvements in the quality use of medicines and medicines safety in clinical practice for medication management.

Electronic Referrals, Specialist Letters and Discharge Summaries

- Improved accuracy of demographic information via healthcare identifiers, promoting the rapid identification of patients, providers and services, minimising duplicate records and accelerating information exchanges for decision making;

- Improved accuracy of clinical information via secure and structured communications between referrers (e.g. general practitioners) and referees (e.g. specialists), promoting safety, error reduction and reduced duplication of clinical and administrative effort;
- Improved cost-efficiencies via increasing interoperability of practices and systems, with a corresponding decrease in miscommunication, unnecessary testing and associated risks; and
- Improved coordination of services and treatments, from diagnosis to interventions, leading to improved continuity of care and increasingly integrated care.

Diagnostic Services, including eRequesting and eReporting for Pathology and Diagnostic Imaging

- Increased confidence that previous results can be matched to the correct person and be considered when producing future cumulative reports;
- Removes the need for multiple messaging portals and increases confidence that results will be delivered to the correct requesters at the correct locations;

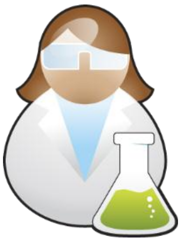
[58] It should be noted, for the current version of ETP as discussed earlier in Section **3.3.2**, that this functionality and that of the dot-point following will not be available, i.e. the signed paper prescription will still be required. This will be required until changes to government regulations are developed and passed changing this requirement, and when software is then updated. This process may take years.

- Supports patient choice of providers, and allows requesting doctors to more easily compare results from different providers on the same patient;

- The generation of an electronic request that is sent to a provider will reduce interpretation and transcription errors resulting from poorly produced handwritten requests, and reduce patient inconvenience due to re-testing, etc.;

- The inclusion of diagnostic test results in consumers' eHealth records will increase the value of the eHealth record system to patients through providing access to results so they can play a greater role in their own health; and

- Access to a patient's prior test results could reduce the number of unnecessary duplicate tests ordered resulting in a decrease in wasted resources and inconvenience to both the healthcare system and to the patient.



The electronic exchange and sharing of patient documents and reports between healthcare providers will ultimately lead to improved safety and quality, through the exchange of timely, accurate and structured information, enabling better patient outcomes and the possibility of reduced medico-legal risk.[59]

As discussed earlier in Section **3.1**, the full availability of some of the above eHealth functions is dependent upon further specifications, and the development and completion of policy and regulatory activities. You can check which eHealth features are available in your Desktop Software from the website included in Section **1.3** above.

4.4 Realisable Benefits for Your Practice

When implemented successfully and used effectively, the eHealth features available in your Desktop Software can provide significant benefits to your practice. As an example, the benefits of using electronic secure messaging include:[60]

- **Fast message delivery and reduced handling**. After the delay from postal delivery, traditionally mail is opened, sorted, placed into a doctor's mail-box, read/actioned, and sent to a nurse or receptionist for action or scanning – and often sits in the scanning pile for 2-3 days. This process is subject to delays, data losses (e.g. through misfiling) and is less organised than secure messaging.

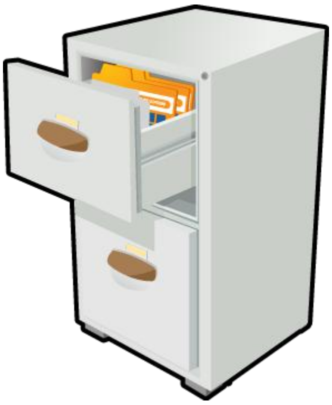
[59] See 'Electronic records tied to fewer malpractice claims' - Reuters Health article: **http://www.reuters.com/article/2012/06/26/us-records-malpractice-idUSBRE85P1EW20120626**

[60] Adapted from "General Practice Cost/Benefits Analysis for Using Secure Messaging", South East Alliance of General Practice, 2008; and also see Medical Observer 16 March 2012, page 5, "Secure messaging switch could save practices $30,000 to offset PCEHR" article.

Secure messages are read and actioned by a doctor, and incorporated into the practice's electronic record. The sender, through the software they use, also receives notification of message receipt or delivery failure;

- **Reliable message delivery**. Reduces resending of information, duplication of effort, and wasted time in chasing up receipt of documents/referrals; and
- **Improved clinical data management**, which reduces clinical errors and directly contributes to better patient care. It is much easier to transfer more comprehensive clinical information to the other healthcare professionals involved in the patient's care directly, thus improving the level of patient care through a better informed care team.

These benefits can result in cost savings for practices that implement secure messaging for incoming and outgoing communications (and other related eHealth features) from such changes as:



- Reduced faxes sent, stationary used, stamps/postage, staff handling and follow-up phone calls;
- Reduced staff time spent keying in data, scanning, filing and retrieving paper documents;
- Increased efficiency in creating clinical documents and reports, as key clinical data is available electronically; and
- More data available electronically, providing improved data searching and patient record interrogation for recalls, reminders, service design, etc.

A benefit from the implementation of Secure Message Delivery (SMD – Section **3.2.2** above) specifications is that healthcare providers will be able to exchange messages with other healthcare providers who also use a messaging service provider that is SMD-compliant[61]. This standardisation will make exchanging messages as easy and as ubiquitous as emailing, but with dramatically higher levels of security and reliability.

4.5 Practice Incentives Program for eHealth (ePIP)

The previous chapter discussed the eHealth features that your practice could utilise through implementing the latest version of your Desktop Software, and the above sections outlined the types of benefits that you should reasonably expect from their use over time.

To encourage the uptake of the national eHealth system, the Australian Government has introduced an update to the Practice Incentive Program (PIP) for eHealth

[61] Note that existing messaging providers will need to update their systems to be SMD-compliant, if not already. In addition, messaging providers will also need to enter into commercial interconnectivity agreements to exchange messages between their systems using SMD.

Incentives (ePIP for short) for accredited general practices, with effect from 1 February 2013.

This adds further encouragement to vendors to include these features in their products, which will also benefit specialist practices that use Desktop Software products that conform to the ePIP requirements.

There are five requirements that general practices need to satisfy in order to gain access to the new ePIP payments. In summary these are:

1. Integrating Healthcare Identifiers into Electronic Practice Records
2. Secure Messaging Capability
3. Data Records and Clinical Coding
4. Electronic Transfer of Prescriptions
5. Personally Controlled Electronic Health Records

Your Medicare Local can provide advice and assistance in having your practice become and remain eligible for the payments from the updated ePIP.

Human Services has sent letters to general practices outlining eligibility requirements and important timeframes for the ePIP, including a helpful Compliance Checklist.

By following the guidance offered in this User Guide, practices will be well positioned to gain access to the ePIP payments. Note that the ePIP program has specific timeframes within which actions are required to be undertaken, so it is recommended that you review the requirements and undertake planning and implementation as soon as is practicable.

Detailed and useful information is available at the following websites:

http://www.racgp.org.au/your-practice/e-health/ehealthrecords/epip/
for useful information on requirements, eligibility and downloadable policy template documents for requirements that require written policies

http://nehta.gov.au/pip
for information specific to the ePIP, including Implementation Overview documents for each requirement

http://www.medicareaustralia.gov.au/provider/incentives/pip/files/9977-1301en.pdf
for a booklet from Human Services outlining practice eligibility and guidelines for the five requirements of the ePIP in greater detail

https://epipregister.nehta.gov.au/registers
to view the PIP eHealth Product Register to see what Desktop Software products are conformant

http://www.medicareaustralia.gov.au/pip
for general information about PIP, including access to forms and guides, and the latest information on requirements and eligibility

https://ama.com.au/getting-ready-pip-ehealth-incentive-and-pcehr
for AMA's advice on getting ready for the ePIP and PCEHR

http://www.nehta.gov.au/registration-support

for helpful resources for organisations providing support to general practices as well as for practices registering independently for the ePIP

The Practice Nurse Incentive Program and the eHealth record system

In addition to the ePIP, accredited general practices, as well as Aboriginal Medical Services and Aboriginal Community Controlled Health Services, may be eligible to participate in the Practice Nurse Incentive Program (PNIP).

The PNIP provides incentive payments to practices to support an expanded and enhanced role for nurses working in general practice. An example of this may be that practices could choose to have their practice nurse talk to patients about the eHealth record system, and help patients set up their record.

Further information on the PNIP is available at:

http://www.medicareaustralia.gov.au/pnip

5 Planning and Implementation

This chapter of the User Guide:

- Commences by discussing important topics and issues that you need to be aware of and do something about in order to obtain optimum benefits from your participation in the national eHealth system. This includes how to identify the work process, organisational and governance changes necessary to make most effective use of the new eHealth features included in the updated Desktop Software you use;
- Then provides planning and implementation guidance initially on the Healthcare Identifiers (HI) functionality, which is an essential prerequisite for all other eHealth features and is a critical initial step in your eHealth journey that is important to get right; and
- Concludes with planning and implementation advice on the other eHealth features, including the eHealth record system, that are within the scope of this release of the User Guide (see Section **3.1)**.

The subsequent chapters that follow this chapter outline steps you can undertake to verify that the implementation of the eHealth features is successful and provides advice on how to access further information and assistance related to their use in your practice.

5.1 Clinical Governance and eHealth

Clinical governance covers areas such as patient safety, risk management and quality improvement. It refers to the set of relationships and responsibilities established by a healthcare service between its executive, workforce (clinical and non-clinical) and stakeholders (including consumers). It provides a system through which clinicians and managers are jointly accountable for patient safety and quality care.

The purpose of clinical governance is the promotion of safety and quality, which eHealth, in addition to other capabilities in your practice, can improve.

The Australian Commission on Safety and Quality in Health Care (ACSQHC) describes a model of governance in Standard 1 in its National Safety and Quality Health Service Standards[62] that includes both corporate and clinical governance, where corporate governance provides a structure through which corporate objectives

[62] See ACSQHC – Standard 1: Governance for Safety and Quality in Health Service Organisations: **http://www.safetyandquality.gov.au/wp-content/uploads/2012/10/Standard1_Oct_2012_WEB1.pdf**; and
ACSQHC – National Safety and Quality Health Service Standards Sept 2012: **http://www.safetyandquality.gov.au/our-work/accreditation/nsqhss/**.

(e.g. social, fiscal, legal and human resources) are set and achieved, and performance is monitored.

The ACSQHC defines clinical governance as:

A system through which organisations are accountable for continuously improving the quality of their services and safeguarding high standards of care.

Accreditation standards, such as those of the ACSQHC, the RACGP and Australian Council of Healthcare Standards (ACHS), require the establishment of clinical governance.

In order to meet the standards applicable to medical practices, including those of the RACGP[63], practices require, amongst other things, good business processes, good information systems and good data. Implementing eHealth as outlined in this guide supports these requirements.

5.1.1 Focus on Clinical Care Outcomes, not Technology

The eHealth literature repeatedly recommends and appeals to those implementing eHealth to focus on improving patient outcomes rather than implementing technology for its own sake. A clinical governance framework for eHealth in your practice should be established with a mandate to provide oversight, monitoring and support for the implementation of eHealth deliverables that impact clinical care and patient outcomes.

The use of eHealth in your practice (especially the eHealth record system) will sharpen the focus on increased clinical safety risks and data governance issues. This is due to increased reliance on the successful integration of health information systems and information sharing models, which are critical both for improved clinical service delivery and collaborative quality improvement activities.

The absence of good clinical governance may create risks where eHealth systems could incorrectly focus on what can be done technologically and not prioritise innovations that are most relevant to enhancing patient care and practice performance.

5.1.2 Data Sharing and Improving the Care Continuum

A key benefit of eHealth's incorporation into clinical governance is that it can reduce fragmentation across the primary and acute sectors, thus strengthening the coordination and integration of patient care processes across organisational boundaries.

[63] See Standards for General Practice 4th edition related to Clinical Governance at: **http://www.racgp.org.au/standards/appendixb**; and **http://www.racgp.org.au/standards/313**; and **http://www.racgp.org.au/afp/201004/201004steer.pdf**.

At a practice level, the introduction of eHealth may for the first time involve practices sharing patient and clinical information electronically with other healthcare providers. This needs to be done in a way that minimises risks related to safety and medico-legal exposure.

Data shared by your practice to others and data you receive from other healthcare organisations will usually be depended upon for clinical decision making.[64]

Hence, this User Guide recommends, as part of your practice's planning for eHealth, that you design and implement effective clinical governance arrangements – both within your practice and in how your practice "connects" with other local and/or regional healthcare organisations for the safe sharing of patient information.

5.1.3 Clinical Governance Elements, Processes and Resources

In developing a clinical governance framework for your practice, the following elements and processes, which have an impact on clinical utility, clinical effectiveness and clinical safety, would need to be considered from an eHealth point of view:

- Consumer input and engagement (patient focused)
- Clinical safety of products and programs being introduced
- Effectiveness (fit for purpose)
- Data quality and its governance
- Appropriateness of the outcomes to patient care and appropriateness of the interventions being delivered
- Clinical risk management including adverse event reporting
- Complaints management
- Workforce training and enablement
- Measurement of benefits, performance and progress (measures will include core, enablers and interim outcome measures)
- Continuous quality improvement including lessons learnt, barriers and enablers.

Organisations that can provide direct advice and support in the design and implementation of clinical governance arrangements include:

- Your College (e.g. RACGP, RACS, RACP, etc.) and the AMA (see below);
- Your Medicare Local;
- The ACSQHC; and
- Your Local Health Network (LHN).

[64] Note also, as previously mentioned in Sections **1.5** and **3.2.3**, you should implement the RACGP's Computer Information Security Standards (CISS) to maximise the protection of your practice's data and information systems.

Useful Resources for Clinical Governance

NEHTA has developed a Clinical Governance Toolkit for use by Medicare Locals to assist them in establishing clinical governance in their own organisations and importantly to support and connect with clinical governance in medical practices in their communities. The Toolkit is not intended for use by medical practices, but you may find it beneficial to read through it for ideas. Please be sure to contact your Medicare Local's Clinical Governance and eHealth teams for advice and assistance in this area.[65]

Of interest too is that an accreditation system is being introduced for Medicare Locals, which sets a range of standards (including for clinical governance, which the above Toolkit for Medicare Locals is designed to assist them with) that Medicare Locals must comply with under the Deed they have signed with the Commonwealth.[66]

In addition, the AMA has published a document titled *AMA Guide to Medical Practitioners on the use of the Personally Controlled Electronic Health Record System*[67], which includes excellent guidance related to policies and protocols that would be valuable input for the development of a clinical governance arrangement for your practice. It also includes discussion on medico-legal considerations.[68]

You may also find a publication from the Australian Institute of Company Directors (AICD) entitled *The Board's Role in Clinical Governance*[69] useful in increasing your understanding of clinical governance in the broader context.

5.2 Quality Improvement and eHealth

Key requirements of an effective approach to quality improvement, within the context of clinical governance, include:

- The collection and analysis of performance data (clinical and organisational);
- The implementation of strategies for performance improvement, including for adverse event prevention, based on evidence; and
- A patient clinical record that allows for the systematic audit of the contents against those Standards with which the practice is required to comply.

[65] The Clinical Governance Toolkit for Medicare Locals is available at: **http://www.nehta.gov.au/medicarelocal-clinical-governance-toolkit**.

[66] Called the Medicare Locals Accreditation Scheme. See **http://www.agpal.com.au/news/story83/**, and **http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/ml-operational-guidelines-toc~accreditation**.

[67] See **https://ama.com.au/ama-guide-using-pcehr**.

[68] See Section 6.7 of the AMA guide, available from the above URL.

[69] Available for purchase from **http://www.companydirectors.com.au/Director-Resource-Centre/Publications/Book-Store/PUB59**.

In terms of the previous point and the importance of having quality health records in your practice, the RACGP recently published *Quality health records in Australian primary healthcare: A guide*, which was developed by an inter-professional Advisory Group in consultation with colleagues across the Australian primary healthcare sector. It is available at:

http://www.racgp.org.au/your-practice/business/tools/support/qualityhealthrecords/

Section 6 of the RACGP guide, titled *Information sharing and a national e-health record system*, is particularly relevant in this context.

5.2.1 Include eHealth in Quality Improvement

Improving your practice's clinical and organisational performance can be greatly enhanced through incorporating a deliberate focus on eHealth in your Quality Improvement activities.

One approach for this that has proven successful is the eCollaborative model[70] – implemented jointly by NEHTA and the Improvement Foundation[71]. The eCollaborative model promotes the following change principles (copied from its website) that position eHealth as an essential component for quality improvement.

In reading these principles please consider their implementation in your practice.

eCollaborative Change Principles

1. **Build and engage your team**
    - Set realistic goals
    - Communicate with other team members
    - Engage the team
    - Assign roles and responsibilities
    - Reflect on and review what you are doing
2. **Undertake foundational work for the eHealth record system**
    - Obtain a healthcare provider identifier for individual health professionals (e.g. general practitioners, registered nurses and Aboriginal health workers) (HPI-I)
    - Obtain a healthcare provider identifier for your organisation (HPI-O)
    - Obtain a patients' individual healthcare identifier (IHI)
    - Use the HPOS system to link your providers and organisation

[70] See **http://www.ecollaborative.com.au** for more details and how to get involved.

[71] See **http://www.improve.org.au**. Note that the responsibility for delivering the Australian Primary Care Collaboratives program (APCC – see **http://www.apcc.org.au**) has been transferred to Medicare Locals. This was announced by the Health Minister on 8 November 2012.

3. Develop systems to improve and maintain data quality across your clinical system

- Archive inactive and deceased patients' records
- Use consistent disease coding
- Develop a practice policy to ensure that patient's current problem and past history diagnoses are reviewed regularly
- Record results in the right place, including pathology results with HL7[72]
- Use your clinical software or compatible data extraction tool to improve data quality
- Develop systems to maintain data quality, particularly for medications, allergies and immunisations lists
- Engage your patients in ensuring the accuracy of the health information in your database

4. Develop systems to support the Shared Health Summary (SHS)

- Use process mapping to identify opportunities to integrate the SHS into the care team flow
- Decide and document the nominated healthcare provider(s) responsible for maintaining the currency and accuracy of the SHS
- Inform your practice team about the processes of uploading a SHS
- Develop policies and procedures for the checking, uploading and maintaining a SHS

5. Engage your patients in the eHealth record system

- Develop a practice policy on identifying those patients who would most benefit from having an eHealth record
- Inform your patients about the eHealth record system
- Develop systems to obtain informed consent from identified patients
- Develop policies about points of care when patients are prompted to review their SHS
- Develop process for patients to advise of any changes to their medication lists
- Seek patient advice on how they would like to use the eHealth record

6. Develop systems to improve the integration of care by the sharing of a patient's eHealth record across their care team (family, carers, health providers)

- Communicate with your local providers concerning shared eHealth records (including specialists and allied health providers)
- Develop ways to use the eHealth record system with other members of the patient's care team
- Develop processes that include the shared eHealth record in team care arrangements, home medicine reviews, mental health plans, referrals to Emergency, specialists and allied health providers
- Explore tools and resources to share care plans electronically
- Include information about the SHS in referral letters to specialists and allied health providers

[72] HL7 is a standard for the structure of electronic healthcare messages. See **http://www.hl7.org**.

- Discuss strategies with patients for sharing their eHealth record across their care team
- Provide the patient with resources that they can share with other providers concerning their eHealth record

7. **Develop systems and processes to improve patients' self-management skills using the eHealth record system**

- Use the eHealth record system to improve health literacy and self-efficacy
- Ensure the whole practice team is aware of and able to access the eHealth record system to enhance patient self-management skills
- Develop systems and processes to improve patients' self-management skills
- Discuss with patients how they use their eHealth record and how they would like to use it
- Use the eHealth record system to promote other online health resources (e.g. Beyond Blue, Diabetes Australia, etc.)
- Bring patients together at practice level to provide feedback about the eHealth record system and how it can be improved and used

5.2.2 Accurate and Up-To-Date Data is Necessary

Item 2 in the list above clearly positions Healthcare Identifiers as an essential early step in your practice's eHealth and quality improvement journey. Having accurate and up-to-date patient identification data in your information systems is an existing requirement of the Privacy Act and is also an essential prerequisite for eHealth. Other prerequisites include accurate and up-to-date identification data for practice clinicians and staff, and your practice organisation.

In addition, the Shared Health Summary (SHS) is identified in item 4 above as a critical component of the eHealth record system[73]. Maintained by a patient's usual practice or health service (via a clinician in the role of being their Nominated Healthcare Provider – see Section **3.3.3**), the SHS is a "clinically reviewed" summary of your patient's health status at a point in time. The content of a SHS is drawn from data in your Desktop Software, so it is imperative that data in it is of the highest quality possible.

To achieve improved performance and to participate in eHealth effectively your practice will need to produce clinical documents that are *safe to share*. For shared health summaries, your practice will need, at the minimum, to maintain accurate and current allergy reports, medication lists, immunisation records and medical histories for most if not all of your active patients. This scope of required minimum data is likely to expand over time.

[73] The fields within a Shared Health Summary are congruent with the RACGP standards for health summaries. This enables easy creation of Shared Health Summaries from local clinical systems, such as your Desktop Software, into the eHealth record system.

The following points outline the important relationship between data quality in your practice and the effective use of eHealth:

- **Accurate and up-to-date** patient identification/demographic information is required in your practice's clinical records system **before patient IHIs can be downloaded, and**;
    - The correct IHI is required **before patient clinical information can be shared** in the eHealth system; and
- **Accurate and up-to-date** clinician, staff and organisation identification information is required for your HPI-Is and HPI-O(s), **and**;
    - These must be established correctly in your practice also **before patient clinical information can be shared**.

Accurate and up-to-date patient clinical information is required in your systems for the **safe sharing** of health summaries and other clinical documents, e.g. eReferrals, etc.

As discussed earlier, there can be serious consequences to your patients and practice from the sharing (outgoing and incoming) of inaccurate data. This may lead to adverse patient outcomes and an increase in medico-legal risk for the practice.

Besides being vigilant about maintaining accurate and up-to-date data in your Desktop Software, your practice may further improve the quality of its data by following the recommendations in this User Guide relating to Data Recording and Clinical Terminology (introduced in Section **3.2.4** above and also discussed later).

5.2.3 Improving Data Quality and Practice Performance

With support from NEHTA, both Pen Computing Systems (PCS) and the Canning Division of General Practice have developed a simple to use tool to help assess, analyse and improve the quality of data contained within most Desktop Software systems.

The Clinical Data Self-Assessment (CDSA) Tool combines the functionality and capabilities of the Pen Clinical Audit Tool (CAT)[74] and the Canning Data Extraction Tool[75] to allow users to interrogate desktop software and provide a report on data completeness and quality.

The CDSA Tool works with most of the popular Desktop Software products and can provide your practice with the following functionality:

- Report on completeness of patient demographic and heath summary data within the clinical system;
- Report on duplicate patient records within the clinical system;

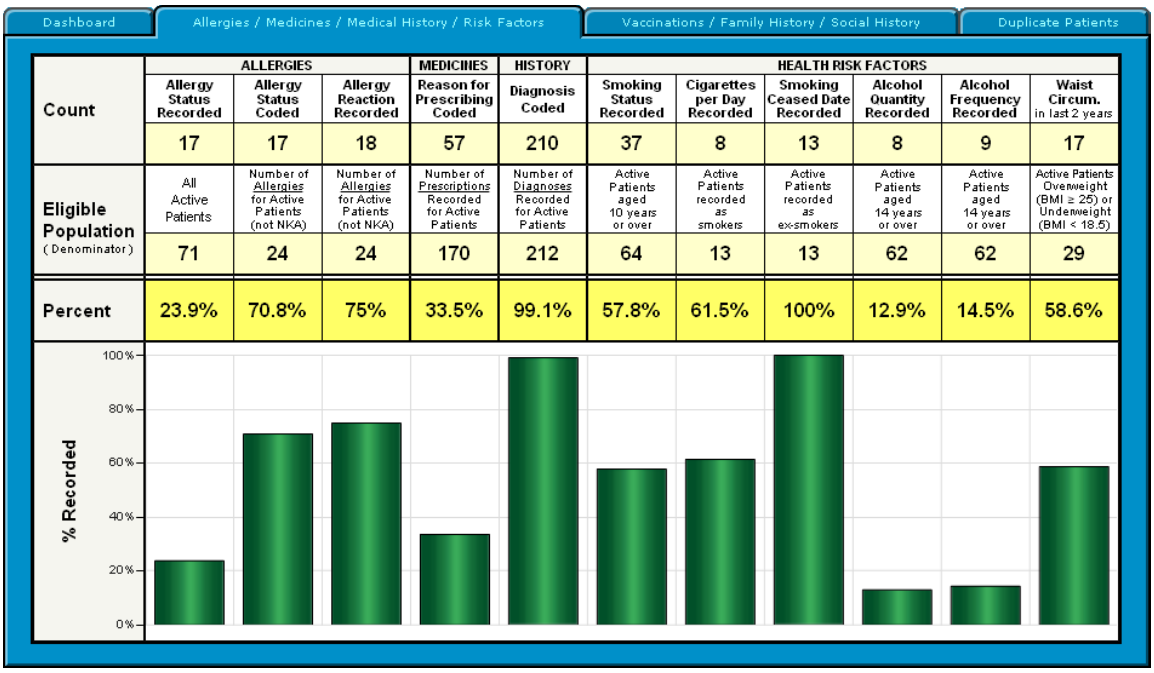
[74] See **http://www.clinicalaudit.com.au/**.

[75] See **http://www.canningtool.com.au/**.

- Provide a ‘dashboard’ or traffic light report on data quality status and improvements which can be made over time; and

- Provide guidance on addressing identified gaps and improving overall clinical data quality.

A sample screen-shot is shown below that illustrates some of the reporting that is possible with the CDSA Tool.


Dashboard
Allergies / Medicines / Medical History / Risk Factors
Vaccinations / Family History / Social History
Duplicate Patients
% Recorded
100%
80%
60%
40%
20%
0%

	ALLERGIES			MEDICINES	HISTORY	HEALTH RISK FACTORS					
Count	Allergy Status Recorded	Allergy Status Coded	Allergy Reaction Recorded	Reason for Prescribing Coded	Diagnosis Coded	Smoking Status Recorded	Cigarettes per Day Recorded	Smoking Ceased Date Recorded	Alcohol Quantity Recorded	Alcohol Frequency Recorded	Waist Circum. in last 2 years
	17	17	18	57	210	37	8	13	8	9	17
Eligible Population (Denominator)	All Active Patients	Number of Allergies for Active Patients (not NKA)	Number of Allergies for Active Patients (not NKA)	Number of Prescriptions Recorded for Active Patients	Number of Diagnoses Recorded for Active Patients	Active Patients aged 10 years or over	Active Patients recorded as smokers	Active Patients recorded as ex-smokers	Active Patients aged 14 years or over	Active Patients aged 14 years or over	Active Patients Overweight (BMI ≥ 25) or Underweight (BMI < 18.5)
	71	24	24	170	212	64	13	13	62	62	29
Percent	23.9%	70.8%	75%	33.5%	99.1%	57.8%	61.5%	100%	12.9%	14.5%	58.6%

At the time of writing, both versions of the CDSA Tool are available for free use. For current licence holders, be sure to download the latest software update to access the CDSA functionality.

For non-licence holders, you can download:

- The Canning Tool from **http://www.canningtool.com.au/**; or

- The Pen CAT tool from **http://install.pencs.com.au/clickonce/clinicalaudit/publish.htm** (user Username cdsa, and Password cdsa1234 when asked).

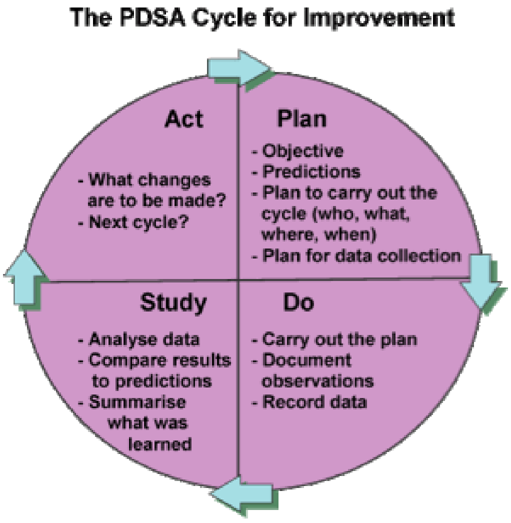
User guides and release notes are available for both versions. For more information about how to improve your data quality using these tools, contact your Medicare Local or your College, including for advice on the potential ongoing costs involved.

Data quality is about more than fixing data errors

The CDSA Tool discussed above can be very useful for your practice to improve the quality of data held in your Desktop Software, but if data quality improvement is not part of an overall and continuous focus on quality improvement, then your practice is not likely to achieve sustainability of the benefits it can bring. In effect, your practice needs an *improvement culture* for these benefits to be sustainable. This approach would, amongst other things, prioritise the prevention of data errors in preference to continual remediation.

The eCollaboratives program introduced above in Section **5.2.1** applies methods and tools from the Australian Primary Care Collaboratives (APCC[76]), which, if you are not already familiar with, would be worthy of your review and serious consideration to implement.

The key component of the APCC's approach is the "Model for Improvement"[77], which provides a framework for developing, testing and implementing changes. It helps to break down the change effort into small, manageable chunks which are then tested to ensure that things are improving and that no effort is wasted. It is worth remembering that while every improvement is a change, not every change is an improvement.


The PDSA Cycle for Improvement
Act
- What changes are to be made?
- Next cycle?
Plan
- Objective
- Predictions
- Plan to carry out the cycle (who, what, where, when)
- Plan for data collection
Study
- Analyse data
- Compare results to predictions
- Summarise what was learned
Do
- Carry out the plan
- Document observations
- Record data

The Model for Improvement includes the PDSA Cycle, which is illustrated in the diagram to the right and can be applied to achieve improved results in many areas of activity in your practice.

In addition to the wealth of useful information and guidance discussed above, the Australian Medicare Local Alliance (AMLA) provides a document entitled "Data Quality Guide: Introduction & Conceptual Framework", which will further improve your knowledge and understanding of improving data quality in primary care. It is available at:

http://www.amlalliance.com.au/__data/assets/pdf_file/0006/43971/Data-Quality-Guide.pdf

The AMLA Guide adopts the Australian Bureau of Statistics' (ABS) Seven Dimensions of Data Quality as the theoretical foundation of data quality. These dimensions are:

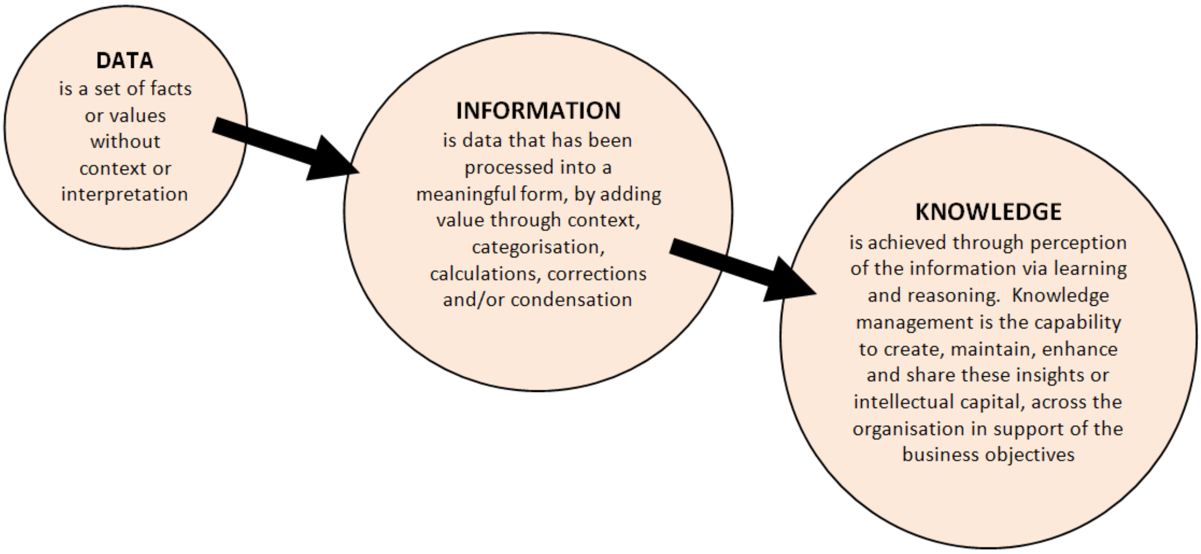
1. Institutional Environment
2. Relevance
3. Timeliness
4. Accuracy
5. Coherence
6. Interpretability
7. Accessibility

In addition, it discusses the "Data-to-Information Pathway Model" (per the diagram below) and the "Eight Essentials for Improving Data Quality", which is a step by step

[76] See **http://www.apcc.org.au**.

[77] See **http://apcc.org.au/about_the_APCC/what_is_a_collaborative/the-model-for-improvement/**.

process that practices may consider moving through to improve data quality. The Guide includes links to useful resources and tools.


DATA
is a set of facts or values without context or interpretation
INFORMATION
is data that has been processed into a meaningful form, by adding value through context, categorisation, calculations, corrections and/or condensation
KNOWLEDGE
is achieved through perception of the information via learning and reasoning. Knowledge management is the capability to create, maintain, enhance and share these insights or intellectual capital, across the organisation in support of the business objectives

5.2.4 Implementing Healthcare Identifiers is an Essential Prerequisite

It is clear from the above that preparing for and implementing Healthcare Identifiers (introduced in Section **3.2.1**) in your practice is a top priority as it is an essential prerequisite for the implementation and use of subsequent eHealth functionality, i.e. none of it can be used without Healthcare Identifiers.

In addition, implementing Healthcare Identifiers in your practice as outlined in this User Guide will further improve the quality of your data and also enable improvements in your practice's overall performance.

5.3 Register of Important eHealth Details

As part of the Quality System for your practice, you will find it useful to maintain a database or register of important eHealth related details, such as:

- Healthcare Identifiers – All HPI-Os of organisations and HPI-Is of clinicians;
- The names of people assigned to Roles, e.g. of RO, OMO(s), Authorised Employees, etc., along with their login usernames, when they were trained on the required policies and any other important information;
- PKI Certificates – A record of all types of PKI certificates used in the practice, i.e. organisational and individual, along with their location, expiry dates, etc.; and
- Other information, such as details related to your Desktop Software, location of the signed eHealth record Participation Agreement, ELS information, SMD provider, and PES provider for ETP, etc.

It will be useful to have this type of information centrally gathered and maintained, so that it is ready-at-hand and up to date when needed. For audit purposes, you may also find it useful for the register to be able to record changes in the information, e.g. who had what Role when, with what login username, and details of replaced PKI certificates, etc.

Your Medicare Local may be able to provide a template and/or advice and guidance on the establishment and use of such a register.

This User Guide recommends that you establish this register and add currently available information to it, and then continue to maintain it as you proceed to the next important steps of implementing the eHealth features, as outlined in the following sections. You will find that having ready access to current eHealth related information for your practice, e.g. of PKI certificates, will be invaluable as you proceed with the approach outlined in this guide.

5.4 Preparations and Considerations for Healthcare Identifiers

This section outlines actions you need to take **BEFORE** installing the software update and utilising the Healthcare Identifier functionality and any other eHealth features it includes. In summary this process entails, in order:

- Understanding how the Healthcare Identifiers Service interacts with other eHealth services and solutions and what the implications are of that for your practice;
- Deciding on a structure for your practice organisation's HPI-O(s), including staff Roles, and taking in consideration factors such as your practice's organisational and business structure, including your PIP entity (for participating general practices); and
- Understanding what's involved in and getting ready to apply for your HPI-O(s) and associating it/them with your clinician's HPI-Is (if needed), including setting up access for nominated staff, and of any necessary security and access control mechanisms, e.g. PKI certificates, Access Flags, etc.

You will find it beneficial to talk about the setting up of Healthcare Identifiers for your practice with your Medicare Local, and/or other organisations that provide you with IT and/or eHealth support, as it can be complex depending on your organisational structure and level of knowledge and experience.

5.4.1 Organisational Entities and HPI-Os

A HPI-O is an identifier for use by a healthcare provider organisation and is a prerequisite for participation in the national eHealth system. The *Healthcare Identifiers Act 2010*[78] defines a healthcare provider organisation as:

> *... means an entity, or a part of an entity, that has conducted, conducts or will conduct, an enterprise that provides healthcare (including healthcare provided free of charge).*

To participate in the HI Service, healthcare provider organisations must register for a HPI-O with the HI Service Operator (currently Human Services). Organisations that are eligible for a HPI-O must meet the following requirements:

- Provide a healthcare service; and
- Employ or contract one or more individual healthcare providers or sole traders who are employed for the purpose of providing a health service.

In addition the eHealth record system has organisational entity requirements that also need to be satisfied before participation can be granted. These are discussed later.

5.4.2 How HPI-Os Could be Used by Your Practice

A key recommendation from this User Guide is for you to keep your practice's HPI-O structure as simple as possible, i.e. ideally with just the one HPI-O (structure options are discussed in the section that follows). If after considering the advice and guidance herein you believe a HPI-O hierarchy is needed for your practice, then it is strongly recommended that you talk about this with your Medicare Local and/or other organisations that provide your practice with eHealth and IT advice and support.

HPI-Os play important roles in different aspects of eHealth, and it is important that you understand these so that your practice's needs can be properly addressed in setting up your HPI-O configuration. HPI-Os are essential foundations for healthcare provider organisations to be clearly and uniquely identified when participating in the eHealth record system, and when utilising Secure Message Delivery (SMD) and other eHealth solutions and services.

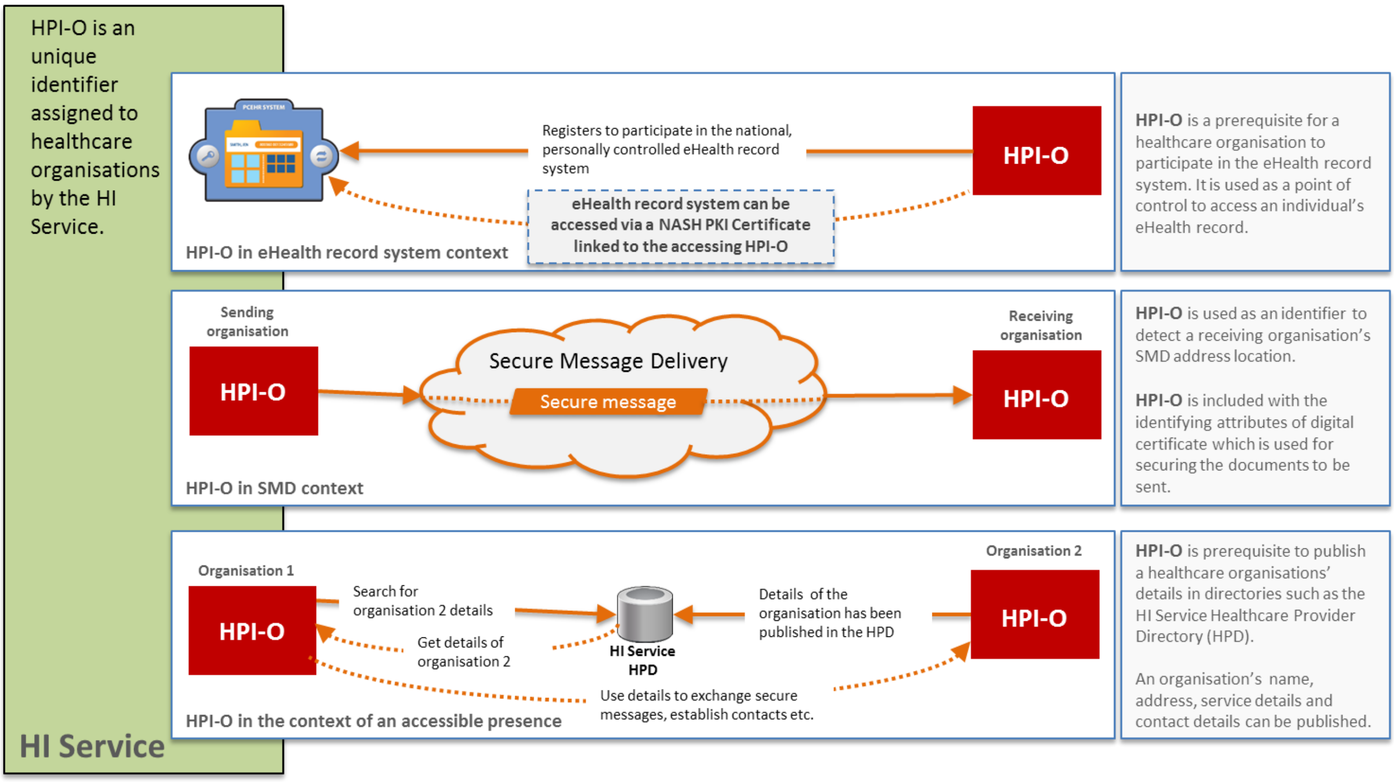
The HI Service is designed to accommodate the needs of a wide range of healthcare provider organisation types and sizes, for example from State health departments, to national chains of medical centres, to single practitioners and everything in between. As a consequence, for organisations like medical practices, it can appear to be complex, which is why this User Guide recommends a simple approach and that you seek advice and assistance.

If the structure of your medical practice organisationally includes separate legal entities, clinics or other services that you wish to be identified separately in the

[78] Healthcare Identifiers Act 2010, Act No. 72 of 2010 as amended; See Section **3.5** for URL.

eHealth system, then it may be advantageous for you to have a structure of HPI-Os, which is discussed later.

The diagram below illustrates that your practice needs a HPI-O[79] to interact with the HI Service, eHealth record system, Secure Message Delivery (SMD) and directories such as the Healthcare Provider Directory (HPD).



HPI-O is an unique identifier assigned to healthcare organisations by the HI Service.

Registers to participate in the national, personally controlled eHealth record system

eHealth record system can be accessed via a NASH PKI Certificate linked to the accessing HPI-O

HPI-O is a prerequisite for a healthcare organisation to participate in the eHealth record system. It is used as a point of control to access an individual's eHealth record.

HPI-O is used as an identifier to detect a receiving organisation's SMD address location.

HPI-O is included with the identifying attributes of digital certificate which is used for securing the documents to be sent.

Search for organisation 2 details

Get details of organisation 2

Details of the organisation has been published in the HPD

Use details to exchange secure messages, establish contacts etc.

HPI-O is prerequisite to publish a healthcare organisations' details in directories such as the HI Service Healthcare Provider Directory (HPD).

An organisation's name, address, service details and contact details can be published.

The key points relating to HPI-Os for your practice to consider are:

- It is possible to use the same HPI-O for all of your eHealth related requirements, i.e. for HI Service access, eHealth record system access, providing contact information of your practice organisation in directories such as the HPD, as a reference for a location for secure messaging, and for your PIP entity (for general practices);
- Alternatively you may establish a separate HPI-O for each, or for a combination of the following, to:
  - Participate in the HI Service;
  - Identify the sending and receiving organisation for secure messaging;
  - Provide a point of control for access to patient's eHealth records and alignment with consent processes to meet patient eHealth record privacy needs (using Access Flags – discussed in Appendix **C.2**);
  - Provide contact and service information of your practice that can be published in directories such as the HPD; and

[79] At least one HPI-O is required, and more may be needed depending on your practice's organisational structure and a number of other factors, which are discussed later.

    - Align with your practice's PIP entity (for general practices).

There are also other uses of HPI-Os, such as being the identifier of a healthcare organisation in all clinical documents (e.g. discharge summaries and referrals), and in NASH PKI certificates. In addition, a record of your practice's HPI-O(s) will be retained by the eHealth record system and the HI Service when they are accessed, for audit purposes as prescribed in the legislation.

Deciding on how you want your practice to participate in the national eHealth system affects what you need to do to register, i.e. there are different forms, rules and processes.

5.4.3 Deciding on Your Practice's HPI-O Structure

The above points introduce important considerations for you in determining how you could design the HPI-O structure for your practice.

As previously mentioned, it is recommended that you consider the simple model of only registering the one Seed HPI-O[80] if your existing practice structure is amenable to it. To assist in your decision process, if your practice meets all of the following criteria, then you could be confident in proceeding with the simple HPI-O model:

- □ That the practice is a single, or has a primary or overarching, entity that:
    - Provides or controls the delivery of the practice's healthcare services, including support services;
    - Is the employer or contracting entity for healthcare professionals working in your practice, or you are a sole practitioner; and
    - (For general practices) is considered one practice (with or without multiple branches) for Accreditation and PIP purposes;

- □ The practice is centrally controlled and uses (or plans to use) one point (or location/mailbox) to send and receive electronic messages via SMD;
- □ The practice organisationally presents to the market and community as one entity, even if it provides services in more than one location[81];
- □ You wish a "name" of the practice, e.g. as it appears on practice stationary and listed in directories such as the White and Yellow Pages, etc., to be the same as used in the eHealth system, i.e. for SMD, etc.;
- □ Patients' records can be viewed and updated by all healthcare professionals in the practice (and branch locations if applicable), and there is a single

[80] This type of HPI-O and the concept of network hierarchies are explained in:
Appendix C: *Further Information on HPI-O Structuring.*

[81] For general practices, if these additional locations are PIP branches, then this is correct; otherwise if the additional locations are separate entities for PIP, then they will require their own HPI-O.

process allowing for patients to provide their consent to this sharing of their information, including in the eHealth record system when your practice uses it; and

☐ The practice uses one Desktop Software product with one shared database to manage the clinical information for all of its patients and that this product is conformant with the necessary eHealth specifications.

If your practice meets the above criteria, then you can proceed confidently with implementing the guidance offered in this User Guide. In which case the practice:

- Will have only a Seed HPI-O (i.e. you will not need to establish a network hierarchy) and the Seed HPI-O will automatically have an Access Flag[82] assigned to it for the eHealth record system by the System Operator;
- Will have:
  - Its existing Human Services Site PKI certificate currently used for Medicare Online business enabled for the HI Service (or a new one if requested); and
  - A single NASH PKI Certificate for Healthcare Organisations for use with both the eHealth record system and SMD; and
- Will have a single organisational entry in the HPD with that entry also containing the sending and receiving location for SMD (i.e. an ELS, as recorded against your practice's HPI-O in the HI Service and published into the HPD).

What to do if you think the simple HPI-O model doesn't apply

It is recognised that the simple Seed only HPI-O model will not be possible for all medical practices. If you believe the simple model is not appropriate for your practice, then it is recommended that you:

- Read the rest of this User Guide and especially ***Appendix C:*** *Further Information on HPI-O Structuring* to increase your awareness and knowledge of the topic; and
- Contact your Medicare Local and/or organisations that provide you with eHealth and IT advice and support to assess your practice's requirements and determine the most appropriate structure.

The guidance offered to keep your HPI-O structure as simple as possible (within the parameters of the eHealth record system participation requirements) still applies in this situation and should be reinforced in your dealings with organisations providing you with advice and support.

[82] Access Flags are explained in ***Appendix C:*** *Further Information on HPI-O Structuring*. If you proceed with this simple HPI-O model you really don't need to worry Access Flags.

5.4.4 Roles for the HI Service and eHealth Record System

Roles in the HI Service have been designed for use by individual healthcare providers and employees of healthcare organisations. These roles also apply to managing your practice's involvement in the national eHealth record system, and have been developed so that appropriate access to the systems can be assigned for each type of use.

The HI Service and the eHealth record system require people to be assigned to roles, which authorise them to perform certain functions. These roles are:

- **Responsible Officer (RO)** – is the officer of an organisation who is registered with the HI Service and has authority to act on behalf of the seed organisation and relevant network organisations (if any) in its dealings with the System Operator of the eHealth record system. The RO has primary responsibility for their organisation's compliance with participation and legislative requirements for HI Service and the eHealth record system. This role may be performed by the Practice Principal/Owner, who may also be the Public Officer of the practice;[83]

- **Organisation Maintenance Officer (OMO)** – is an officer of an organisation who is also registered with the HI Service and acts on behalf of a seed organisation and/or network organisation in its dealings with the Service Operator of the HI Service (Human Services) and the System Operator of the eHealth record system (Department of Health). An OMO has responsibility for the day to day administrative tasks (including maintaining information about their organisation) related to the HI Service and the eHealth record system. Healthcare organisations can have more than one OMO if they desire. This role may be assigned to the Practice Manager, if you have one, and/or other senior staff who are familiar with the practice's clinical and administrative systems. Alternatively, the RO may take on the OMO role as well;[84]

- **Authorised employee** – an individual within an organisation who requires access to IHI records and provider identifiers from the HI Service to assist with patient administration;

- **Authorised user** – a person authorised by a healthcare organisation to access the eHealth record system on behalf of the organisation. Authorised Users may be individual healthcare providers and other local users who have a legitimate need to access the eHealth record system as part of their role in healthcare delivery; and

- **Individual healthcare provider** – a health professional who provides healthcare services to the general public, who has an HPI-I.

Note that these roles are not mutually exclusive. An individual person may be assigned to one, some or all of them, e.g. the RO could also be the OMO for a solo

[83] See the following information provided by the RACGP on the appointment of an RO: **http://www.racgp.org.au/yourracgp/news/fridayfacts/01-02-2013/** (Second item in RACGP News).

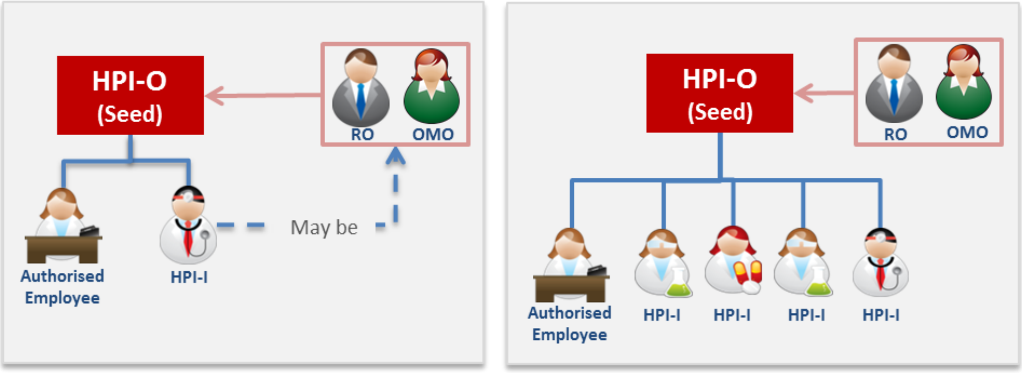
[84] Initially an OMO needs to be set up for the Seed HPI-O. This OMO may then later assign others to the role.

GP practice. The Human Services HI web-page has Information Guides available that explain the responsibilities for the roles above that are related to the HI Service and the eHealth record system:

http://www.humanservices.gov.au/hiservice

The PCEHR Rules 2012 defines the roles of RO and OMO as having the same meanings as specified in the Healthcare Identifiers Act 2010. The Rules include specific responsibilities and obligations for these roles for the eHealth record system that mostly relate to healthcare organisations that plan to have a network hierarchy. If you plan to have a network hierarchy for your practice, then it would be wise to reread the Rules in detail and confirm or change your selection of people nominated for these roles appropriately.

The diagram below illustrates how these roles might be set up for a Seed only HPI-O practice configuration.



Users can only access the HI Service and eHealth record system with strictly controlled access credentials to perform their duties. Functions they are able to perform depend on their role(s). These credentials are controlled with PKI certificates and ensure that each user is able to access their permitted functions with a high degree of security and information protection. The types of PKI certificates that are used by the HI Service and eHealth record system are described earlier in Section **3.2.3**.

Please note that all permitted uses of PKI certificates issued by Human Services should be referred to within the PKI policies for the relevant certificate on their website:

http://www.humanservices.gov.au/pki

The following table summarises the functions that each of the RO and OMO roles may perform on the HI Service and the eHealth record system.

You may also find the following recorded webinar helpful:

http://www.nehta.gov.au/media-centre/multimedia/436-pcehr-responsible-officer-and-organisation-maintenance-officer

Role	HI Service	eHealth Record System
RO	Register a Seed organisation Request a PKI certificate (or link an existing one) for the organisation Maintain the HPI-O details with the HI Service Maintain their RO details with the HI Service (add or remove RO) Maintain OMO details with the HI Service (add or remove OMO) for seed and network levels Retire, deactivate and reactivate the HPI-O Maintain links between the Seed organisation (and any Network organisation/s) and any Contracted Service Providers	Authorising the addition/removal of HPI-Os Adjusting the eHealth Record Access Flags for participating organisations within their hierarchy (OMO at Seed level can also do this) Setting HPI-O/HPI-I authorisation links (OMO can also do this)
OMO	Maintain their own personal OMO details Register a network HPI-O for network levels below Register OMO details for network levels below Validate, link or remove linked HPI-Is to HPI-O(s) they are linked to Publish HPI-O details in the Healthcare Provider Directory (HPD) for HPI-Os they are linked to Request PKI certificate(s) (or link existing one) for organisation(s) they are linked to If required, to maintain a list of authorised employees within the organisation who access the HI Service	Setting and maintaining access flags according to the organisational network hierarchy, in accordance with meeting the principles outlined in the PCEHR Rules Authority to act on behalf of the Seed and Network organisation(s) (that they are linked to) according to the hierarchy Maintain accurate and up-to-date records of the linkages between organisations within their network hierarchy

5.4.5 Setting Up Your Practice's HPI-O and User Roles

The process to actually apply for your HPI-O and assign people to the roles introduced above is outlined in detailed steps later in Section **5.6**, and is described on the Human Services HI Service web-page.[85]

There is a form that will need to be completed and sent in, with the extent of information to be provided dependent upon some pre-conditions related to how your practice organisation and staff are currently “known” to Human Services. It is likely that Evidence of Identification (EoI) documentation will need to be provided to Human Services as part of this process.

[85] See **http://www.humanservices.gov.au/hiservice**.

The process can be comparatively straight forward if your practice organisation is currently registered for Medicare Online (e.g. for online billing), in which case:

- The Human Services Site PKI certificate currently used for Medicare Online Business can be used for the HI Service, but it will need to be HI-enabled (discussed later);

- The person set up as your practice's Duly Authorised Officer (DAO) for your Human Services Site PKI certificate could be set up as the Responsible Officer (RO) for the HI Service[86]; and

- You may choose to set up your RO also as your practice's OMO, or alternatively the Practice Manager and/or other senior staff members may be set up as the Seed OMO.

The above approach is not mandatory and you may choose a different approach, but in the majority of cases in medical practices, this may be the most appropriate.

As part of the process of preparing for implementation, it is recommended that you confirm the current status of PKI certificates for your practice and clinicians. The existence of relevant PKI certificates can be ascertained by searching at the following website:

http://www.certificates-australia.com.au/general/cert_search_health.shtml

Human Services and NEHTA continuously look for opportunities to streamline the application processes for eHealth. A recent improvement is a single form that can be used to:

- Register a Seed Organisation, a Responsible Officer (RO) and an Organisation Maintenance Officer (OMO) with the HI Service and receive a HPI-O;

- Register the Seed Organisation with the eHealth record system; and

- Apply for the PKI certificate necessary to access the HI Service or to HI-enable your existing Human Services Site PKI certificate, if your practice has one.[87]

This form should be reviewed so that you are aware of the information you are required to provide and other actions necessary as part of the application process for both the HI Service and the eHealth record system. Other such improvements may continue to be provided, including implementation of online forms, so please check the Human Services website for updates.

This form *(2978 – Application to Register a Seed Organisation)* is available at:

http://www.humanservices.gov.au/hiservice

[86] The RO for your practice performs this role for both the HI Service and the eHealth record system.

[87] Note that the NASH PKI certificate required to access the eHealth record system and to use SMD can only be applied for after your practice has been registered with the HI Service and issued with a HPI-O.

You should not complete and send in this form at this stage as other prerequisite actions are necessary, which are outlined later. The purpose at this stage in the process is to familiarise yourself with what is required and to gather the necessary information.

If there are any areas that you are unsure about, you may find it beneficial to contact the Human Services HI Service help desk and/or your Medicare Local's eHealth Team for advice and assistance – see Chapter **8**.

5.4.6 Linking Clinicians to Your Practice's HPI-O

In addition to the steps above, it is recommended that the HPI-Is of doctors and other clinicians working at your practice are linked with the practice's HPI-O in the HI Service. In preparation for this:

- You should now collect all the HPI-Is for clinicians in your practice. You will need these at least to enter them into your clinicians' profiles in your Desktop Software (when it is updated) as a valid HPI-I is necessary for the creation of conformant clinical documents. Clinicians should have their HPI-I from correspondence sent to them from AHPRA[88], or they can obtain it from the AHPRA website (**http://www.ahpra.gov.au/**) using their login account, or by contacting Human Services;

- Your practice's clinicians need to be registered as individual healthcare providers with the HI Service. Healthcare providers who are accredited with AHPRA are automatically registered with the HI Service[89]. If your practice has healthcare providers who are not eligible for registration through AHPRA (e.g. dieticians), they may still be eligible to register with the HI Service through contacting Human Services; and

- While not mandatory, it is also strongly recommended that clinicians in your practice:

  - Have their own Individual PKI Certificate[90] should they wish to access the Human Services HPOS website for HI Service and eHealth record functionality; and

  - Set the flag on their HPI-I profile that enables them to be visible in the Healthcare Provider Directory (HPD). This can be done on the HPOS website or by contacting Human Services.

Your practice's OMO will link the HPI-Is of healthcare providers working in your practice with your practice's HPI-O in the HI Service – this can be done in HPOS. When this is done and the clinician consents to their details being visible (per above bullet point), the linkage between them and your practice will then be visible in the HPD.

[88] Australian Health Practitioner Regulation Agency.

[89] AHPRA issues an HPI-I to every registered practitioner in the national registration scheme.

[90] When obtained, it is recommended that clinicians' HPI-Is and details of their PKI certificates be recorded in the Register described in Section **5.3**.

Note that the process described above is different to the linking required between your HPI-O and your clinicians' HPI-Is in the eHealth record system for them to access patient records through that system's Provider Portal. This can also be done in HPOS and is described later.

The process for the above is described in the eHealth implementation steps outlined later in Section **5.6**. At this stage it is recommended that you gather all of this information and establish your practice's readiness in preparation.

5.4.7 Authorised Employees and the HI Service

ROs and OMOs have certain responsibilities under the HI Act, including that they must understand the responsibilities of maintaining a register of individuals or identifying them appropriately in transmissions, i.e. to the HI Service. By having their HPI-I recorded in your Desktop Software, clinicians will be identified in transmissions they make to the HI Service through your Desktop Software.

With regards to Authorised Employees[91], to comply with this requirement of the HI Act, your practice should consider the following:

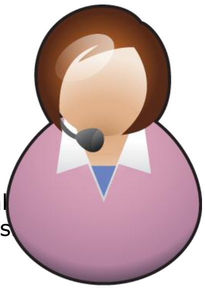
- Your practice should have a policy for user login account management for your computer systems that allocates each user with a unique login code. Besides being considered best practice and aligned with the RACGP's CISS[92], this supports a requirement for use of the eHealth record system under the PCEHR Act[93], which is discussed later. If your practice does not already have this in place, then you will need to do so before progressing to implementing the eHealth record system;

- Your Desktop Software should, through being conformant, pass this unique user login code to the HI Service in each transmission thus permitting the user to be identified in the HI Service;

- You are required by law to maintain the details of employees who access the HI Service, including for up to seven years after they have ceased working at your organisation. The HI Service can request details of these authorised employees under the legislation. You may consider maintaining this list in your practice's Quality System, as discussed in Section **5.3** above; and

- Human Services's HPOS website has a facility where you may upload and maintain a list of the details of authorised employees who your practice allows to access the HI Service on its behalf;

    - It is not mandatory to do this, but you may find it useful if you wish staff to contact the HI Service by telephone



[91] This role is intended for staff, e.g. including those at reception, who are responsible for mal identification information in your Desktop Software is correct, up to date and has an IHI ass

[92] See Section **3.2.3**

[93] The Act requires users of the eHealth record system to be individually identified. Participating healthcare organisations need to be able to identify each person who accesses the system on their behalf, including, for example, all providers, health students, and administrative staff.

to request patient IHIs. This list allows the HI Service to verify your employee's identity before IHIs will be disclosed over the telephone; and

  - If your practice does not require your staff to contact the HI Service by telephone, then maintaining the list of authorised employee details yourself, as discussed
above, should be sufficient.

Authorised Employees do not require a Human Services Individual PKI certificate, and instead access the HI Service through your Desktop Software with its embedded HI functionality[94]. Similarly, access to the eHealth record system is also through your Desktop Software but by using a NASH PKI certificate for Healthcare Provider Organisations. Clinicians do not require NASH Individual PKI certificates to use the eHealth record system, unless they wish to access it through the system's Provider Portal.

The process for setting up Authorised Employees is outlined later in Section **5.6**.

Further Information

The document titled *Healthcare Identifiers Service information guide – Introduction and overview* is recommended reading – available at:

http://www.humanservices.gov.au/hiservice

5.5 Preparations for Other eHealth Services and Solutions

As previously mentioned, implementing the HI Service in your practice is an essential prerequisite for other eHealth functions. The guidance provided above for preparing for its implementation is now extended below with guidance for preparing your practice for:

- The eHealth record system;
- Clinical Terminology;
- Secure Message Delivery (SMD); and
- Electronic Transfer of Prescriptions (ETP).

The guidance suggested in this section assumes that you have decided on your practice's HPI-O structure and the other related HI requirements, as outlined above in Section **5.4**.

[94] Your Desktop Software accesses the HI Service via your practice's Human Services Site PKI certificate.

5.5.1 eHealth Record System

BEFORE applying to register your practice for participation in the eHealth record system and installing the update to your Desktop Software that includes its functionality, you will need to do the following:

- Understand the Legislative and Regulatory Framework;
- Check with your MDO that your Practice is covered (this is not a requirement, but is recommended);
- Review and decide that your practice's legal entity is willing to sign the Participation Agreement; and
- Implement the required written policies.

The above requirements are discussed below.

5.5.1.1 Understand the Legislative and Regulatory Framework

It is important that you understand the legal obligations of participating in the national eHealth record system. These are set out in the:

- Personally Controlled Electronic Health Records Act 2012 (as amended):

  http://www.comlaw.gov.au/Details/C2013C00295

  See Appendix **D.1** for an overview of the Act;

- PCEHR Rules 2012:

  http://www.comlaw.gov.au/Details/F2012L01703

  See Appendix **D.2** for the Rules that are relevant to written policies and user login account management.

  The purpose of the PCEHR Rules is to prescribe requirements for access control mechanisms, identity verification, the handling of specified types of records and participation requirements, including security requirements for healthcare provider organisations;

- Personally Controlled Electronic Health Records Regulations 2012:

  http://www.comlaw.gov.au/Details/F2012L01399

  The purpose of the regulation is to support the effective operation of the PCEHR system by ensuring that HI Service Operator can carry out its expanded functions and share critical information with the PCEHR System Operator, and by providing additional detail in respect of critical definitions in the Act, the operation of the advisory committees and the interaction of state and territory laws; and

- The PCEHR Participation Agreement (discussed below).

A list of legislation relevant to eHealth is included in Section **3.5**. If you have any questions or concerns regarding the legislative instruments relevant to the eHealth record system, you are encouraged to contact the PCEHR Enquiry Line on 1800 PCEHR1 (1800 723 471).

5.5.1.2 Check with Your MDO that Your Practice is Covered

It is your practice organisation, as a legal entity, that signs the Participation Agreement. If there are privacy breaches or other events that create medico-legal exposure related to the eHealth record system, then your current MDO cover may not be adequate, if it is only at the individual clinician level. All the major MDOs have worked collaboratively with NEHTA and The Department of Health in the development of the eHealth record system, are generally supportive of the system and provide policy options at the practice level.

This User Guide does not offer legal advice, but as it is your practice organisation that contracts with the eHealth record System Operator (Department of Health), there are some responsibilities that fall upon your practice to minimise risks related to use of the system by your practice’s clinicians and staff.

These responsibilities include the establishment of written policies (discussed below) and protocols that are:

- Taught to clinicians and staff in your practice;
- Are kept up to date and accurate; and
- Are adhered to.

It is understood that if your practice organisation attends to the above and there is a privacy breach or medico-legal event, then these in-place policies and protocols could be a defence in the case of a suit. You are advised to contact your MDO and check your level of indemnity cover **BEFORE** registering for participation in the eHealth record system and if necessary acquire appropriate practice level insurance.

5.5.1.3 Review and Decide that Your Practice’s Legal Entity is Willing to Sign the Participation Agreement

Each healthcare provider organisation registering to participate in the eHealth record system must enter into a Participation Agreement with the System Operator. The Participation Agreement includes rights and obligations for both the healthcare provider organisation and the System Operator.

The key purpose of the Participation Agreement is to set out obligations relating to the uploading of records to the eHealth Record System, intellectual property arrangements, the allocation of liability between the parties, and the processes for notifying key events and changes.

You may find it beneficial to read the PCEHR (Participation Agreements) Rules 2012:

http://www.comlaw.gov.au/Details/F2012L01704

An executed copy of the Participation Agreement must be submitted with the PCEHR Application Form. Your practice's Seed HPI-O and, if applicable each separate legal entity within a Network HPI-O structure, must sign a copy of the Participation Agreement and attach it to the form.

There are seven different versions of the Participation Agreement to accommodate different types of legal structures for healthcare provider organisations. These and other useful information (including FAQs) about the agreement are available from the following website:

http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/providerregistration_participationagreement

Before signing the Agreement it is important that you read and consider the following documents (available from the above website):

- *Participating in the personally controlled electronic health record system: a registration guide for healthcare organisations*;
- *Frequently Asked Questions for Healthcare Provider Organisations*;
- *Participation Agreement (including the explanatory notes in the margin)*; and
- *Participation Agreement FAQs.*

Participation Agreement

Personally controlled electronic health record system

You need to sign the Participation Agreement **BEFORE** applying to participate in the eHealth record system, as the signed agreement needs to be submitted as part of the registration process. The steps for this are outlined later in Section **5.6**.

At this stage you should review the agreement and decide if your practice's legal entity is willing to sign it. The agreement includes details of who to call for enquiries. If you decide to not sign it, then your practice will not be able to participate in the eHealth record system.

5.5.1.4 Implement the Required Written Policies

Healthcare organisations are required to develop, maintain, enforce and communicate to staff a written policy that ensures the organisation's use of the eHealth record system is secure, responsible and accountable. The requirement for this policy is legislated and applies to all healthcare organisations that wish to participate in the eHealth record system, i.e. it is not a requirement specific only to the updated ePIP scheme. The policy must be reviewed at least annually and when any material new or changed risks are identified by the healthcare organisation.

The policy, in response to Rule 25, needs to address matters such as how authorised persons access the system, the training delivered to staff before accessing the eHealth record system, and the physical and information security measures used by the organisation. Healthcare organisations may choose to update their current security policies to be in line with the requirements of Rule 25. Alternatively, healthcare organisations may choose to implement a new PCEHR-specific policy – sample policy text is available and is discussed below.

To meet the requirements of Rule 25, each organisation's policy should cover (at least) in summary the following key aspects:

- The manner of authorising persons to access the PCEHR on behalf of the healthcare organisation;
- The manner of suspending or deactivating those who leave the healthcare organisation, whose security has been breached or whose duties no longer require access;
- The training that is required before a person accesses the PCEHR, including:
    - How to use the system accurately and responsibly; and
    - The legal obligations on the healthcare organisation and providers using the system and consequences of breaching those obligations (such as, where relevant, civil penalties under the PCEHR Act and/or cancellation, suspension or deactivation of a healthcare organisation's registration);
- The process of identifying a person who accesses the PCEHR;
- The physical and information security measures that must be established and adhered to by the healthcare organisation and people accessing the PCEHR on behalf of the organisation, including:
    - Restricting access to the PCEHR to those persons who require access as part of their duties;
    - Uniquely identifying individuals accessing the PCEHR;
    - Having password and/or other access mechanisms that are sufficiently secure;
    - Closing user accounts when PCEHR access is no longer required by the individual to the PCEHR; and
    - Suspending user accounts when awareness of PCEHR access mechanisms or security is/has been compromised; and
- Security risk mitigation measures to identify, act and report risks to management.

The exact wording of Rule 25 is included in Appendix **D.2** for your easy reference.

There is a provision for "small organisations" that may be relevant to your medical practice, whereby if a requirement is not applicable to the organisation due to its limited size, the organisation's policy need not address that requirement. This is likely to apply to sole practitioners and very small healthcare provider organisations – for example, because there are no other staff that need training. If you feel this provision may apply to your practice, then it would be prudent to seek advice before proceeding on that basis.

The System Operator may also request a copy of a healthcare organisation's written policy, as per Rule 26, which is also included in Appendix **D.2**.

In addition to the above, the Rules include requirements for the management of user login accounts used in your Desktop Software – please see Rule 27 in Appendix **D.2**. You will need to review your practice's current approach to user login account management and make any changes that are necessary to comply with this rule.

To assist medical practices comply with the requirement for written policies related to the eHealth record system[95], it is suggested you contact your Medicare Local, who can provide advice and assistance, including possibly of template policy wording specific for your practice.

The following website provides sample policy templates and other useful information:

Section 5 – Sample eHealth Policies section of
http://www.nehta.gov.au/our-work/implementation-and-adoption/ehealth-registration-support/general-practice-registration-workbook

You may also find useful information in Chapter 7 of the AMA's guide to the eHealth record system regarding protocols for your practice's participation:

https://ama.com.au/ama-guide-using-pcehr

The implementation of these written policies is required **BEFORE** you can apply for registration in the eHealth record system.

5.5.2 Data Recording and Clinical Terminology/Coding

As discussed in Section **3.2.4** above, the main requirement for your practice to implement Clinical Terminology is to have the users of your Desktop Software use the drop-down and check-box type methods for selecting various data options for your patients' records, rather than them entering free text into data entry fields. This would require training for your clinicians and staff, and monitoring to encourage compliance.

This method of data entry is necessary so that the code from the coding system built into your Desktop Software is stored into your patient's record, and, as the software is conformant, that this code will be used in any eHealth-related information sent from your practice, e.g. in a Shared Health Summary to the eHealth record system, and in referrals via SMD, etc. This ensures that the information that is coded in this way can be consistently interpreted by software systems used by other healthcare providers (and the patient via their portal), as they too are conformant to the same specifications.

Written Policy for Clinical Terminology

Medical practices are encouraged to implement a written policy along the lines described above in order to improve the reliability of the data they share. Sample policy wording is available in:

[95] For general practices wanting to access the updated ePIP payments, you should also be aware that written policies are also required for SMD, Clinical Terminology and ETP.

Section 5 – Sample eHealth Policies section of **http://www.nehta.gov.au/our-work/implementation-and-adoption/ehealth-registration-support/general-practice-registration-workbook**

For general practices wishing to access payments from the updated ePIP scheme, the implementation of such a policy is mandatory, as outlined in Requirement 3 – see Section **4.5**.

5.5.3 Secure Message Delivery (SMD)

As introduced in Section **3.2.2** above, implementing SMD in your practice requires that you have a HPI-O that you intend to use for SMD (see Section **5.4**)[96], an SMD conformant Desktop Software product and messaging provider(s), an Endpoint Location Service (ELS) published in the HPD and the NASH PKI certificate for Healthcare Organisations (i.e. the same as required for the eHealth record system).

Choosing SMD Products for Your Practice

If your practice is currently using one or more messaging providers, then you will need to assess whether the providers' messaging services are conformant to the SMD specification and also will operate with your updated Desktop Software product. The following website lists SMD conformant products and service providers:

https://epipregister.nehta.gov.au/registers/secure-message-delivery

All products listed on the above register conform to the required 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 for implementation and configuring, and you will need to decide whether that expertise is needed in house or is provided externally, e.g. via a support contract.

It is recommended that you ask your current or preferred SMD product supplier about the capabilities and options provided by their product and seek advice regarding the configuration that best suits your practice, ***BEFORE you commit to a particular product***. You should also ask if they have established interconnect agreements with other suppliers, since even though the products may be technically compatible, intermediaries will generally require commercial agreements to be in place to exchange messages with other intermediaries.

In most cases, the SMD capability will be provided by a separate product from your Desktop Software (however, there are some exceptions to this). Also in most cases, Desktop Software products use a preferred SMD service provider, but they should be able to be configured to use any SMD conformant service.

[96] If you are proceeding with the Seed HPI-O only configuration, then this will be the HPI-O used for SMD.

Therefore, it is recommended that when you choose one or more SMD products you consider whether and how the product(s) will integrate with your Desktop Software. You should seek advice from both your Desktop Software vendor and your preferred SMD product supplier regarding product compatibility and integration.

Status of SMD Interconnectivity

At the time of writing, the SMD vendor community (in collaboration with NEHTA) were testing the interconnectivity of their products, i.e. along the lines as discussed in Section **3.2.2**. Several vendors have demonstrated live interconnectivity between practices and are in the process of establishing commercial interconnectivity agreements.[97]

Achieving comprehensive secure messaging interconnectivity across the whole healthcare system is obviously desirable – and is the goal. The reality though is that this may take some time as different healthcare organisations are at different stages in implementing clinical information systems that are compliant, and the software and messaging vendors are at different stages of incorporating standards in their products and establishing commercial interconnectivity agreements. The standards too evolve over time to match emerging requirements of the healthcare system.

You are advised to check with your current or prospective SMD vendor regarding their progress towards universal interconnectivity.

Approach to and Prerequisites for Installation and Configuring

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.

In addition to deciding on who will install and configure SMD in your practice, **BEFORE** installing it you will also need to:

- Establish if your SMD vendor requires your practice to have them act as a CSP to access the HI Service (discussed in Section **3.2.1**) on your behalf and undertake actions as advised by them to make this happen;
- Publish and link your practice's HPI-O and clinician's HPI-Is in the HPD;
- Confirm which Endpoint Location Service (ELS) will be used for your practice (in consultation with your Desktop Software and SMD vendors) and have the details on-hand as it will be necessary for this to be published in the HPD for your HPI-O in the HI Service; and

[97] See this NEHTA media release: *Australian eHealth a step closer with successful trial of Secure Message Delivery*, at **http://www.nehta.gov.au/media-centre/news/398-australian-ehealth-a-step-closer-with-successful-trial-of-secure-message-delivery**.

- Apply for and receive a NASH PKI Certificate for Healthcare Provider Organisations for your practice.[98]

Written Policy for Secure Messaging

In order to use secure messaging effectively, medical practices are encouraged to implement a written policy specifically for SMD, covering matters such as:

- How, when and by whom secure messaging is used;
- To whom secure messaging communicates with;
- Maintenance of the secure messaging software; and
- How the use of secure messaging is promoted.

Sample policy wording is available in:

Section 5 – Sample eHealth Policies section of
http://www.nehta.gov.au/our-work/implementation-and-adoption/ehealth-registration-support/general-practice-registration-workbook

For general practices wishing to access payments from the updated ePIP scheme, the implementation of such a policy is mandatory, as outlined in Requirement 2 – see Section **4.5**.

5.5.4 Electronic Transfer of Prescriptions (ETP)

In order to send electronic prescription information to a Prescription Exchange Service (PES – as introduced in Section **3.3.2** above), your practice needs to have an agreement with a PES. At the time of writing there were at least two businesses operating as a PES, with both working with most of the prominent Desktop Software products.

The implementation of electronic sending of prescription information should not introduce any major workflow changes to how you prescribe from your Desktop Software. Conformant products include the ability to send prescription information to a PES and to print the script (i.e. the legal document) with a bar-code that, once scanned, enables most pharmacies to download the electronic copy of the prescription from the PES it was uploaded to for dispensing.[99]

Conformant Desktop Software products typically have a relationship with one PES, i.e. they can only send prescription information to one and only one PES. Some products can be configured so that you can select which PES to use at set up time, but the software will still only work with the PES selected, i.e. it is not possible to select a different PES at the time of writing a prescription. **You will need to check**

[98] Note that it is not necessary for individual clinicians in your practice to have an Individual PKI certificate for SMD use, but you will probably find it beneficial for them to have ones that are necessary for other reasons, e.g. to use the HPOS website and to access the Provider Portal for the eHealth record system.

[99] The software used by dispensers needs to have this capability.

this with your Desktop Software vendor as it may limit your choice in selecting a PES for your practice.

The two PES providers have recently enabled their services to interoperate, i.e. so that a prescription copy can be downloaded by a pharmacy regardless of which PES it was uploaded to.[100]

This current implementation of ETP is described as a Stage 1 design, where the paper prescription remains as the legal document and the ETP functionality supports the existing processes. National ETP specifications that go beyond this, i.e. that include eSignatures and do not require paper (Stage 2), are currently being considered by Standards Australia. Changes to government regulations are also required before prescriptions can be paper-less. In due course, including after the regulatory changes, there will be a requirement for your Desktop Software to be compliant with these Standards Australia specifications. Further information about this and the broader scope of eMedication Management can be found in Appendix **B.4**.

In the meantime this current implementation of ETP can be used to provide your practice and patients with some of the benefits available from electronic prescriptions (see Section **4.3**).

As the current implementation of ETP was developed before the national standards were specified and endorsed, the PKI certificate requirements for prescribers and dispensers are determined by the PES vendors. **You should check with your Desktop Software vendor and PES provider about what PKI certificate is required for ETP to work in your practice.**

The RACGP has very useful information, including a video, about ETP at:

http://www.racgp.org.au/your-practice/e-health/electronic-medication-management/etp

Written Policy for ETP

In order to use it effectively, medical practices are encouraged to implement a written policy specifically for ETP, covering matters such as:

- How, when and by whom ETP is used;
- To whom ETP communicates with;
- Maintenance of ETP; and
- How the use of ETP is promoted.

Sample policy wording is available from the following website:

http://www.racgp.org.au/your-practice/e-health/ehealthrecords/epip/

[100] See the following article for further information on PES interoperability: **http://pulseitmagazine.com.au/index.php?option=com_content&view=article&id=1299**.

5.6 Implementing the eHealth Functionality

When you have considered the options, made the necessary decisions and undertaken the required pre-implementation preparations as outlined in Sections **5.3**, **5.4**, and **5.5** above, you should be ready to carry out the steps outlined below. This will involve in summary:

- Completing and submitting some forms accompanied by necessary documentation, and the receiving of notifications of registrations and PKI certificates; and
- Installing the update to your Desktop Software and configuring it to utilise the eHealth functionality.

The steps outlined in this section assume that you wish to establish a Seed-only HPI-O structure for your practice (as outlined in Section **5.4.3** above). If this is not the case, then it is recommended that you seek advice and assistance from your Medicare Local and/or other organisations that provide you with IT and/or eHealth support.

5.6.1 Application Forms, Registration and PKI Certificates

The following steps outline a suggested sequence for you to follow in order to set your practice up for:

- The HI Service;
- The eHealth record system;
- Secure Message Delivery (SMD); and
- Electronic Transfer of Prescriptions (ETP).[101]

Step 1 HI Service and eHealth Record System

You will need to complete the form *2978 – Application to Register a Seed Organisation* (introduced in Section **5.4.5**) that can be used to apply for both a Seed HPI-O and to register your practice for the eHealth record system[102]. It is available at:

http://www.humanservices.gov.au/hiservice

This form can be used to have your existing Human Services PKI Site certificate (i.e. as used for Medicare Online Business) linked for use in the HI Service, or to

[101] For Clinical Terminology there are no further implementation steps required beyond those outlined in Section **5.5.2**.

[102] If you already have a Seed HPI-O, then you can use HPOS to register for the eHealth record system or complete Part B of this form.

apply for a new PKI certificate of this type if your practice does not have one. In addition, the form allows you to nominate people for the roles of RO and OMO.

You will have already obtained and reviewed this form and assembled all the supporting documentation necessary to accompany its submission, including the signed Participation Agreement for the eHealth record system (per Section **5.5.1**).

You can select the Participation Agreement type that is appropriate for your practice's legal entity from:

http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/providerregistration_participationagreement

The application form includes information about how to contact Human Services if you have any enquiries about completing the form.

Once the form and agreement are completed and signed, they can then be submitted as per the instructions on the application form. It is suggested that you keep a copy of what is submitted and record this action in the Register in your Quality System, i.e. as recommended in Section **5.3**.

Note that it is a prerequisite for your practice to have the written policies discussed in Section **5.5.1.4** above in place and operational, i.e. your practice would be in breach of its registration in the eHealth record system if this was not the case. This includes complying with PCEHR Rule 27 regarding user login account management for your Desktop Software.

Your Seed HPI-O number is required for many of the following actions, so it is best that you wait until you have it along with the other information and outcomes that will come with it before proceeding. In the meantime you may find it useful to read ahead and make any preparations for the following actions that you are able.

When your HPI-O and other related information arrives, be sure to record the details in the Register in your practice's Quality System.

Step 2 *NASH PKI Certificate for eHealth Record System and SMD Use*

A separate form is used to apply for the NASH PKI certificate for Healthcare Provider Organisations that is required for your practice to access the eHealth record system and for it to use SMD. The form to apply for this PKI certificate (*AH2542 – Application to Register a National Authentication Service for Health Public Key Infrastructure Certificate for healthcare provider organisations*) is available at:

http://www.humanservices.gov.au/nash

Your practice needs to be registered with the HI Service, i.e. you'll need your HPI-O, before this form can be completed and submitted. The application form includes information about who to contact if you have any enquiries about completing the form.

Once completed and duly signed, you can submit the form. When the NASH PKI certificate arrives, be sure to record the details in the Register in your practice's Quality System.

Step 3 Fast Track Option

After you have received your practice's HPI-O and the related Human Services PKI certificates (per Step 1) and while you are waiting for the NASH PKI certificate for Healthcare Organisations to arrive (per Step 2), you may optionally consider fast tracking the overall implementation process by undertaking the first or both of the following:

1. Perform Step 5 below, which requires the RO or OMO to perform functions on the Human Services HPOS website using their Human Services Individual PKI certificate.

   This will have the effect of establishing your practice in the HI Service **BEFORE** your Desktop Software is updated, i.e. defining your practice's settings in the HI Service ready for later use.

2. You may then additionally choose to also (i.e. do now or leave until later):

   - Skip ahead to Section **5.6.2** and install the update to your Desktop Software; and

   - Then implement the post-installation actions specifically for the HI Service as outlined in Section **5.7.1**, before resuming the steps outlined below.

   This will have your Desktop Software updated and using the HI Service, and ready to be configured for the eHealth record system and other eHealth functions that you later plan to implement.

Note that you cannot configure your Desktop Software to use the eHealth record system or SMD until the NASH PKI certificate arrives and is installed and configured for use.

If you choose not to perform this optional fast track Step, then you may proceed with the steps outlined below, i.e. the above actions will be performed in later steps.

Step 4 SMD and ETP

If you plan to implement SMD and ETP, then, as discussed in Sections **5.5.3** and **5.5.4** respectively, you will need to ensure your practice:

- Is aware of and accepts the SMD provider that will operate (by default) with your Desktop Software, ***or*** if your software permits it, to purposefully select an alternative messaging provider, if preferred; and
  - Is aware of and accepts the ELS to be used by your practice and has the information at hand that is necessary for your ELS to be published in the HPD for your HPI-O in the HI Service. Your SMD provider would advise and/or assist you in doing this; and
- Is aware of and accepts the ETP provider that will operate (by default) with your Desktop Software, ***or*** if your software permits it, to purposefully select an alternative provider; and
  - Has the information at hand that is necessary to establish this for your practice to use ETP.

In some cases it may be necessary for your practice to enter into a contract with either or both the SMD and ETP provider, and to provide specific information, e.g. the HPI-Is of clinicians. If so, then it is recommended that you review, sign and submit these contracts as required at this stage.

You will have your practice's HPI-O and Human Services PKI certificate details for the HI Service at this stage and, if necessary your clinicians' HPI-Is and other required information from the Register in your practice's Quality System (per guidance provided in Section **5.3**). If either of the providers requires details of your NASH PKI certificate, then you will have to wait until it arrives (per Step 2 above) before completing this step.

Step 5 Establish Your Practice, Clinicians and Authorised Employees (if necessary) in the HI Service

If not already performed per the optional Step 3 above, you can, BEFORE installing the update to your Desktop Software and configuring it for use, undertake the following actions. Note this Step may be performed after installing the software update, if you so prefer.

To perform the actions outlined in this Step, your practice's RO or OMO will require their Human Services Individual PKI certificate as they will be logging onto the Human Services HPOS website. The association between the RO and OMO roles and your practice's HPI-O will have already been established in the HI Service through the processing of the application form (from Step 1), and the Human Services individual PKI certificates for these people will have already been set to allow them to access the HI Service.

You may find it beneficial to review Sections **5.4.6** and **5.4.7** above for an overview on setting up the links between your practice's HPI-O and:

- Clinicians' HPI-Is; and
- Authorised Employees (if necessary). The website for creating and maintaining the list of Authorised Employees in the HI Service is

  http://www.medicareaustralia.gov.au/hpos/online-user-guides/hi/hi-services-authorised-employees.jsp

The Human Services website includes an online user guide that describes these and other functions, such as publishing your HPI-O in the HPD, which can be performed in HPOS for the HI Service, which is available at:

http://www.medicareaustralia.gov.au/hpos/online-user-guides/hi/

You may find it useful to have the above website open in a separate window on your computer to refer to as you use Human Services's HPOS website, which is at:

http://www.medicareaustralia.gov.au/hpos/

5.6.2 Install the Update to your Desktop Software

If you have followed the advice and steps outlined in this guide so far, then you should be in good shape to plan and undertake the next step of installing the update to your Desktop Software that includes the eHealth functionality that you wish to implement for your practice.

Updating any software can be complex and prone to errors and unintended outcomes, if not planned and implemented expertly.

Problems may be caused from any or all of the following, or more:

- Technical aspects of the installation process itself (including not following the steps in your Desktop Software vendor's installation manual);
- Mismatched or not-updated business processes that use or depend upon functions in the software; and
- User errors from lack of training, documentation or support, or errors in these.

If you normally and successfully install updates to your Desktop Software yourself, then you should assess if this update is more complex than previous ones you have undertaken and consider if it is safe to perform the update as you have done in the past – even if with some extra attention to detail and care.

This User Guide's recommendation is that you do seek expert advice and assistance with this update as it contains many changes that have implications and consequences beyond what could be considered a "normal" update. This is especially the case if your practice is new to eHealth and has had little or no experience in sharing information electronically outside of the practice.

To inform you and to assist organisations that provide medical practices with advice and support for eHealth implementations, a number of useful resources are available and recommended:

- Making Sense of eHealth Collaboration – A guide to getting started, available at:

  http://www.nehta.gov.au/our-work/implementation-and-adoption/ehealth-sites/resources

  This guide is designed to act as a common starting point and as a useful reference during an eHealth project for the implementation team, clinical and business leads and interested parties from acute and primary care. It does not provide detailed technical or step-by-step guidance on specific eHealth IT solutions; however, links to documentation that offers this level of support are provided. The primary focus of the guide is for eHealth implementations that involve collaboration between different organisations.

  It includes best practice information for planning and implementing eHealth projects.

- Commissioning Requirements for Secure Message Delivery[103]

  http://pip.nehta.gov.au/pip-implementation-overviews > Secure Messaging Capability > Additional Reference Material[104]

  This document defines the commissioning requirements for installation, configuration and operation of SMD products. The document is written for general practices and references the updated ePIP requirements, but is applicable for medical practices wishing to implement SMD.

  It has two main sections, each with a different audience and purpose:

  - Section 2 is intended to help a practice verify that its secure messaging product has been installed and configured correctly. and does not require detailed knowledge of the SMD specification; and
  - Section 3 is intended for commissioning agents – the parties who will install and configure an SMD product for use by a 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. Practices with the necessary in-house IT support may wish to undertake the work themselves.

- Go Live Readiness Checklist

  See **Appendix E:**

  This checklist has been adapted from training material provided by NEHTA to Medicare Locals to assist them in supporting eHealth record system adoption in general practices. You may use it as is or adapt it for use in your medical practice. It broadly covers the following areas of Go Live readiness:

  - Organisation readiness
  - Application readiness
  - User readiness
  - Consumer readiness
  - Go Live day support activities
  - Authorisation processes

Providing advice and guidance in this area of expertly planning and implementing an eHealth project, which this Desktop Software update essentially is, is beyond the

[103] At the time of writing this type of document was only available for SMD. There may be similar documents created for other eHealth services and solutions, so be sure to search the website to see if there are others.

[104] The document may alternatively be downloaded directly from: **http://pip.nehta.gov.au/component/docman/doc_download/74-pip-smd-commissioning-requirements-**.

scope of this User Guide. There are many methodologies, checklists, etc. that can be utilised, but they all depend on the application of expertise and experience to obtain a successful outcome. So please **don't risk your practice's eHealth implementation (and potentially your whole IT environment) by underestimating the value of expert advice and assistance**.

You can see from the above information and referenced resources that this is not just about installing the software update. There are many other things that need to be considered and actioned before, during and after the act of performing the update itself.

Remember too that the software update is likely to include other changes to your Desktop Software, i.e. in addition to the eHealth functionality. You should review the Release Notes to see what else, if anything, has changed and be sure that your update and testing plan also incorporates these changes.

When you are confident that you have completed all the prerequisites (including planned the post-installation actions – see next section), your practice (the organisation, clinicians and staff) is prepared, and you have enlisted the assistance of appropriate expertise, then you could proceed with the update.

The documentation that came with the software update will outline how you should go about doing this for the particular Desktop Software product that you use. If you have any questions or concerns regarding installing the update, then be sure to also contact the vendor of the product. As each product is different, this User Guide does not provide product-specific guidance.

5.7 Post-Installation Actions

When the installation of the update has been successfully completed, including the installation and configuring of the necessary PKI certificates, then there are a number of post-installation actions that need to be done before the eHealth features can be used in your practice. The actions outlined in this section should be completed **BEFORE**:

- The steps outlined in Chapter **6** are performed to verify that the eHealth features operate correctly in your practice; and
- The eHealth features are used in actual practice, i.e. by clinicians and staff in their dealings with patients.

Now is also a good time to ensure that the non-technical implementation requirements have also been undertaken, which include:

- That your practice has implemented the requirements for written policies as outlined in Section **5.5**, including the training of clinicians and staff; and
- That PCEHR Rule 27 relating to user login account management has been implemented.

5.7.1 Healthcare Identifiers

Now that you have established the roles of RO, OMO(s) and authorised employees (if applicable), your practice's HPI-O and the links to it in the HI Service for your clinicians and nominated staff, and implemented the update to your Desktop Software that includes the HI functionality and configured it correctly, there are a number of things that it is suggested you then do:

- Firstly, your updated Desktop Software will most likely have a feature to record a clinician's HPI-I with their user profile or address book entry. This may need to be manually typed in. The HPI-I needs to be stored this way as it is needed for clinicians to perform eHealth functions that require access to the HI Service, which is something they will all do.

- Secondly, you'll need to decide on an approach to adding patient IHIs to your practice's patient records system by downloading them from the HI Service. This is discussed in the following sections.

In addition, if not already done in your practice, you should now consider:

- Designing an approach and commence reviewing and improving the quality of the data stored in your systems about your patients. This should be done generally as part of good clinical practice, and importantly also in preparation for your practice's participation in eHealth – as discussed in Section **5.2** above; and

- Implementing and/or participating in a clinical governance arrangement that can enhance your practice's ability to deal with clinical safety risks and data governance, and importantly "connect" your practice more effectively with other healthcare providers involved in your patient's care – as discussed in Section **5.1** above.

5.7.1.1 Adding IHIs to Patient Records

When the steps outlined thus far are complete and your software is configured to suit, you will be able to commence downloading your patients' IHIs from the HI Service and having them stored in your Desktop Software's database. However, before you do this it is suggested that you review and where needed correct data stored in your practice information systems. Particular focus on data related to patient demographics is suggested.[105]

Data cleansing of patient identification information held in your systems should be undertaken on a regular basis in order to ensure a more accurate match with data held in the HI Service.

[105] See Section **5.2.3** for information about the CDSA Tool that can assist with this process.

When an attempt to download an IHI is made in your Desktop Software, the software and the HI Service compares some or all of the following data fields, depending on the search performed:

- Surname (mandatory)
- Date of Birth (mandatory)
- Gender (mandatory)
- Given Name
- Medicare or DVA number
- Address

Note: the items marked as mandatory must be present in your system to conduct an IHI search. The others are optional, however at least additionally using the patient's Medicare or DVA number will result in improved match results.

It is essential that data in your practice information system matches **exactly** with data on the patient's Medicare card and in the HI Service. If there is an error on even one item, then the attempt to download the IHI will fail. The HI Service is purposely designed to notify only that the attempt has failed and not to advise of which data fields are correct and which are incorrect. This feature is present to prevent fraudulent searching of IHIs, e.g. to address concerns of identity theft.

If present, you will also need to resolve duplicate records for the same patient before attempting to match records with the HI Service. Your Desktop Software should indicate to you if duplicate patient records exist and not allow the allocation of the same IHI to more than one record, or more than one IHI to the same person. This is a mandatory requirement of conformant software.[106]

Some common issues that have been identified through initial use at a number of locations include failures to match with IHI records as a consequence of errors in the patient's:

- Medicare number and IRN or DVA number;
- Surname and/or Given name(s), including, for example, the inclusion of multiple names (or initials) in data fields intended to have only single names;
- Address, e.g. including mixing up street and postal addresses;
- Date of birth; and
- Gender.

By improving patient identification data stored in your Desktop Software system staff can increase match rates when searching for patients' IHIs and the associated data in the HI Service. It has been observed that more recent patient information (for example, less than 2 years old) will result in greater likelihood of a match.

It is possible that a patient's data held in the HI Service may be out of date or incorrect, for example if they have changed address, in which case you can advise your patient to update their Medicare details via myGov[107] or with a Medicare Service Centre.

[106] The CDSA Tool introduced in Section **5.2.3** can be used to resolve duplicate patient records, i.e. before IHI downloading is attempted.

[107] **http://my.gov.au** – the preferred portal for users to access online Government services.

If it is not possible to download a patient's IHI, then this does not affect in anyway their ability to receive care or anything related to their payment arrangements. It means though that your practice won't be able to include the eHealth record system in the care you provide them until the data is corrected.

Online Patient Verification (OPV) and IHI Searching

As part of attempting to verify patient identification information, your practice may use the OPV feature in your Desktop Software or via the HPOS website. It is important to be aware that there are different legislative constraints on the search functionality available for OPV for Medicare numbers and searching for an IHI in the HI Service.

The HI Act 2010 provides the legislative framework governing the search requirements for returning an exact IHI match in the HI Service. This stringent framework does not apply to OPV searches and as a consequence whilst a demographic search for a patient's Medicare number may return a positive result even when one of the data elements does not match, use of the same demographic data plus the Medicare number will not return an IHI. In these circumstances healthcare organisations will need to revalidate the demographic data with the patient or alternatively the patient should directly contact Medicare.

The Status of IHIs

Your Desktop Software product also now includes data fields related to your patients' IHI's Status, which it will keep up to date once the IHI is correctly downloaded and regularly validated. An IHI's number status will be one of the following:

> **Verified IHI** – When an IHI has a verified status it means the HI Service Operator (Human Services) has seen evidence of an individual's identity, such as a passport, birth certificate or driver's licence. When a person enrols in the Medicare program or registers with the Department of Veterans' Affairs, Human Services automatically allocates them a verified IHI if an unverified IHI does not exist.
>
> **Unverified IHI** – When an IHI has an unverified status, it means the healthcare identifier was created for an individual at a healthcare facility, such as a hospital, and Human Services hasn't been provided with evidence of their identity, or the individual's IHI could not be accessed or located.
>
> **Provisional IHI** – When an IHI has a provisional status it means the identifier was created at a healthcare facility when the patient was unable to identify themselves (for example, they were unconscious). Provisional IHIs are temporary and expire after 90 days of no activity. If the individual does have a verified IHI, then the provisional IHI can be merged with this once the individual or a family member is able to provide information about the individual's identity.

Note that your Desktop Software would likely only save Verified IHIs into its database. You should check this in the product's documentation. At the time of writing it is understood that the Unverified and Provisional settings (as above) are not implemented in Desktop Software, but they may be at a later time.

In addition to the status of the IHI *number* (as above), the HI Service also maintains status information of the consumer's IHI *record*, as described below:

Active – an IHI is active when it does not have a date of death on the record, and the age is not greater than 130 years.

Deceased – an IHI is deceased when there is a date of death present on the record but it has not yet been matched with Fact of Death Data (FoDD) from Births, Deaths and Marriages Registries and age is not greater than 130 years.

Retired – an IHI is retired when there is a date of death present on the record and it has been matched with FoDD or has reached an age of 130 years (verified IHI records only).

Expired – an IHI is expired where it is provisional and there has been no activity on the record for 90 days, or where it is unverified and has reached an age of 130 years.

Resolved – an IHI is resolved when it has been linked with another record as part of resolving a provisional record or resolving a duplicate record, or end dated as part of the replica resolution process.

5.7.1.2 Options for Downloading Patient IHIs

In terms of downloading IHIs into your system and keeping patient data up to date, there are a number of options available to you (depending on the functionality included in your Desktop Software). These are outlined below, and are not mutually exclusive:

- When a patient (existing or new) presents at your practice you may find it effective to have your reception staff, as part of the current process of verifying basic demographics, to also see if an IHI is present in their patient record. If one is not recorded the reception staff could initiate an IHI search, which your Desktop Software will be able to do.

  Note that all staff who you wish to be able to perform searches and maintain IHI-related data via your Desktop Software, e.g. those at reception, will need to be established by your practice as Authorised Employees, as discussed in Section **5.4.7** and **Step 5** in Section **5.6.1**. Clinical staff, e.g. a practice nurse, will need their HPI-I set up to do this.

  If the software reports a match, then the IHI will be added to your patient's record.

  If the software does not report a match, it is possible that the data in your system and/or the HI Service is incorrect (see list of common matching errors above). This will need to be resolved before the patient's IHI can be downloaded, which may require the patient attending a Human Services shop-front.

- It is possible that your Desktop Software has a feature for bulk downloading or for bulk verifying of patient IHIs. This functionality could be used as an initial step to load IHIs and also on a regular ongoing basis to check for data changes.

  Please see your Desktop Software documentation for how these features work and how to set them up if this method is of interest.

- It is probable too that your Desktop Software will allow IHIs to be directly typed in, e.g. in cases where the patient has their IHI on a letter or other official document. In these cases, the software will attempt to validate the IHI with the HI Service and will advise the user of the result. If the IHI provided by the patient is reported as being not valid by the HI Service, your Desktop Software will not store it in its database.

  The same types of matching checks as discussed above are also carried out for this approach, so it is essential that data in your system matches data in the HI Service.

You should be aware that consumers are able to view activity related to their IHI, including when it is downloaded, through an audit log that is available when they are logged into their eHealth record on the system's portal.

Having IHIs in your patient records and keeping them maintained will enable your practice to fully participate in the national eHealth environment, including the eHealth record system, as further functionality is implemented and made available to your practice through updates to your Desktop Software.

5.7.2 eHealth Record System (further considerations)

When the update to your Desktop Software that includes the functionality to access the eHealth record system has been installed and correctly configured, and all the other prerequisite actions previously outlined have been completed (including policies and training), it is recommended that the following be done:

- Set your clinicians up to be able to access the eHealth record system via the Provider Portal, if your practice desires this additional form of access to patient records; and
- Set your practice up to provide its patients with assistance in establishing their own eHealth record by using the feature in your Desktop Software or installing the Assisted Registration Tool.

These set up actions can be performed before or after verifying that the eHealth record system operates correctly through your Desktop Software – per Section **6.3**.

5.7.2.1 Setting Up Provider Portal Access for your Clinicians

While not mandatory, it is recommended that your clinicians be set up so that they can access the eHealth record system via the system's Provider Portal. This form of access is performed through a web-browser and not through your practice's Desktop Software, which means it is available from anywhere that your clinicians can access the internet with a web-browser.

The Provider Portal is currently a read-only service, which means that clinicians will not be able to use it to upload documents to patients' eHealth records or modify them. This can only be done from conformant clinical systems, like your Desktop Software.[108]

The following steps are necessary to enable your clinicians to use the Provider Portal:

1. They and your practice need to be registered with the HI Service, and your practice needs to be registered with the eHealth record system. Both of these should be already set up if the approach outlined in this guide has been followed;

2. They need to have an NASH PKI Certificate for Individual Healthcare Providers. The form to apply for this, which needs to be signed by the clinician, is available at:

   http://www.humanservices.gov.au/nash

   When the application is accepted, the clinician will receive the requested PKI certificate in the form of a USB token or Smart Card; and

3. The practice's RO or an OMO needs to establish a list of Authorisation Links, which creates an authorised association between your practice's HPI-O and their HPI-I(s). This effectively allows these listed clinicians to access the eHealth record system provider portal on behalf of your practice.

   This can be done over the phone by your RO or an OMO calling the System Operator on 1800 723 471, or by using the form available at the bottom of the following web-page:

   http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/providerregistration_eBooklet

   When the process is complete, your practice's RO will receive confirmation from the System Operator. Your practice's list of authorised individual healthcare professionals must always be kept up to date. Changes can be notified to the System Operator by calling 1800 723 471 or using the above form.

5.7.2.2 Setting Up for Assisted Registration

For your practice and patients to receive the benefits from the eHealth record system both need to be registered with and actively use the system. By following the approach outlined in this guide your practice will be set up and able to use it effectively. But this will not be beneficial unless your patients are also registered for their eHealth record.

While it is voluntary to assist your patients to register for an eHealth record, as a post-installation activity you may consider setting your practice up so that

[108] It is anticipated that future updates to the Provider Portal may introduce the ability for an authorised healthcare provider to write information to a consumer's eHealth record.

appropriately authorised and trained staff can assist patients with the registration process at your practice when they visit for a consultation.

To offer assisted registration your practice must have a HPI-O and be registered to participate in the eHealth record system. You can offer assisted registration to a person who is 14 years or older. You cannot offer assisted registration to any adult who does not have capacity or who is acting on behalf of an adult in their care.

It is likely that your Desktop Software has the Assisted Consumer Registration (ACR) functionality built into it. If not, there is a software tool that can be downloaded and used by your practice.

Information about Assisted Registration, including the pre-requisites to offer it as a service to your patients, the downloadable software tool (if needed), and a detailed step by step process for establishing it for your practice is available at:

http://ehealth.gov.au/internet/ehealth/publishing.nsf/content/assistedregguide

Once this capability has been established, you may consider how your practice could utilise it to the best effect. For example, you could ask patients who don't have an eHealth record when they present if they would like to have your practice assist them in registering for theirs, or you may consider notifying patients, e.g. via your practice newsletter or with a specific mail-out, that your practice has the ability to assist in their registration for when they next visit.

This and other ideas to promote your practice's eHealth capabilities are discussed later.

Written Policies and Other Requirements

As a registered healthcare provider organisation your practice must comply with the PCEHR Rules. Organisations that choose to provide assisted registration must also comply with the PCEHR (Assisted Registration) Rules 2012, which are available at:

http://www.comlaw.gov.au/Details/F2013C00314

The Rules include the requirement to develop and implement assisted registration policies for your practice. At the time of writing sample policy templates were not available. You may find it helpful to ask your Medicare Local if they can assist with this requirement.

5.7.3 Clinical Terminology, SMD and ETP

These three eHealth features do not require any additional implementation steps beyond those already outlined in the sections above, viz:

- Data Recording and Clinical Terminology/Coding – see Section **5.5.2**;
- SMD – see Section **5.5.3** and **Step 4** in Section **5.6.1**; and
- ETP – see Section **5.5.4** and **Step 4** in Section **5.6.1**.

6 Verifying Correct Operation

This chapter outlines steps you may consider taking to verify that the eHealth functionality you have implemented operates as intended in your practice. While the update to your Desktop Software is unlikely to contain faults in the newly included eHealth functionality (due to the conformance testing process – discussed below), it is still prudent to verify that these features operate correctly in your practice's computer environment. [109]

A challenge for medical practices to verify the correct operation of the implemented eHealth features is that there currently is not a specific *test* environment for end-user healthcare organisations, i.e. where you can test the connectivity of your Desktop Software with the eHealth system[110]. There is only the *live* (or production) environment, and the Healthcare Identifiers and PCEHR legislation specifies that these eHealth systems may only be used for the purposes of healthcare. This is good in that it means the live environment should not contain test data that may interfere with actual usage, but it limits the extent of actions that could be undertaken to verify that the systems operate correctly after installation and configuration.[111]

Despite this limitation, this User Guide suggests actions in the sections that follow that, if successfully completed, should give you confidence that your practice's Desktop Software is configured correctly to interact with the national eHealth system.

The chapter that follows this chapter includes some ideas that you may consider adopting in your practice to assist it achieve the benefits that you should reasonably expect from the *use* of the eHealth features.

6.1 Conformance Testing Process

All the new eHealth features as they are developed and released by software suppliers are put through a rigorous conformance testing process to ensure the software is clinically safe. This includes the current updated version of your conformant Desktop Software and any subsequent updates that also pass the testing process.

Healthcare providers investing in clinical information software systems need confidence that the products they choose are able to safely and reliably operate

[109] The software update is most likely to also include other new, enhanced and/or corrected features, i.e. in addition to the new eHealth functionality, which you should consider also testing and verifying by whatever means you feel is appropriate.

[110] It is understood that such a facility is being worked on and should be available in due course.

[111] Test environments do exist for software vendors to use as part of their product development, but these environments are not accessible for end-user organisations such as your practice. The lack of a test environment for end-user organisations is a known issue that is being considered by NEHTA, Human Services and Department of Health.

within Australia's eHealth system. The national Compliance, Conformance and Accreditation (CCA) program is a key part of a national framework designed to assure that eHealth products and services comply with Australian specifications and demonstrate appropriate standards of interoperability, security and clinical safety in the way they handle and exchange information. [112]

Information about the CCA program is available at: **http://ehealthcca.com.au/**

Information specifically about software conformance as it relates to the HI Service, SMD, Clinical Terminology, ETP and the eHealth record system is available at:

http://pip.nehta.gov.au/software-vendors

NEHTA manages, on behalf of The Department of Health, the *eHealth Register of Conformity*, which provides information on health software systems and organisations that meet national eHealth standards and specifications. See:

http://www.nehta.gov.au/our-work/ehealth-register-of-conformity

By way of example, a summary of what's happened to make it possible for the Healthcare Identifiers functionality to be included in your Desktop Software is outlined below.

- The HI Service has undergone extensive consultation throughout the design, development and implementation stages to ensure clinical safety risks are minimised. Consultation has involved representatives from across the health sector, the vendor community, and government agencies. Representatives have provided feedback on privacy, policy and the legislative framework, functionality, integration and usability. In addition, the HI Service has been designed and built to Australian Standards;

- The software vendors have had to pass Notice of Connection (NOC) testing with Human Services (as the HI Service Operator) and a CCA testing process with a NATA accredited testing laboratory[113] in order for their products to be permitted to electronically connect to the HI Service;

- The specifications for incorporating the HI Service into Desktop Software have been developed and finalised through extensive consultation, review, testing and sign-off;

- The Desktop Software vendors, Human Services and NEHTA have participated in a collaborative approach to have the products comply to those specifications; and

[112] The CCA Program's approach to conformity assessment is based on international and Australian standards including the ISO/IEC 17000 series for conformity assessment and other key standards such as IEC 80001 and ISO 31000, ISO/IEC 31010 series (risk management standards); ISO/IEC 27001 and ISO 27799 (information security); and ISO/IEC 20000 (IT service management).

[113] This testing has been conducted by testing laboratories that have been accredited by the National Association of Testing Authorities (NATA) specifically to perform HI and SMD testing. These laboratories are independent organisations that understand the risks associated with incorrect use of healthcare identifiers and perform tests to reduce these risks.

- In addition, the vendors own internal software quality assurance methodologies have been applied as part of their normal product development.

Similar processes are followed for the other eHealth features incorporated into clinical information systems.

The sections that follow outline steps you may consider undertaking to verify the correct operation of the HI Service and other eHealth functionality that you may have implemented through following the steps outlined earlier in this User Guide.

6.2 Healthcare Identifiers

To a large extent the HI functionality in your Desktop Software is intended to operate as a supporting function to the eHealth features that will be used more centrally in your clinical practice, e.g. eReferrals, eHealth records, etc. Hence the approach to verification is fairly straight forward.

To proceed with the verification approach suggested in this guide, the person logged into your practice's Desktop Software will need to either:

- Have a HPI-I and be registered with the HI Service, or
- Be established by your practice as an Authorised Employee.

Suggested steps include:

1. In your Desktop Software, ensure that your practice's HPI-O is recorded accurately.
2. Select and view a patient record that:
   - Does not have an IHI recorded against it, and
   - Has been recently used in an electronic transaction with Human Services,[114]
3. Check that data entered in the following fields appears to be valid:
   - Medicare Card number or DVA number
   - Surname
   - Given Name
   - Date of Birth
   - Gender
   - Address

[114] Note that it is not necessary to obtain your patient's consent to download their IHI into your Desktop Software, and it is not essential that they have their eHealth record established.

4. Use the function in your Desktop Software to request the patient’s IHI.
5. If the software reports the result as successful:
    - Check that the patient’s IHI data field contains 16 digits and that the IHI Status fields show the IHI as being “verified”.
6. If the result is not successful, there may be a number of reasons why an exact match is not possible:
    - The practice may need to review the data it holds to determine currency (e.g. patient change of name) and accuracy (e.g. date of birth is recorded correctly). This can be checked with the patient at their next visit and updates made to the data in your Desktop Software.
    - The patient may not have renewed their current details with Human Services. It would be helpful to advise the patient to contact Human Services to have their data checked and updated.
    - You may need to check that the practice software has been correctly installed.

When you have successfully downloaded a patient’s IHI into your Desktop Software system, you can be confident that your software can interact with the HI Service as intended.

Establishing that the HI Service operates correctly in your practice’s Desktop Software is a significant accomplishment and indicates that the key foundations required for most other eHealth functionality are present and ready to support their use. Steps that you may consider undertaking to verify the operation of these other functions are outlined in the sections that follow.

6.3 The eHealth Record System

Having established that the HI Service operates correctly in your practice, you may next consider verifying that the eHealth record system operates as intended.

As mentioned above there is no specific eHealth test environment with which you could connect your Desktop Software to check the new functions that came in the update to your software. Hence, when installed and configured correctly your Desktop Software is connected to the live environment, i.e. for real data and real patients.

An approach used by some practices that were early eHealth record system implementers, is to access the eHealth record of a clinician or staff member in the practice, who is also a patient and, importantly as part of a consultation, to create and upload a Shared Health Summary (or an Event Summary) to their record. You may consider using this approach where the clinician or staff member is a patient of your practice, it is done in a proper consultation, and where all other requirements, including of the PCEHR Rules, are adhered to.

It is a violation of the PCEHR legislation to use the eHealth record system for anything other than supporting the provision of healthcare, so it is important that the use your practice makes with the system in verifying its operation complies with this. This User Guide does not suggest or recommend you use the system in any way that violates the legislation.

When you have successfully created and uploaded a Shared Health Summary (or an Event Summary) from your Desktop Software to the eHealth record system you can be confident that the functionality operates as intended for your practice.

The processes to verify the correct operation of the other eHealth features discussed in this User Guide (i.e. Clinical Terminology, SMD and ETP) are also largely subject to the limitations discussed above, i.e. as related to the HI Service and the eHealth record system. The following sections describe the status for each.

6.4 Data Recording and Clinical Terminology/Coding

There is no suggested verification process specifically for clinical terminology as it operates in an embedded way with the other eHealth functions, e.g. the data contained in Shared Health Summaries (SHS) and other clinical documents is coded by conformant clinical software products, such as your Desktop Software, and also interpreted by them.

If your practice has followed the guidance offered in this document, i.e. related to improving data quality and not entering key clinical data into free text fields, then the data that is copied to eHealth documents such as a SHS from your Desktop Software should be accurate and suitable for sharing.

It is required though that the clinician who creates a SHS (or other clinical document) checks its contents and reviews it with the patient before it is uploaded to the eHealth record system. The process of observing this data and comparing it to what is stored in the patient's record in the practice's Desktop Software is in effect a verification step.

If there is a mismatch between the two, then it is likely that clinical data for the patient in the Desktop Software is not properly recorded. This should be corrected before recreating the eHealth document, and certainly before uploading or sending it. If this does not correct the mismatch, then it is recommended that you do not upload the document and you contact the vendor of your Desktop Software.

6.5 Secure Message Delivery (SMD)

As discussed in Section **5.5.3** interconnectivity between all or most providers of SMD products was (at the time of writing) not available, but is being worked on.

If your SMD provider does support interconnectivity then that is good, but it is possible that the SMD providers of other healthcare providers to which you wish to send a secure message (or receive one from) do not. Unless you know for certain that the other's provider is conformant, then it is not possible to suggest an approach specifically to verify the correct operation of SMD in your practice.

If you are aware of another healthcare provider who does use a conformant SMD product, then when the next opportunity arises with a patient where it is clinically necessary to send them a secure message, e.g. a referral, then this may be a way to verify that sending via SMD in your practice operates as intended. Of course the full functionality of SMD can only be verified when your practice also receives a secure message from another healthcare organisation also using a conformant SMD product.

It may also be possible that your SMD provider has a test environment with which you could send and receive secure test messages. You could ask if they have such a capability.

It is anticipated that Release 3 of this User Guide will include a more comprehensive approach.

6.6 Electronic Transfer of Prescriptions (ETP)

As suggested above for verifying the correct operation of the eHealth record system in your practice (Section **6.3**), you may consider a similar approach for ETP, i.e. create a prescription for a clinician or staff member who is also a patient of your practice, as part of a consultation, and send the prescription information electronically to your practice's PES.

If the clinician or staff member, in their role as a patient, is able to successfully obtain the medication from a pharmacy that downloads the prescription information from a PES, then you can be confident that ETP works as intended in your practice's Desktop Software.

6.7 Achieving Meaningful Use

The benefits to your practice from implementing the eHealth features in the updated version of your Desktop Software, as outlined in this User Guide, relate mainly to:

- Enhancing clinical governance arrangements and your practice's approach to quality improvement;
- Establishing the essential foundations, in terms of staff roles, work processes, data quality and initial eHealth technologies that will enable your practice to commence achieving the expected benefits; and
- Providing your patients with improved care through being able to share essential information, e.g. via Shared Health Summaries, with other providers and therefore making information about their medicines, allergies, etc. available to a broader audience in the patient's care pathway.

Further eHealth features will utilise what you have now implemented and enable you to conduct a wide range of clinically meaningful transactions more efficiently, more accurately and more safely. Importantly the national eHealth system will assist with “closing the loop” on many, e.g. for referrals with specialist letters and for matching prescriptions with dispensing records.

This User Guide will continue to be updated to cover the expanded scope of eHealth functionality expected to be available in updates to your Desktop Software, including via on online web version. Please check the guide’s web-page for the latest information:

http://www.nehta.gov.au/eHealth-Clinicians-User-Guide

7 Using eHealth Effectively

It is not sufficient to just install the update to your Desktop Software in order for your practice to gain the maximum possible value from the eHealth functionality it provides access to. Through following this User Guide, your practice is now eHealth capable and on the eHealth journey, so it makes sense to do all you can to exploit it to the benefit of your patients and practice. In support of this goal, this chapter presents a range of actions for you to consider that are intended to:

- Promote your practice as being eHealth-capable and connect it with other healthcare providers who also advocate eHealth for the benefits of their patients;
- Engage with your patient community about eHealth and encourage them to sign-up and use its features to increase their involvement in their own care; and
- Ensure your practice's clinicians and staff maintain a high awareness in eHealth and increase their effectiveness in using it in their interactions with patients and other healthcare providers.

In addition, this chapter includes a Section that outlines what to do if you become aware of any clinical incidents that arise from the use of eHealth in your practice.

7.1 Promote Your Practice as Being eHealth Capable

From following the suggestions in this User Guide, your practice will have:

- A clinical governance arrangement in place that includes eHealth as a key enabling capability (for, amongst other things, managing risk and improving quality), and your practice-level arrangement is connected with your Medicare Local's clinical governance (see Sections **5.1** and **5.2**);
- Access to the eHealth functionality described in Chapter **3** (that your Desktop Software supports);
- Consider implementing Assisted Registration for the eHealth record system (see Section **5.7.2.2**) and potentially have a nurse[115] or other staff member trained and able to talk with patients about having an eHealth record; and
- Your practice and clinicians (with their consent) information published in the HPD and other key directories for eHealth (see Section **3.2.1**).

This is a significant accomplishment. Your practice is now positioned take advantage of this new capability and to achieve the potential that eHealth promises.

[115] For eligible practices, the Practice Nurse Incentive Program (PNIP –discussed in Section **4.5**) may provide funding for such a role.

Some Ideas to Consider

Some practices that were early implementers of eHealth have found it beneficial to undertake a range of actions to promote eHealth and their practice. For your practice, you could consider the following:

- Include regular articles in your practice newsletter and website[116] about eHealth, e.g. how you've implemented it and what it could mean for your patients;

- Create a mail-out campaign sending letters to patients who may benefit from eHealth inviting them to come to the practice and ask about eHealth at their next appointment;

- Contact other healthcare providers that you often communicate with and let them know that your practice is now eHealth capable and that you prefer electronic communications, e.g. via an email-out; and

- Be interviewed or submit a story to your local newspaper about eHealth and how it works in your practice.

Some Medicare Locals have provided advice and assistance to practices in their areas with the above types of actions, including, for example, providing letter templates and assistance with mail-merge for patient mail-outs. Your Medicare Local may be able to assist your practice similarly.

In addition to the above ideas, for when patients are present at your practice, you may consider:

- Having posters and flyers available in the waiting area for patients to read;
    - You may also consider making it clear in this type of material that it is your practice's preference to use the eHealth record system as part of the way the practice provides care;

- When a patient arrives at the reception and it is noticed in your software that they don't have an eHealth record, ask if they would like some information or have someone talk with them about it; and
    - If the answer is yes, then you may also offer to assist them to register for their eHealth record using the Assisted Registration process; and

- Having clinicians and staff, including of any clinics or other services associated with or collocated with your practice, e.g. pharmacy, pathology, etc., talk with patients about eHealth and why it is beneficial to them and the practice.

The last point above would be supported through regular discussions and updates on eHealth at staff meetings.

[116] You may also consider putting an eHealth record system "badge" on your website. Details of how to, etc., are available at: **http://www.health.gov.au/internet/main/publishing.nsf/Content/eHealthBadges**.

You may also find it beneficial to measure and report on the level of eHealth record take-up by your patients and to evaluate the impact it has on a range of measures, e.g. patient satisfaction, treatment conformance, etc. as part of your practice's Quality System.

Medicare Locals are able to supply practices with a range of brochures, flyers, templates, etc., such as those available at the website below:

http://www.amlalliance.com.au/medicare-local-support/ehealth/ehealth-brochure-orders

In addition, a range of brochures and other materials can be downloaded and ordered from:

http://www.nehta.gov.au/media-centre/nehta-publications/brochures

7.2 User Checklists for eHealth

The following checklists are provided to assist clinicians and practice staff remember the key things that need to be done in relation to using eHealth in their day to day activities, assuming it has been all set up and verified as outlined in this User Guide.

7.2.1 For Front-Desk and Practice Administration Roles

Patient Contact Information and their IHI

- ☐ 1. To interact with the HI Service for managing patient identification information, you need have a registered HPI-I or be an Authorised Employee.
    - Note that searching for an IHI should only be done when required as part of providing healthcare, and that an audit record is stored of HI Service uses.
- ☐ 2. As part of reviewing a new or existing patient's demographic and Medicare details in your Desktop Software:
    - ☐ 2.1 If an IHI exists in their record, then proceed to your next normal step in the process you are performing.
    - ☐ 2.2 Otherwise check:
        i. That the Medicare/DVA card number is correct
        ii. That the Surname and Given Name(s) are the same as on the Medicare/DVA card
        iii. Date of Birth
        iv. Gender
        v. Address
    - ☐ 2.3 When this data is entered, use the feature in your Desktop Software to download the patient's IHI.

☐ 2.4 If this is successful, then proceed to your next normal step in the process you are performing.

☐ 2.5 Otherwise:

i. There is a mismatch of the above data between what the patient has advised and what is stored in the HI Service.

ii. The patient will need to contact Human Services to resolve the error(s). They should try and correct their data through calling Human Services or through its online services. Depending on the error, they may need to go to a Human Services shop-front.

iii. The patient's visit with the Doctor can proceed without any limitation, except that some eHealth activities cannot be conducted.

Changes in Organisation and Staff

- The OMO in your practice is required to maintain records in the HI Service for:
    - The practice organisation (HPI-O)
    - Links with clinicians' HPI-Is
    - The Healthcare Provider Directory (HPD)[117]
    - Authorised Employees (if necessary).
- When any such information changes, you need to advise the OMO promptly so that the data in the HI Service can be updated.
- Note that having two OMOs removes reliance on one person to keep records up to date in a timely fashion.

7.2.2 For Medical Practitioners and Other Clinicians

As the HI Service is intended to mostly operate in the background and assuming the practice's front-desk or administration staff manage patient IHIs, there is not a lot that clinicians need to concern themselves about the HI Service on a day to day basis. It is acknowledged that this may not be the case for practices that do not have non-clinical staff.

Many of the suggested actions below can be conducted via the Department of Human's Service HPOS website or alternatively, increasingly via your Desktop Software.

Key responsibilities for medical practitioners and other clinicians include:

☐ 1. Obtain your HPI-I and provide it to the OMO (e.g. Practice Manager) of the healthcare organisations in which you work.

[117] Note that is for the practice organisation(s). Your clinicians will need to maintain their own HPD entries.

□ 2. Make sure you have and maintain:

- A Department of Human Services Individual PKI certificate (needed for accessing the HI Service via HPOS and for some other eHealth and administration functions in HPOS); and
- A NASH PKI Certificate for Individual Healthcare Providers (needed for clinicians to access the Provider Portal on the practice's behalf).

It is a good idea that the OMO(s) of healthcare organisations in which you work knows you have these, and be sure to remember your PKI certificates' PICs.

□ 3. As per good practice, ensure your user account/profile details in the practice's Desktop Software is up-to-date and that you record accurate clinical data for your patients. This is especially important for medical histories, allergies, medications and immunisations.

□ 4. If your contact or professional information changes and you are registered with AHPRA, you will need to contact AHPRA or login to their website to update the relevant information. This data will then be sent to the Department of Human Services and information in their systems, including in the HI Service, will be updated[118]. These changes will pass through to the Healthcare Provider Directory (HPD) based on what data you have consented for viewing. You may wish to check the HPD to ensure the correct details are displayed.

□ 5. You should login into Human Services's HPOS website to view and verify information related to your HPI-I and how your information is displayed in the HPD (so that other healthcare providers can accurately identify you when they search it). Note you must provide your consent for your information to appear in the HPD, which can be done in HPOS.

□ 6. You may use the HPD to search for healthcare providers relevant to the care of your patients, e.g. for a referrals or general advice, if they have their contacts details published in the HPD.[119]

For the eHealth record system, clinicians are encouraged to talk with their patients about the associated risks of limiting access to all or part of their eHealth record, and to use their normal clinical judgement in situations where information may be absent or incorrect.[120]

[118] If you registered with the HI Service for your HPI-I (i.e. not AHPRA), you will need to inform the HI Service of any changes.

[119] Note that an update to the HI Service is being made that will permit healthcare providers to search for the HPI-I of other providers regardless of whether their details are published in the HPD or not.

[120] See the AMA PCEHR Guidelines for further related information **https://ama.com.au/ama-guide-using-pcehr**.

7.3 Clinical Incident Reporting

The eHealth Record System and foundation eHealth products enable improved access to clinical information, helping clinicians provide better, safer care to their patients.

It is important to recognise however that implementation of any new system in healthcare (electronic or otherwise) must be carefully monitored to ensure that any incidents[121] are identified and addressed. With the eHealth Record System, clinical incidents may relate to clinicians' interaction with the eHealth Record System directly, or the behaviour of their own Desktop Software when handling information from the eHealth Record System. These incidents may have safety, usability, technical, privacy or security components.

Incidents need to be documented so that the cause(s) can be identified and addressed. The developers and operators of the HI Service and of the eHealth Record System support their users and have processes to ensure that incidents are appropriately addressed. To do this, users need to report incidents in order to inform improvements and make it possible to later disseminate lessons to the wider audience of users. The process for doing this is discussed below.

The guiding principles of eHealth-related clinical incident reporting are important:

1. Reporting is voluntary (except in the case of data breaches, which are mandatory);
2. Only de-identified incident data should be reported for analysis to vendors; and
3. Clinical incidents should be reported to the appropriate organisation – see table on the next page.

If you identify an unexplained error in a clinical document that you have uploaded to a consumer's eHealth record, or have encountered a technical problem or service disruption while using the eHealth record system which may affect the care provided to your patient, you should call your software vendor in the first instance to determine whether the error can be resolved locally. You should also call the eHealth helpline on 1800 723 471 and select option two (provider enquiries). When speaking to the operator, let them know that you have identified a clinical safety issue.

Medicare Locals have a role in identifying issues that are of a general concern to the provision of safer care to patients. Hence, in addition to reporting clinical incidents formally as outlined in this Section, it is suggested that they should also be reported to your Medicare Local's Clinical Governance Committee for monitoring and follow up as required.

[121] Defined as "An event or circumstance that resulted or could have resulted, in unintended and/or unnecessary harm to a person and/or a complaint loss or damage", by ACSQHC, at: **http://www.safetyandquality.gov.au/wp-content/uploads/2011/09/NSQHS-Standards-Sept-2012.pdf.**

Key Contacts

The contacts below provide first line support, including for the referral of issues that may have clinical safety significance.

Topic	Key Contact
Local clinical information systems	Contact your software supplier's Helpdesk
Healthcare Identifiers Service	Department of Human Services Phone: 1300 361 457
PKI certificates	For Medicare certificates: the Department of Human Services eBusiness Service Centre Phone: 1800 700 199
eHealth record system Data Privacy Breaches	The eHealth record System Operator, i.e. The Department of Health Phone: 1800 723 471 Office of the Australian Information Commissioner: **http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/pcehr-system-mandatory-data-breach-notification-september-2012/mandatory-data-breach-notification-in-the-ehealth-record-system-text-des**
Other enabling products and services, e.g. National Clinical Terminology Information Service (AMT, SNOMED-CT-AU)	Email: **terminologies@nehta.gov.au**
Technical specifications	NEHTA Service Desk Support Email: **help@nehta.gov.au**

A sample reporting form is included in **Appendix F:**

Types of Issues to Monitor and Report

Issues in the operation of the eHealth systems are likely to arise from three main sources:

1. Clinical Software that connects to the HI Service and eHealth Record Systems;
2. Enabling infrastructure and services such as:
    a. Identification (HI Service) and authentication (PKI) and other services that are operated by third parties (including Contracted Service Providers (CSP); and
    b. Clinical documents in the eHealth Record System, including the way these are displayed; and
3. The eHealth Record System operated by The Department of Health, including the availability and display of clinical information.

Specifically, clinical incidents that occur in the course of treatment, that may be related to the eHealth Record System and may be contributory factors to patient harm, may include, but not be restricted to, those described below:

Practice Management Issues[122]

- Patient administration data, including identity or contact information may be missing, incorrect, incomplete, out of date or corrupt
- Misleading or absent information in a patient's clinical record
- Misleading, absent or conflicting information required for the management or planning of structured care
- Reference data is absent or incorrect

Clinical Systems Issues

- Clinical information is presented inappropriately or in a manner that its context is misleading or cannot be ascertained
- Failure to manage the scheduling or requesting of care services or the resources required to operate services
- Failure to manage the resources required to operate services
- Operational data analysis used to reduce clinical risk (e.g. audit/logs) not completed or completed incorrectly
- Data in inbound (or outbound) messages is incorrect, absent or is sent to the wrong destination
- Clinical System background tasks not completed or incorrectly completed

[122] This list is adapted from the BT Health Sentry System, which is licenced for use in Australia by NEHTA.

- A Clinical System feature intended to control clinical risk functions incorrectly installed or not at all

Service System Issues

- The Service and/or System performance is inadequate to support the clinical environment in which the system is intended to be used

- Whole or part of the Service and/or System is unavailable or access is inappropriately denied.

The process for reporting eHealth-related clinical incidents will be updated from time to time. Please check The Department of Health eHealth website for the latest information:

http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/Content/faqs-hcp

8 Resources for Support

The following table lists how you might go about addressing a range of support requirements related to implementing the eHealth features presented in this User Guide.

Requirement	Suggested Source
Specifically about your Desktop Software product and/or secure messaging service	The product's Vendor, e.g. from their website and Help Desk.
eHealth programs in your Local Area, including related to clinical governance and quality improvement	Your Medicare Local – find it at: **http://amlalliance.com.au/about-us/medicare-local/find-your-local-medicare-office**; or at: **http://www.medicarelocals.gov.au/** Your Local Health Network – find it at: **http://yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/lochospnetwork**
The Healthcare Identifier (HI) Service provided by Human Services, e.g. for: • HI Service general information and questions • Completing seed and network HPI-O applications • Registering or updating an RO's/OMO's details • Registering for a HPI-I	**http://www.humanservices.gov.au/hiservice** HI Service online user guide: **http://www.medicareaustralia.gov.au/hpos/online-user-guides/hi/** HI Service enquiries: Phone: 1300 361 457 Email: **healthcareidentifiers@humanservices.gov.au** See below for whom to contact for advice related to complex seed and network organisation HPI-O structures.

Requirement	Suggested Source
The national eHealth record system, e.g. for: • eHealth record general information and questions • Completing eHealth record Applications • Completing Participation Agreements	**http://www.ehealth.gov.au** eHealth record system enquiries: Phone: 1800 723 471 (select option 2) Note: eHealth record system registration can be completed online via Health Professional Online Services (HPOS) once HI Service registration is complete, at: **http://www.humanservices.gov.au/hpos** Registration and access to the eHealth record system as a consumer should be at: **http://my.gov.au**
PKI Certificates, e.g. for: • NASH PKI certificates general information and questions • Human Services site PKI certificates general information and questions • PKI certificates installation support • PKI certificate and tokens lost / forgotten passwords	**http://www.humanservices.gov.au/pki** eBusiness Service Centre: Phone: 1800 700 199 (option 2) Email: **nash.pki@humanservices.gov.au** Note: you may also find it beneficial to contact the vendor of your Desktop Software and/or secure messaging service for support relating to PKI certificates in your practice.
PIP, including the eHealth Incentive Payment scheme	**http://www.medicareaustralia.gov.au/pip** **http://www.nehta.gov.au/pip** For general enquiries about the PIP, eHealth Incentive payments or how to apply, email **pip@humanservices.gov.au**, or contact the PIP enquiry line on 1800 222 032

Requirement	Suggested Source
Complex seed and network organisation HPI-O structures Secure Message Delivery (SMD)	For General information and guidance on eHealth registration and implementation, Seed and Network structure questions, and SMD general information and questions. Online form to request on-site assistance: **http://www.nehta.gov.au/help-centre/online-assistance?view=form** NEHTA Helpdesk: Phone: 1300 901 001 Email: **help@nehta.gov.au**
Assisted registration to the eHealth record system, for: • Assisted Registration functionality available to healthcare provider organisations to assist their patients to register for an eHealth record	**http://ehealth.gov.au/internet/ehealth/publishing.nsf/content/assistedreg_01** eHealth record enquiry line: Phone: 1800 723 471 Email: **PCEHR.AssistedReg@health.gov.au**

Appendix A: Glossary

Website links are included as an aid to the reader where relevant.

Acronym/Term	Meaning
ACIR	Australian Childhood Immunisation Register – is a national register administered by the Department of Human Services that records details of vaccinations given to children under seven years of age who live in Australia. **http://www.humanservices.gov.au/customer/services/medicare/australian-childhood-immunisation-register**
AODR	Australian Organ Donor Register – is the only national register for organ and/or tissue donation for transplantation. It is administered by the Department of Human Services. The AODR keeps a record of an individual's stated decision with regard to organ and tissue donation. **http://www.humanservices.gov.au/customer/services/medicare/australian-organ-donor-register**
ACSQHC	Australian Commission on Safety and Quality in Healthcare – is a government agency that was established by the Commonwealth, with the support of State and Territory governments. It leads and coordinates national improvements in safety and quality in health care across Australia. **http://www.safetyandquality.gov.au/**
AHPRA	Australian Health Practitioner Regulation Agency – is the organisation responsible for the implementation of the National Registration and Accreditation Scheme across Australia. It works with 14 National Health Practitioner Boards in implementing the Scheme. **http://www.ahpra.gov.au/**
AMA	Australian Medical Association – is the peak membership organisation representing the registered medical practitioners (doctors) and medical students of Australia. It promotes and protects the professional interests of doctors and the health care needs of patients and communities. **http://www.ama.com.au**

Acronym/Term	Meaning
AMLA	Australian Medicare Local Alliance – is a national, government funded not-for-profit company which has been established to spearhead an organised system for primary health care across the country through a network of 61 primary health care organisations called Medicare Locals (MLs). **http://www.amlalliance.com.au/**
B2B	Business to Business – this is electronic communication between one business system and another business system.
CDA	Clinical Document Architecture – is a HL7 standard for the representation and machine processing of clinical documents in a way that makes the documents both human readable and machine processable. **http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7**
CDSA Tool	Clinical Data Self Assessment Tool – is a simple-to-use tool that helps assess, analyse and improve the quality of data contained in most desktop clinical software systems. **http://publiclearning.ehealth.gov.au/hcp/preparing-your-data/implement-data-quality-improvements/make-use-of-clinical-software-tools/**
DC	Document Code – is a code which may be used to restrict access to individual documents within an individual's eHealth record. This was previously referred to as a Limited Document Access Code (LDAC) or Provider Access Consent Code Extended (PACCX).
DHS	Department of Human Services
Department of Health	Commonwealth Department of Health – has a diverse set of responsibilities and aims to deliver better healthcare services for all Australians including the eHealth record system. **http://www.health.gov.au/**
DVA	Commonwealth Department of Veterans' Affairs – is responsible for carrying out government policy and implementing programs to fulfil Australia's obligations to veterans, war widows and widowers, and serving and former members of the Australian Defence Force. **http://www.dva.gov.au/**

Acronym/Term	Meaning
DAO	Duly Authorised Officer – is the contact person in practices for Medicare Online. The DAO can be the business owner, manager or an individual health provider (with a provider number) e.g. Doctor.
Desktop Software	Clinical Information Systems and/or Patient Management Systems used in medical practices that stores clinical data such as the patient's history of illness and the interactions with healthcare providers.
eHealth record	An eHealth record enables the collection of health information about registered individuals from a number of different sources and allows that information to be used and disclosed to registered participants in accordance with the access controls set by the individual. Note: this was previously referred to as the 'PCEHR'. It is now referred to in the first instance as 'the personally controlled electronic health (eHealth) record' and 'eHealth record' thereafter.
eHealth record system	The personally controlled electronic health (eHealth) record system was launched on 1 July 2012 and provides a way of managing health information online that will make it more accessible to Australians who chose to sign up with the system, and their chosen healthcare professionals. The eHealth record system is supported by a legislative framework consisting of the Personally Controlled Electronic Health Records Act 2012, the amended Healthcare Identifiers Act 2010, PCEHR Regulations, amended Healthcare Identifiers Regulations and PCEHR Rules. For information: **http://www.ehealth.gov.au** For registration and access: **http://my.gov.au**
ES	Event Summary – is a clinical document that may be uploaded to an individual's eHealth record summarising one or more healthcare events.
Healthcare Organisation	A Healthcare organisation is an entity, or a part of an entity, that has conducted, conducts, or will conduct, an enterprise that provides healthcare (including healthcare provided free of charge). An example of a healthcare organisation is a public hospital or a corporation that runs a medical centre.
Healthcare Professional	A healthcare professional is a person who is involved in or associated with healthcare delivery. For the purposes of the eHealth record system a healthcare professional is a person who has a HPI-I and is authorised by a registered healthcare organisation to access the eHealth record system on their behalf. This was previously referred to as Individual Healthcare Provider.

Acronym/Term	Meaning
Healthcare Provider	This term is no longer used. Healthcare Organisation or Healthcare Professional (see above) are to be used in preference to clearly distinguish the two roles.
HI Act	The Healthcare Identifiers Act 2010 – establishes the Healthcare Identifiers Service and regulates related matters. **http://www.comlaw.gov.au/Details/C2012C00590**
HI Service	Healthcare Identifiers Service – enables unique identifiers to be created for individuals and healthcare providers across the Australian health system – see IHI, HPI-I and HPI-O.
HI Service Operator	The role performed by the Commonwealth Department of Human Services (Human Services) in operating the HI Service as provided for in the HI legislation.
HL7	Health Level Seven – is the global authority on standards for interoperability of health information technology with members in over 55 countries. **http://www.hl7.org**
HPD	Healthcare Provider Directory – is a provider directory service established and maintained by the HI Service Operator. **http://www.humanservices.gov.au/hiservice** (go to HPD link)
HPI-I	Healthcare Provider Identifier – Individual – is a 16 digit unique number used to identify individual healthcare professionals who deliver healthcare in the Australian healthcare setting.
HPI-O	Healthcare Provider Identifier – Organisation – is a 16 digit unique number generated by the HI Service and used to identify individuals who receive healthcare in the Australian health system.
HPOS	Health Professional Online Services – offers access to Medicare online services for health professionals through a single entry point. It provides access to information about your identity (inc. in the HI Service), eligibility under Medicare arrangements and information on payment of Medicare claims. **http://www.medicareaustralia.gov.au/hpos/**

Acronym/Term	Meaning
Human Services	Australian Government Department of Human Services – is responsible for the development of service delivery policy and provides access to social, health and other payments and services. Human Services operate Service Centres offering Medicare services, the helpline and the HI Service. **http://www.humanservices.gov.au/**
IHI	Individual Healthcare Identifier – is a 16 digit unique number used to identify individuals who receive or may receive healthcare in the Australian health system.
IRN	Individual Reference Number – appears to the left of an individual's name on their Medicare card.
LHN	Local Hospital Network (also called Local Health or Local Health and Hospital Network in different jurisdictions) – A total of 136 LHNs have been established across all states and territories. They manage the delivery of public hospital services and other community based health services. **http://www.yourhealth.gov.au/internet/yourhealth/publishing.nsf/Content/lochospnetwork**
MBS	Medicare Benefits Schedule – is a listing of the healthcare services subsidised by the Australian government under the Health Insurance Act 1973. The MBS is part of the wider Medicare Benefits Scheme managed by The Department of Health and administered by Department of Human Services. **http://www.medicareaustralia.gov.au/provider/medicare/mbs.jsp** **http://www.mbsonline.gov.au/**
MDO	Medical Defence Organisation – a company that provides medical indemnity insurance to medical practitioners and practices.
Medicare	A program run by the Department of Human Services. See Human Services.
ML	Medicare Local – is a primary health care organisation established to coordinate primary health care delivery and address local health care needs and service gaps. There are 61 Medicare Locals across the country. The AMLA is the national body. In most cases MLs replaced Divisions of General Practice. **http://www.medicarelocals.gov.au**

Acronym/Term	Meaning
NASH	National Authentication Service for Health – is a secure and authenticated service for healthcare provider organisations and personnel to exchange sensitive eHealth information. The service will issue digital credentials, including digital certificates managed through the Public Key Infrastructure (PKI) and secured by tokens such as USB sticks and smartcards. **http://www.nehta.gov.au/our-work/nash** **http://www.humanservices.gov.au/nash**
NEHTA	National E-Health Transition Authority – was established by the Commonwealth, state and territory governments to develop better ways of electronically collecting and securely exchanging health information and was managing agent for the design and build of the eHealth record system. **http://www.nehta.gov.au**
NESAF	National eHealth Security and Access Framework – is the nationally recommended structure for security management of information resources for healthcare in Australia. The NESAF is based on the International Standards Organisation's principles (ISO27799 and ISO27002). **http://www.nehta.gov.au/our-work/security** **http://www.racgp.org.au/your-practice/e-health/cis/national-e-health-security-and-access-framework-(nesaf)/**
Network Hierarchy	A network hierarchy is a connected group of healthcare organisations, comprising one seed organisation and one or more network organisations linked to the seed organisation.
Network Organisation	A network organisation is part of, or subordinate to, a seed organisation, has its own HPI-O and provides health services.
NHSD	National Health Services Directory – is implemented by Healthdirect Australia on behalf of, and with the support of, all Australian Governments. The NHSD provides service and contact information for general practices, pharmacies, hospitals and emergency departments, and plans to include other providers and more comprehensive information. **http://www.nhsd.com.au**

Acronym/Term	Meaning
NPDR	National Prescription and Dispense Repository – as part of the national eHealth record system (as a Registered Repository), stores information about medicines that have been prescribed and dispensed to a consumer.
NPDV	National Prescription and Dispense View – is a way for consumers and healthcare providers to view information about prescribed and dispensed medicines displayed in one location. NPDV is available to consumers through their eHealth record portal and to healthcare providers via the eHealth record system's provider portal or through clinical software that has the NPDV functionality.
OAIC	Office of the Australian Information Commissioner – has oversight of the operation of the Freedom of Information Act 1982 and review of decisions made by agencies and ministers under that Act, functions conferred by the Privacy Act 1988 and other laws, and government information policy functions. The Commissioner is the key regulator for the eHealth record system and has the capacity to conduct audits, commence investigations, impose a range of sanctions and accept enforceable undertakings. **http://www.oaic.gov.au/**
OMO	Organisation Maintenance Officer – is a person registered under the HI Service and has authority to act on behalf of a healthcare provider organisation in its dealings with the System Operator of the eHealth record system.
PBS	Pharmaceutical Benefits Scheme – is a program for providing pharmaceutical benefits to eligible Australians under the National Health Act 1953. **http://www.pbs.gov.au**
PCEHR	See eHealth record
PCEHR ACT	The Personally Controlled eHealth Records Act 2012 (PCEHR Act) provides the critical components of the eHealth record system, while the operational detail is contained in the PCEHR Regulations and PCEHR Rules. It commenced on 29 July 2012. The PCEHR Act establishes the role of the eHealth record System Operator and its advisory committees, a privacy and security framework, penalty provisions and common mechanisms associated with the transparency and scrutiny of the Act. **http://www.comlaw.gov.au/Details/C2013C00295**

Acronym/Term	Meaning
PCEHR Regulations	The Personally Controlled eHealth Records Regulations (PCEHR Regulations) provide operational detail to support the eHealth record system. The PCEHR Regulations came into effect on 29 July 2012. **http://www.comlaw.gov.au/Details/F2012L01399**
PCEHR Rules	The Personally Controlled eHealth Records (PCEHR) Rules contain requirements regarding the day to day operation of the eHealth record system. **http://www.comlaw.gov.au/Details/F2012L01703**
PIC	Personal Identification Code – provided by Human Services for use with PKI certificates as part of the authentication process. Similar to a PIN used for banking.
PKI	Public Key Infrastructure – is a set of procedures and technology that provides security and confidentiality for electronic business. **http://en.wikipedia.org/wiki/Public_key_infrastructure** **http://www.humanservices.gov.au/pki**
RC	Record Code –is a code which may be used to restrict access to an individual's eHealth record. The code is provided to a healthcare provider to grant access to the individual's eHealth Record. This was previously referred to as a Record Access Code (RAC) or the Provider Access Consent Code (PACC).
RO	Responsible Officer – is a person registered under the HI Service and has authority to act on behalf of the seed organisation and relevant network organisations in its dealings with the System Operator.
Seed Organisation	A seed organisation, for the purpose of participating in the eHealth record system, is an entity that provides or controls the delivery of healthcare services.
SHS	Shared Health Summary – is a clinical document summarising an individual's health status and includes important information such as allergies/adverse reactions, medicines, medical history and immunisations. Only a nominated healthcare provider can create or update the Shared Health Summary.

Acronym/Term	Meaning
SMD	Secure Message Delivery – is a set of specifications that defines an approach to eHealth communication using widely supported IT industry standards. It focuses on the secure delivery of messages, which contain clinical documents and/or information, between healthcare organisations. **http://www.nehta.gov.au/our-work/secure-messaging**
System Operator	The System Operator of the eHealth record system is the person with responsibility for establishing and operating the eHealth record system. The System Operator is presently the Secretary of The Department of Health. **http://www.ehealth.gov.au**
RACGP	Royal Australian College of General Practitioners – is the professional body for General Practitioners in Australia. It researches, lobbies and advocates on issues that influence GPs and their practice teams. **http://www.racgp.org.au**

Appendix B: Further Information on eHealth Features

The following subsections provide information additional to that provided in Sections **3.2** and **3.3**.

B.1 eHealth-related Directories

The following is an overview of the following four eHealth directories in Australia:

- Healthcare Provider Directory (HPD)
  http://www.humanservices.gov.au/hpos/
  (requires a PKI certificate to access)
  http://www.humanservices.gov.au/hiservice
- National Health Services Directory (NHSD)
  http://www.healthdirect.org.au/service/national-health-services-directory
- Healthcare Public Directory
  http://www.certificates-australia.com.au/general/cert_search_health.shtml
  > Healthcare Public Directory
- NASH Directory
  http://www.certificates-australia.com.au/general/cert_search_health.shtml
  > NASH Directory (requires a PKI certificate to access)

Healthcare Provider Directory (HPD) (also known as HI Provider Directory in HPOS)

The Healthcare Provider Directory (HPD) is an opt-in listing of healthcare organisations and providers registered with the Healthcare Identifiers (HI) Service that can be accessed only by authorised users of the HI Service.

Healthcare providers can use the HPD to look up details of healthcare organisations and individuals. They can do this by searching the HPD using a HPI-I or HPI-O number, or demographic details. This can help when sending secure messages, referrals, discharge summaries and forwarding diagnostic test requests for patients.

Your privacy is protected because you give consent to be listed in the HPD and control which contact and demographic details are visible.

National Health Services Directory (NHSD)

The NHSD is a consolidated and comprehensive national directory of health services and provider information. It covers all Australian jurisdictions with services across the public and private sector.

The NHSD currently provides essential service information such as location, opening hours and contact details for general practices, pharmacies, hospitals and emergency departments.

In the future, the NHSD may include service details for specialists, allied health professionals, local hospital and community services and also provides information about deputising, virtual and telehealth services, as well as languages spoken, bulk billing and access to disabled facilities.

For more information on the NHSD please see:
http://www.nhsd.com.au/sites/default/files/NHSD_Overview_A4_FA.pdf

Healthcare Public Directory (also known as Certificates Australia or X.500 Directory)

The Healthcare Public Directory is a publicly accessible directory which contains a list of the public key and limited identifying information that is attached to active, suspended and unexpired Human Services PKI Certificates.

The Directory acts as a 'White pages' and can be searched on key words to find organisations and individual PKI certificates. It contains information regarding the type of PKI certificate, its Registration Authority (RA) number and expiry dates.

The Healthcare Public Directory contains a link to the NASH Directory.

NASH Directory

The NASH Directory is a secure directory which lists the public key and limited identifying information that is attached to each NASH PKI Certificate for Healthcare Provider Organisations and NASH PKI Certificate for Supporting Organisations.

The Directory acts as a 'White pages' and can be searched on key words to find an organisation PKI certificate.

Further Information

Open "Section 7 – Useful Information" on the following web-page for the *Overview of eHealth Directories* document:

http://www.nehta.gov.au/our-work/implementation-and-adoption/ehealth-registration-support/general-practice-registration-workbook.

In addition, the following web-page provides useful information:

http://www.humanservices.gov.au/nash

B.2 NESAF

The vision for the NESAF is:

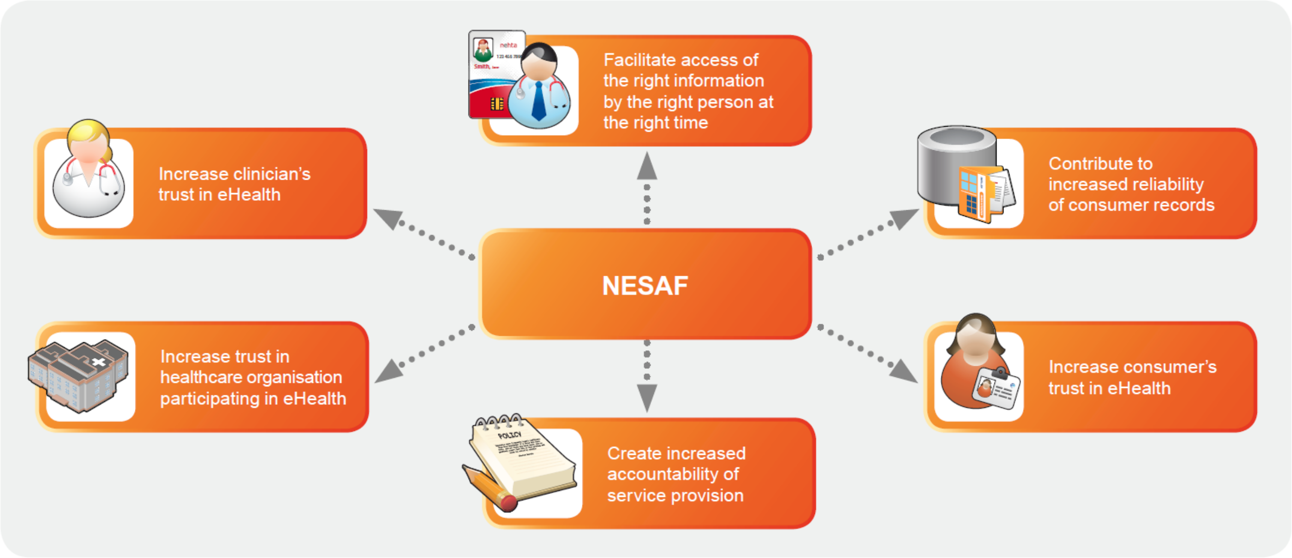
> *"To increase certainty that health information is created and accessed in a secure and trustworthy manner"*
> – the NESAF Vision Statement

The mission for the NESAF is to:

- Ensure that access to consumer health information is consistently controlled and monitored as it transitions through independent organisations, business processes and systems in the Australian health sector; and
- Make sure that the provenance of all electronic health information is traceable from its creation at a verifiable trusted source, through its transition and possible augmentation on route to its destination.

To achieve this vision and mission, NESAF supports organisations engaged in national eHealth to adopt a consistent approach to and application of health information security standards, and provides guidance in relation to eHealth-specific security and access practices. As eHealth becomes more prevalent in medical practice and offers further improvements for shared care and care planning, there is a greater need to protect the privacy alongside this increased sharing of sensitive data. [123]

The NESAF recommends that healthcare organisations establish an information security infrastructure using a risk-based approach. This is based on the premise that security is not a single solution, but a process of risk assessment, together with appropriate controls. Managing local security and access measures will ensure higher trust in the system and will result in a greater uptake of eHealth initiatives. The benefits of the NESAF are illustrated in the diagram below.


Facilitate access of the right information by the right person at the right time
Increase clinician's trust in eHealth
Contribute to increased reliability of consumer records
NESAF
Increase trust in healthcare organisation participating in eHealth
Increase consumer's trust in eHealth
Create increased accountability of service provision

[123] Some information in this section is adapted from **http://www.racgp.org.au/download/documents/e-health/2012nesaf_information.pdf**.

The NESAF is the nationally recommended structure for security management of information resources, and is a foundation for information security management within medical practice. The NESAF is based on the same international standards[124] as that of the RACGP's CISS. Further information on the NESAF is available at:

http://www.nehta.gov.au/our-work/security

B.3 Clinical Terminology Systems for Australian Medical Practice

NEHTA is playing a key leading role in the development of the following clinical terminologies: [125]

- **Australian Medicines Terminology (AMT) –** The AMT delivers standardised identification of brand (trade) products and equivalent generic medicines along with associated components that are supported through standard naming conventions that accurately describe medicines;[126]
- **SNOMED CT** – The Systematized Nomenclature of Medicine, Clinical Terms (SNOMED CT®) is considered the most comprehensive, multilingual clinical terminology in the world. When implemented in software, SNOMED CT represents clinically relevant information consistently, reliably and comprehensively as an integral part of the electronic health record; and
- **SNOMED CT Australia** –SNOMED CT-AU is the Australian extension to SNOMED CT, and includes the international resources along with all Australian developed terminology and documentation for implementation in Australian clinical IT systems. SNOMED CT-AU provides local variations and customisations of terms relevant to the Australian healthcare community.

SNOMED CT has been identified by NEHTA as the preferred clinical terminology and has been endorsed as Australia's national standard.[127]

Desktop Software products commonly used by medical practices in Australia do not as yet have SNOMED CT-AU "inside", as the selection of this standard for Australia was made in recent years and certainly after most of these products were designed. The developers of these products designed their own vocabulary systems or adapted those used in other products. Consequently in Australia we have a variety of vocabulary systems in use, including DOCLE, LOINC, PYEFINCH and ICPC2+, as examples.

The developers of Desktop Software commonly used in medical practices are working to ensure their products can exchange clinical information reliably by using

[124] International Standards Organisation's principles (ISO27799 and ISO27002).

[125] See **http://www.nehta.gov.au/our-work/clinical-terminology**.

[126] See **http://www.nehta.gov.au/our-work/clinical-terminology/australian-medicines-terminology**.

[127] See **http://www.nehta.gov.au/our-work/clinical-terminology/snomed-clinical-terms**.

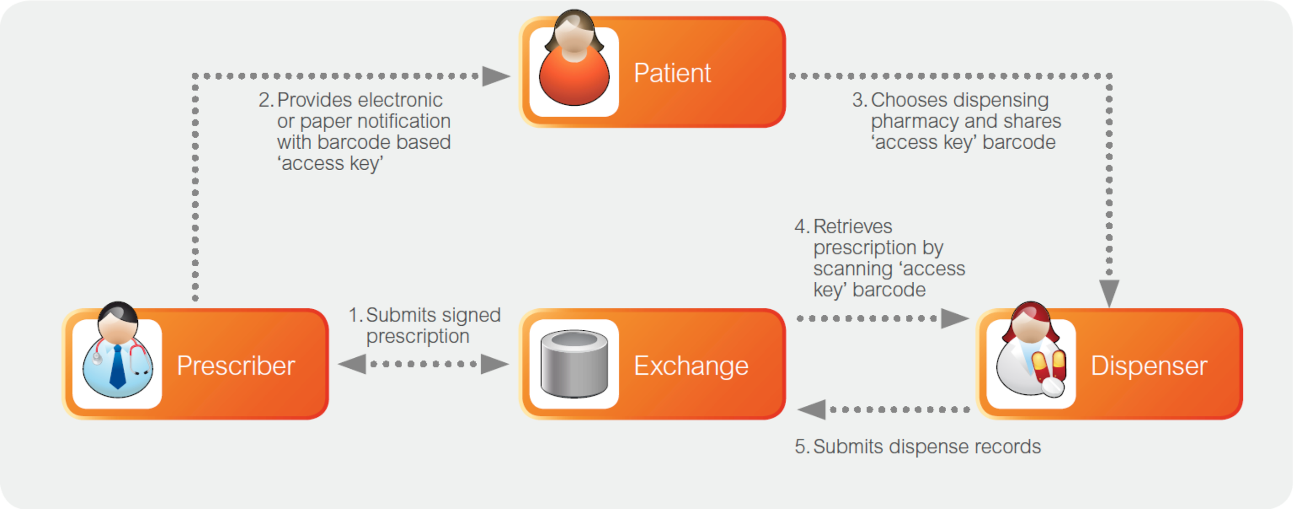
a process of mapping the codes in their vocabulary systems to SNOMED CT-AU, so that standard clinical terminology definitions can be shared as part of electronic clinical communications and in the eHealth record system.

The National Clinical Terminology and Information Service (NCTIS) within NEHTA is responsible for managing, developing and distributing SNOMED CT-AU and the Australian Medicines Terminology (AMT) in Australia. This responsibility extends to distributing and licensing SNOMED CT on behalf of the International Health Terminology Standards Development Organisation (IHTSDO), in which Australia's membership is represented by NEHTA.[128]

B.4 eMedication Management Overview

This appendix provides an overview of the broader subject of eMedication Management, i.e. as introduced and discussed in Sections **3.3.2, 3.3.3**, **4.3** and **5.5.4**, in relation to ETP[129]. It also describes the NPDR[130], which was launched at the time of writing and associated functionality.

The diagram below illustrates how ETP is designed to work, with the box labelled as "Exchange" being the PES (Prescription Exchange Service) as introduced earlier.


Patient
2. Provides electronic or paper notification with barcode based 'access key'
3. Chooses dispensing pharmacy and shares 'access key' barcode
4. Retrieves prescription by scanning 'access key' barcode
Prescriber
1. Submits signed prescription
Exchange
Dispenser
5. Submits dispense records

By way of explanation:

The Prescriber – The prescribing system consists of desktop software installed in a doctor's office. With the patient's consent, doctors will be able to:

a) Create a digitally signed, legal, electronic prescription (pending legislative approval);

b) Securely submit the prescription to an Exchange Service;

[128] See **http://www.ihtsdo.org/**.

[129] Electronic Transfer of Prescriptions. Introduced in Section **3.3.2**.

[130] The National Prescription and Dispense Repository. Discussed in Section **3.3.3**.

c) Provide a paper or electronic notification to inform the patient of what medication they have been prescribed; and

d) View and cancel prescriptions prior to dispensing.

The Exchange – The Prescription Exchange Service (PES) acts as an intermediary between the prescriber and the dispenser. It provides a single point of control allowing:

a) Patients to choose their dispensing pharmacy; and

b) Dispensers to securely access records via a digital key.

The Dispenser – The dispensing system is desktop software that resides in pharmacies and interacts with the Exchange to:

a) Retrieve prescriptions for dispensing medication;

b) Submit Dispense Records to the Exchange upon dispensing; and

c) Terminate or reverse a previously initiated dispensing process.

In addition, ETP will enhance the processes related to repeat prescriptions.

The implementation of ETP, as described above, will be possible when technical specifications are finalised and endorsed by Standards Australia, legislation is passed permitting paper-less prescriptions and the software used by prescribers and dispensers is updated to support this new functionality and the related processes. In the meantime the current implementation of ETP, particularly now that the PESs can interoperate, can be used by prescribers and dispensers for the benefit of their patients and their workflow.

It is important to distinguish between the roles of ETP and the NPDR, i.e. as part of the eHealth record system:

- ETP, in its current form and next version, is intended to support the *transactions* and processes related to prescriptions between prescribers and dispensers, i.e. it acts as a sort of post-box for the *legal* form of the prescription and hence also how it relates to PBS (and RPBS) for payments, etc.; and
- The repository (NPDR) stores prescription and dispense information in the form of clinical documents (i.e. in CDA format) that is indexed to a patient’s eHealth record, i.e. as a *record* of what has been prescribed and what has been dispensed, and not as the *legal* prescription (i.e. as the instrument that carries with it certain attributes like the authority for dispensing and access to payment via the PBS and RPBS).

The way the two will work together is that when an electronic prescription is created, the prescriber, through their updated Desktop Software, will be able (relying on the consumer’s standing consent obtained at registration) to:

- Send the prescription (as the legal instrument) to the PES; and
- To have it uploaded it as a clinical document to the patient’s eHealth record via the NPDR.

If a patient has an eHealth record and their healthcare provider is using ETP and is registered with the eHealth record system, a copy of prescription information will flow through to the NPDR via the PES, as long as the patient has not withdrawn their consent for the information to be uploaded. If consumers don't consent for this to occur, then the prescriber is required to note in their records that this was the case.

Similar to prescribers, dispensers, through their updated software, will be able to send a dispense notification to the PES, which will upload a dispense document to the NPDR that becomes linked to the corresponding prescription document viewable in the patient's eHealth record.

Through this approach, all authorised healthcare providers, i.e. not just the prescriber and dispenser, will be able to view patients' prescription and dispense information through the eHealth record system. This innovation will provide significant value to healthcare providers who currently may have incomplete or inaccurate medicines information about their patients.

Release 3 of this User Guide will provide further information, including implementation advice and guidance, on the enhanced ETP and the integration of prescription and dispense information (via the NPDR) in the eHealth record system, for medical practices.

NEHTA's website has a section on eMedication Management, which is at:

http://www.nehta.gov.au/our-work/emedication-management

Appendix C: Further Information on HPI-O Structuring

This appendix provides information additional to that in Section **5.4** for practices that wish to consider establishing a HPI-O hierarchy, i.e. instead of the simple model of having just a Seed HPI-O.

In addition to the information below, it is suggested that you read the following document:

http://www.nehta.gov.au/component/docman/doc_download/1599-seed-and-network-configuration-guidance

C.1 HPI-O Structure Options

There are two organisation types that can be registered within the HI Service:

- **Seed Organisation** – identified as having a Seed HPI-O; and
- **Network Organisation** – identified as having a Network HPI-O.

A healthcare provider organisation that participates in the HI Service could have:

- A configuration of one Seed Organisation; or
- A Seed Organisation with one or more Network Organisations under the Seed (this is called a network hierarchy).

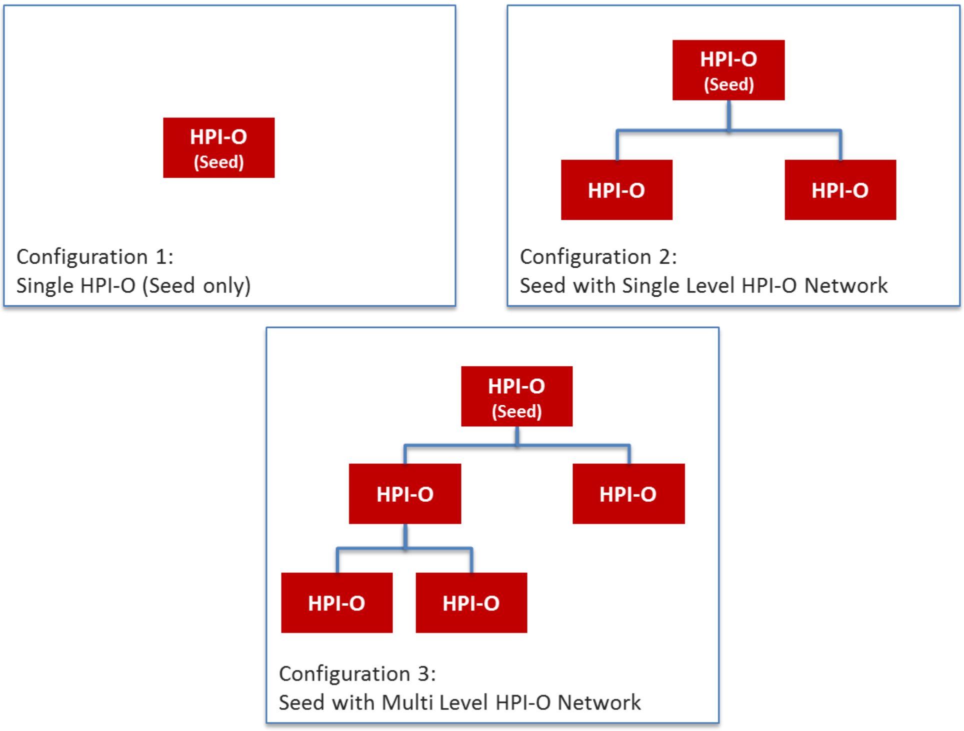
A **Seed Organisation** is an organisation within Australia that provides or controls the delivery of healthcare services.

A **Network Organisation** is linked to and provides services on behalf of a seed organisation within a network hierarchy; and is part of or subordinate to a seed organisation in a legal, business and/or administrative sense. Every network organisation must be associated with a seed organisation. Network organisations can be used to represent different departments, sections or divisions within an organisation (e.g. departments within a hospital) and can be separate entities from the seed organisation.

For the purposes of accessing and using the eHealth record system, a **network hierarchy** is a connected group of healthcare provider organisations, comprising of one seed organisation and one or more network organisations linked to the seed organisation. An example of a seed organisation with a network hierarchy could be a hospital, a regional health service district or a network of GP clinics. A network hierarchy is created and managed by the seed organisation in accordance with both the HI Act 2010 and with the PCEHR Rules 2012.

If you have separate legal entities in your practice organisation structure and if participation in the eHealth record system is required for such entities, then each legal entity will also be required to separately sign the Participation Agreement. However, it is not essential that each legal entity have its own HPI-O.

The types of network hierarchies that are possible are illustrated in the diagram below.



Configuration 1:
Single HPI-O (Seed only)

Configuration 2:
Seed with Single Level HPI-O Network

Configuration 3:
Seed with Multi Level HPI-O Network

In order to avoid undue complexity, this User Guide does not provide guidance for practice organisations that have an arrangement with a CSP (Contracted Service Provider – see Section **3.2.1** above). Such practice organisations would be aware of this and the contracted service provider would liaise with the practice organisation to design and bring into effect the most suitable HPI-O configuration.

C.2 Access Flags for the eHealth Record System

Access Flags can also be set at different points in the network hierarchy to control access to patients' eHealth records. They are a feature of the eHealth record system that facilitates a consumer's ability to control access to their eHealth record. An access flag is set against the HPI-O(s) specified by the healthcare provider's RO or an OMO (of the Seed HPI-O).

Access flags need to be set and maintained by healthcare provider organisations in a way that balances **reasonable consumer expectations** about the sharing of information as part of providing healthcare to the consumer, and **arrangements**

within the organisation for access to health information collected by the organisation.[131]

In particular, the assigning of access flags should:[132]

- Ensure that a consumer is able to receive the healthcare that he or she needs while also ensuring that access to his or her eHealth record does not extend beyond the registered healthcare organisations reasonably necessary for this to occur; and

- Support a consumer's ability to ascertain quickly and simply which additional registered healthcare organisations (if any) would have access to the consumer's eHealth record if a particular registered healthcare organisation were to be added to the access list for the consumer's eHealth record.

If an access flag is not specifically assigned to a network organisation in a network, that organisation can still access the eHealth record system and view and upload information to a consumer's eHealth record. However, it effectively does so under the access of the first organisation above them in the network hierarchy that has been assigned an access flag. This would be the seed organisation if no other organisation in the network has been assigned an access flag.

In a network hierarchy with multiple HPI-Os, when a consumer views their audit log or receives a notification that an organisation has interacted with their eHealth record, this relates to the HPI-O that has accessed their record.

Each eHealth record has a Provider Access List, which identifies the organisation in a hierarchy to which an access flag has been assigned. When a healthcare provider organisation accesses a consumer's eHealth record for the first time, that organisation's HPI-O is added to the consumer's Provider Access List.

The information provided to a consumer in their eHealth record will identify activity undertaken in connection with a record at a healthcare provider organisation level. This means that any healthcare provider organisation that has an HPI-O can be identified as having accessed or uploaded documents to an eHealth record.

However, a consumer's capability to limit access to an eHealth record, or documents within it, is managed at an access flag level. An access flag is automatically assigned to a seed organisation, because from a practical perspective, a seed organisation must always be assigned an access flag.

The Responsible Officer (RO) or a Seed Organisation Maintenance Officer (OMO)[133] is responsible for assigning access flags to Network HPI-Os in their practice's HPI-O hierarchy. Access flags are assigned as part of the eHealth record system registration process and need to be updated whenever necessary.

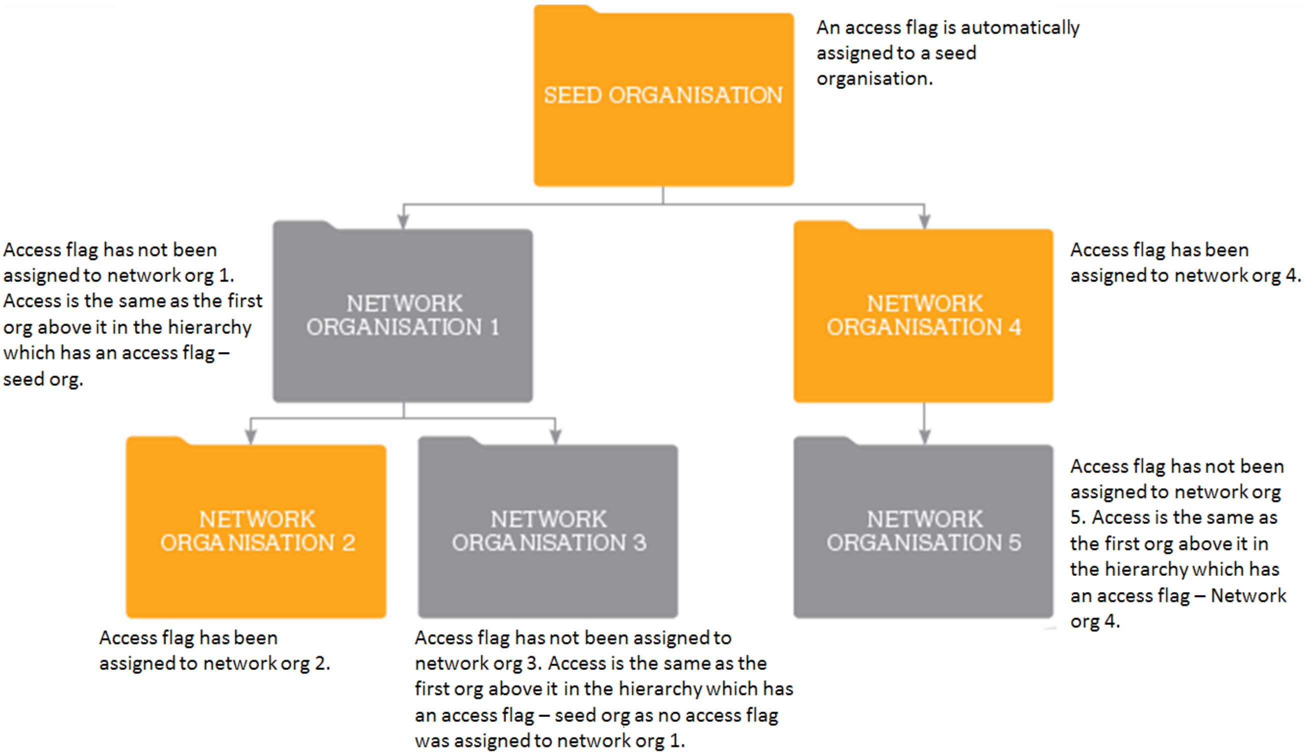
[131] This is from Section 9 of the PCEHR Rules 2012.

[132] This is from the PCEHR Provider Registration Booklet – available from: **http://www.ehealth.gov.au/internet/ehealth/publishing.nsf/content/providerregistration_eBooklet**.

[133] These roles are discussed in Section **5.4.4**.

As previously mentioned, for the eHealth record system, it is required that each legal entity in your healthcare provider organisation separately sign the Participation Agreement.

The diagram below illustrates an example of a network hierarchy with access flags set at different points to highlight the effect of their settings on access to patient eHealth records.



An access flag is automatically assigned to a seed organisation.

Access flag has not been assigned to network org 1. Access is the same as the first org above it in the hierarchy which has an access flag – seed org.

Access flag has been assigned to network org 4.

Access flag has not been assigned to network org 5. Access is the same as the first org above it in the hierarchy which has an access flag – Network org 4.

Access flag has been assigned to network org 2.

Access flag has not been assigned to network org 3. Access is the same as the first org above it in the hierarchy which has an access flag – seed org as no access flag was assigned to network org 1.

For further information on the principles that must be applied when assigning access flags, and a worked example, please see the Provider Registration Booklet.

C.3 Deciding on Your HPI-O Structure

As introduced in Section 5.4.2, choosing an appropriate HPI-O configuration is an important factor that influences your practice organisation's participation in:

- **The Healthcare Identifiers (HI) Service** – for searching for and validating healthcare identifiers, i.e. IHIs, HPI-Os and HPI-Is;
- **The eHealth Record System** – for setting Access Flags to control posting to, viewing of and retrieving from patient records;
- **Secure Message Delivery (SMD)** – for inbound messages to reach and be decrypted by a specific part of your practice organisation, and for the sending identity of outbound messages to be appropriate for the intended purpose, and encrypted; and
- **Directories** such as the Healthcare Provider Directory (HPD) – so that your practice organisation (and any subsets, and individual clinicians where appropriate) can be discoverable for eHealth communications, e.g. referrals.

In most cases for medical practices, the most suitable HPI-O configuration will be the simplest, i.e. just a Seed HPI-O (configuration 1 in the diagram in Appendix **C.1** above), which also is established automatically with a single Access Flag for the eHealth record system.

However, practice organisations that have multiple sites and/or business units, e.g. clinics, pharmacies, etc. that operate separately as part of an over-arching organisational or corporate structure, will likely require a different configuration, i.e. a Seed HPI-O and one or more Network HPI-Os under that, and potentially other Network HPI-Os under Network HPI-Os.

In addition to organisational or corporate structure considerations, some factors that may influence you in determining an appropriate HPI-O configuration include:

- Whether you have or need separate endpoints[134] for secure messaging. If so, a separate Network HPI-O may be required for each. If you don't then your Seed HPI-O or a single specific Network HPI-O may perform this role;

- Whether you need separate control points for accessing the eHealth record system, e.g. for within separate business units from the rest of the practice organisation, e.g. clinics. If so, separate Network HPI-O(s) may be required so that Access Flags can be set at that point in your HPI-O hierarchy (as discussed in the previous section). Note too that access to the HI Service and the eHealth record system is recorded in an audit log against each HPI-O; and

- If a presence in the Healthcare Provider Directory (HPD) or other directories is required for separate organisational or business units, e.g. clinics. If so, Network HPI-O(s) may be required for these. Note, this may or may not also be for the same entities for the purposes of secure messaging, as discussed above.

If you feel that your practice organisation requires more than the simple configuration of just a Seed HPI-O, then it is recommended that you seek advice, and if necessary assistance, from your Medicare Local and the organisations that provide your practice with eHealth and IT advice and support.

[134] Endpoints for secure messaging are organisational locations or business units that you require to be defined with their own identity for receiving and/or sending SMD-compliant messages. The HPI-O and related PKI certificate information for secure messaging is held in an Endpoint Location Service (ELS).

Appendix D: PCEHR Related Legislative Information

This appendix includes information relevant to legislation and rules for the eHealth record system that is referred to elsewhere in the User Guide.

D.1 Outline of the PCEHR Act 2012

The following information is extracted from the Act itself to provide a summary of its contents and intents. The full Act is available at:

http://www.comlaw.gov.au/Details/C2013C00295

Object of the Act

The object of this Act is to enable the establishment and operation of a voluntary national system for the provision of access to health information relating to consumers of healthcare, to:

a) help overcome the fragmentation of health information; and

b) improve the availability and quality of health information; and

c) reduce the occurrence of adverse medical events and the duplication of treatment; and

d) improve the coordination and quality of healthcare provided to consumers by different healthcare providers.

Simplified Outline of the Act

(1) This section provides a simplified outline of this Act.

(2) This Part contains definitions and other preliminary provisions. It defines key concepts, including:

a) the PCEHR system, which is an electronic system for collecting, using and disclosing certain information and involves the System Operator; and

b) the PCEHR of a consumer, which is constituted by a record created and maintained by the System Operator and information that can be obtained by means of that record; and

c) the entities that are participants in the PCEHR system.

(3) Part 2 is about the System Operator, the System Operator's functions, committees to advise the System Operator and the functions of the Chief Executive Medicare.

(4) Part 3 is about the registration by the System Operator of consumers, healthcare provider organisations, repository operators, portal operators and contracted service providers. Registration enables them to participate in the PCEHR system. It does so:

a) by authorising them to collect, use and disclose health information in specified circumstances; and

b) by imposing certain obligations on them to maintain the integrity of the PCEHR system.

(5) Division 1 of Part 4 provides for civil penalties for:

a) unauthorised collection, by means of the PCEHR system, of information included in a registered consumer's PCEHR; and

b) unauthorised use or disclosure of such information.

(6) Division 2 of Part 4 contains authorisations of various collections, uses and disclosures. The authorisations also have effect for the purposes of the Privacy Act 1988.

(7) Contraventions of this Act relating to health information included in a consumer's PCEHR can also be investigated under the Privacy Act 1988.

(8) Part 5 contains additional civil penalty provisions to maintain the integrity of the PCEHR system.

(9) Parts 6 and 7 support the civil penalty provisions and provide for enforceable undertakings and injunctions.

(10) Part 8 provides for general matters, including:

a) review of decisions; and

b) annual reports to be provided by the System Operator and the Information Commissioner; and

c) legislative instruments, including the PCEHR Rules.

D.2 PCEHR Rules Related to Written Policies

The following information is extracted from the Rules itself to highlight to the reader key sections relevant to the requirements for written policy and other matters related to security and access control, viz. 25, 26 and 27. The full Rules document is available at:

http://www.comlaw.gov.au/Details/F2012L01703

25. Healthcare provider organisation policies

(1) Healthcare provider organisations must have a written policy that reasonably addresses the matters specified in subrule (4).

(2) Healthcare provider organisations must communicate the policy mentioned in subrule (1), and ensure that the policy remains readily accessible, to all its employees and to any healthcare providers to whom the organisation supplies services under contract.

> *Example: A healthcare provider organisation that supplies information technology services to individual healthcare providers, via which those providers access the PCEHR system, must communicate the policy to the providers.*

(3) Healthcare provider organisations must enforce the policy mentioned in subrule (1) in relation to all its employees and any healthcare providers to whom the organisation supplies services under contract.

(4) Without limiting the matters a healthcare provider organisation's policy must reasonably address, the policy is, subject to subrule (5), to address the following:

a) the manner of authorising persons accessing the PCEHR system via or on behalf of the healthcare provider organisation, including the manner of suspending and deactivating the user account of any authorised person:

   i. who leaves the healthcare provider organisation;

   ii. whose security has been compromised; or

   iii. whose duties no longer require them to access the PCEHR system;

b) the training that will be provided before a person is authorised to access the PCEHR system, including in relation to how to use the PCEHR system accurately and responsibly, the legal obligations on healthcare provider organisations and individuals using the PCEHR system and the consequences of breaching those obligations;

c) the process for identifying a person who requests access to a consumer's PCEHR and communicating the person's identity to the System Operator so that the healthcare provider organisation is able to meet its obligations under section 74 of the Act;

d) the physical and information security measures that are to be established and adhered to by the healthcare provider organisation and people accessing the PCEHR system via or on behalf of the healthcare provider organisation, including the user account management measures that must be implemented under rule 27; and

e) mitigation strategies to ensure PCEHR-related security risks can be promptly identified, acted upon and reported to the healthcare provider organisation's management.

(5) If in the reasonable opinion of a healthcare provider organisation, a requirement in subrule (4) is not applicable to the organisation due to the limited size of the organisation, the organisation's policy need not address that requirement.

(6) Healthcare provider organisations must ensure that:

a) the policy mentioned in subrule (1) is:

i. drafted in such a manner that the organisation's performance can be audited against the policy to determine if the organisation has complied with the policy; and

ii. kept up-to-date;

b) each iteration of the policy contains a unique version number and the date when that iteration came into effect;

c) without limiting paragraph (6)(a)(ii) – the policy is reviewed at least annually and when any material new or changed risks are identified. The review must include consideration of:

i. factors that might result in:

A. unauthorised access to the PCEHR system using the healthcare provider organisation's information systems;

B. the misuse or unauthorised disclosure of information from a consumer's PCEHR by persons authorised to access the PCEHR system via or on behalf of the healthcare provider organisation; and

C. the accidental disclosure of information contained in a consumer's PCEHR;

ii. any changes to the PCEHR system that may affect the healthcare provider organisation; and

iii. any relevant legal or regulatory changes that have occurred since the last review; and

d) a record of each iteration of the policy mentioned in subrule (1) is retained in accordance with the record keeping obligations (if any) applicable to the healthcare provider organisation.

26. Policy to be provided to the System Operator on request

(1) The System Operator may request in writing that a healthcare provider organisation give it a copy of the policy mentioned in subrule 25(1).

(2) A healthcare provider organisation must comply with a request from the System Operator under this rule within 7 days of receiving the request.

(3) The System Operator may request a healthcare provider organisation's current policy or the policy that was in force on a specified date.

27. User account management within healthcare provider organisations

Healthcare provider organisations must ensure that their information technology systems, which are used by people to access the PCEHR system via or on behalf of the healthcare provider organisation, employ reasonable user account management practices including:

a) restricting access to those persons who require access as part of their duties;

b) uniquely identifying individuals using the healthcare provider organisation’s information technology systems, and having that unique identity protected by a password or equivalent protection mechanism;

c) having password and/or other access mechanisms that are sufficiently secure and robust given the security and privacy risks associated with unauthorised access to the PCEHR system;

d) ensuring that the user accounts of persons no longer authorised to access the PCEHR system via or on behalf of the healthcare provider organisation prevent access to the PCEHR system; and

e) suspending a user account that enables access to the PCEHR system as soon as practicable after becoming aware that the account or its password or access mechanism has been compromised.

Appendix E: Go Live Readiness Checklist Sample

The following checklist has been adapted from training material provided by NEHTA to Medicare Locals to assist them in supporting eHealth record system adoption in general practices. You may use it as is or adapt it for use in your medical practice. It broadly covers the following areas of Go Live readiness:

- Organisation readiness
- Application readiness
- User readiness
- Consumer readiness
- Go Live day support activities
- Authorisation processes
- Going Live!

Your Medicare Local and/or other organisations supporting your practice in eHealth may also be able to provide similar checklists.

No	Activity	Complete?
1.	Has the HI Service registration been completed for HPI-O, RO and OMO individuals?	Y/N
2.	Do the individuals and organisations have a PKI certificate for access to the HI Service (including the HPD)?	Y/N
3.	Has the Seed (and Network Organisation if applicable) structure been set up in the HI Service?	Y/N
4.	Have the HPI-O details been published to the Healthcare Provider Directory (HPD)?	Y/N
5.	Have the individual providers with a HPI-I in your practice consented to having their information published in the HPD?	Y/N
6.	Are the HPI-Is linked to your organisation Seed (and Network if applicable) structure in the HI Service (using HPOS) and in the HPD?	Y/N
7.	Have you developed appropriate policies to conform to the PCEHR Rules, and any associated procedures your practice wishes to enforce?	Y/N

No	Activity	Complete?
8.	Has the PCEHR Registration been completed and Participation Agreement signed?	Y/N
9.	If applicable, have the required Access Flags been established in your Seed and Network structure?	Y/N
10.	Have you obtained the NASH Organisation PKI certificate for the practice (for the eHealth record system and SMD)?	Y/N
11.	Where necessary for Provider Portal Access, have the individual healthcare providers obtained a NASH PKI certificate for Individual Healthcare Providers?	Y/N
12.	Where necessary for Provider Portal Access, have the appropriate HPI-I users been linked to your HPI-O structure via HPOS or completion of the PCEHR Authorisation Link form?	Y/N
13.	Has the new software been configured to enable appropriate access? This may include unique log on, user group/role access and security password functions?	Y/N
14.	Have you installed/configured the software with appropriate PKI certificates to undertake access to HI Service and PCEHR System functions?	Y/N
15.	Has the software been tested to your satisfaction?	Y/N
16.	Are the user guides, cheat sheets and reference material easily available for users?	Y/N
17.	Have all staff (clinicians and end users) been trained in software functionality for safe and accurate access to HI Service and PCEHR?	Y/N
18.	Have all staff been made aware of their responsibilities as per the Acts for them accessing the HI Service and PCEHR?	Y/N
19.	Have all staff (clinicians and end users) who will access the PCEHR been trained on the new PCEHR policies and procedures?	Y/N
20.	If applicable, have all (clinicians and end users) undertaking consumer registration been trained on the evidence of identity processes being used by the practice, and in the Assisted Registration processes?	Y/N
21.	Have all staff (clinicians and end users) been trained in process of how to notify errors to the Vendors/PCEHR System Operator/HI Service Operator?	Y/N
22.	Have patients/consumers been identified who may benefit from the practice's use of eHealth?	Y/N

No	Activity	Complete?
23.	Is there consumer support material (registration information/brochures/videos) available in the waiting room?	Y/N
24.	Is there a ‘trained guide’ on board for the go live week to assist consumers in the waiting room?	Y/N
25.	Has a ‘go live day plan’ been set identifying resources and activities to be supported for the day?	Y/N
26.	Are there sufficient resources available /planned to support go-live? Including additional staff, guides, prompts and contact lists?	Y/N
27.	Have communications been ramped up as the approach to the go-live approaches? Is everyone aware of the activity and knows where to get help if needed?	Y/N
28.	Is there a fail over plan and business continuity plan in place to restore Business As Usual should issues arise on the day?	Y/N
29.	Are the mechanisms for capturing issues with the go live process in place?	Y/N
30.	Is there a support process in place to deal with any technical problems? Are the helpdesk and support contact numbers available?	Y/N
31.	Is there clear delegation of authority and an active approval process for go live based on sign off of all go live criteria?	Y/N
32.	Has approval for go live been given?	Y/N

Appendix F: Sample Form for Reporting eHealth–related Clinical Incidents

The following form, reproduced with the permission of AMLA, can be used to document eHealth-related clinical incidents and for reporting them, as discussed in Section **7.3**.

Incident Report Form			
Date of incident:	____ / ____ / ____	**Time of incident**	___________am/pm
Location: (Include address, where applicable.)			
Name of person completing form:			
Position of person completing form:		**Contact number:**	
Employees, Volunteers or Directors involved in incident:			
Name:		**Contact number:**	
Clients or community members involved in incident:			
Name:		**Contact number:**	
1.			
Description of incident and background: (Include all relevant circumstances and information leading up to the incident, whether the incident was witnessed, and any other relevant issues.)			
____ ____			

Incident Report Form

____

____

____

____

Who was informed of the incident?

(For example, CEO, manager, Vendor, NEHTA DHS/Medicare and so on.)

1.	

Actions taken to date:

(Including date and time of contact, contact number, and other contact numbers of agencies or people who were informed, as well details of support provided.)

1.

Follow up actions planned:

1.

Critical Incident Report Form authorised by:

____
(Signature of employee)

Date: ____ / ____ / ____

____
(Signature of manager)

Date: ____ / ____ / ____

This page intentionally blank