



My Health Record Guidelines for Pharmacists



Australian Government
Australian Digital Health Agency



My Health Record

PSA Australia's peak body for pharmacists



© Pharmaceutical Society of Australia Ltd., 2019

These guidelines contain material that has been provided by the Pharmaceutical Society of Australia (PSA), and may contain material provided by the Commonwealth and third parties. Copyright in material provided by the Commonwealth or third parties belongs to them. The PSA owns the copyright in these guidelines as a whole and all material in the guidelines that has been developed by PSA. In relation to PSA-owned material, no part may be reproduced by any process except in accordance with the provisions of the Copyright Act 1968 (Cth) or the written permission of PSA. Requests and inquiries regarding permission to use PSA material should be addressed to: Pharmaceutical Society of Australia, PO Box 42, Deakin West ACT 2600. Where you would like to use material that has been provided by the Commonwealth or third parties, contact them directly.

ISBN-13: 978-0-908185-18-4

Title: My Health Record Guidelines for Pharmacists

Date of publication: June 2019

Date of endorsement by PSA Board: June 2019

Publisher: Pharmaceutical Society of Australia

Digital 978-0-908185-06-1

Contents

Executive summary	4
Acknowledgements	4
Introduction	5
Terminology	6
About My Health Record	9
System architecture	10
Healthcare identifiers	10
Legislation	10
Privacy	11
Consent	11
Governance	13
Policies and procedures	13
Quality assurance	15
My Health Record and the pharmacist	16
Access to My Health Record	16
Access by non-pharmacist staff	17
Pharmacy workflow considerations	17
Viewing records	17
Documents in My Health Record	18
Medicines Information View	20
Prescription and Dispense View	20
Contributing clinical information	20
Dispensing information	21
Pharmacist Shared Medicines List	22
Event Summaries	22
Editing or deleting clinical documents	22
Standards of documentation	22
Access history	23
My Health Record and the patient	24
Patient control	24
Patient support	24
Health literacy and e-health literacy	25
Appendix 1: Accessing My Health Record via conformant software	26
Appendix 2: Accessing My Health Record via the National Provider Portal	27
Appendix 3: My Health Record security and access policy	28
Appendix 4: Sensitive information	31
Appendix 5: My Health Record decision tool—appropriate access scenarios	32
Appendix 6: Standards of documentation	33
References	35

Executive summary

The My Health Record system provides online access to an individual's key health information, including medicines, allergies, medical conditions and pathology results, and supports improvements in the safety, quality and efficiency of Australia's healthcare system.¹

The need to create a repository to consolidate patient health information has come about in part because of increasing volumes of patient health data, which are often held in a number of different locations by different healthcare providers. Timely access to health information is essential to promote continuity of patient care and improve health outcomes.

Following the My Health Record opt-out period, records have been created for all Australians, except for those who chose not to have one. The My Health Record system will support timely access to important health information by individuals (and their carers, where appropriate) and their healthcare providers. The ability for pharmacists to contribute patient health information (e.g. dispense records, immunisation records) to My Health Record may improve communication with other healthcare providers caring for their patients and improve health outcomes.

These guidelines provide information and guidance to pharmacists on the appropriate use of the My Health Record system, including:

- privacy and patient consent
- pharmacists' responsibilities and obligations
- accessing clinical information
- contributing clinical information
- patient support.

These guidelines do not replace the need for pharmacists to exercise professional discretion and judgement when using the My Health Record system. The guidelines do not include clinical information or detailed legislative requirements. At all times, pharmacists using the My Health Record system must comply with all relevant Commonwealth, state and territory legislation, as well as program-specific standards, codes and rules.

Acknowledgements

Development of *My Health Record Guidelines for Pharmacists* has been funded by the Australian Digital Health Agency.

The work to update the guidelines has included review by experts, stakeholder feedback, and the consensus of organisations and individuals involved.

The Pharmaceutical Society of Australia (PSA) thanks all those involved in the review process and, in particular, gratefully acknowledges the contribution of the following individuals and organisations.

Project Advisory Group

Sam Keitaanpaa, Chair
Richard Brightwell, Consumers Health Forum
Helen Dowling, Medicines Safety Program Steering Group
David Freemantle, Medical Software Industry Association
Allan Groth, Indigenous Allied Health Australia
Dr Steve Hambleton, Medicines Safety Program Steering Group
Grant Martin, Australian Association of Consultant Pharmacy
Andrew Matthews, Australian Digital Health Agency
Jarrod McMaugh, Pharmaceutical Society of Australia
Vincent O'Sullivan, Pharmacy Guild of Australia
Mike Stephens, National Aboriginal Community Controlled Health Organisation
Ben Wilkins, Pharmacy Board of Australia
Gilbert Yeates, Pharmaceutical Defence Limited
Jerry Yik, Society of Hospital Pharmacists of Australia

Project Team

Jan Ridd
Emma Abate
Daniela Gagliardi
Tracy Leung
Peter Guthrey



Introduction

The My Health Record system has been designed to allow the secure sharing of patient health information via an online platform.²

For the pharmacist, greater access to patient health information in this way may:

- enable more efficient and effective medication reconciliation
- enhance the pharmacist's contribution to the quality use of medicines
- improve continuity of patient care.

A pharmacist's contribution to medication safety and quality use of medicines will be enhanced by their ability to access a patient's My Health Record. Access to health information will allow pharmacists to deliver more effective and efficient care. Dispensing information, immunisation records, Event

Summaries (e.g. allergies) and Pharmacist Shared Medicines Lists that are contributed to patient records by pharmacists will facilitate meaningful clinical engagement with other healthcare providers.

Pharmacists have a professional responsibility to review their practice and integrate the use of the My Health Record system into patient care, where appropriate. Pharmacists are encouraged to use communication tools to advise their patients of their use of, or decision not to use, the My Health Record system.

Terminology

Table 1 provides definitions of terms used in the guidelines.

Table 1. Guideline terms, definitions and equivalent terms

Term	Definition	Source
Access history	An audit trail of all activity related to a patient's My Health Record, detailing when it was accessed and when a document was changed or removed	3
Accredited continuing professional development (CPD) organisation	An organisation able to accredit CPD activities for pharmacists under the auspices of the Australian Pharmacy Council. Includes Australian College of Pharmacy, Pharmacy Guild of Australia, Pharmaceutical Society of Australia, Society of Hospital Pharmacists of Australia and NPS MedicineWise	4
Adverse drug reaction	A drug response that is noxious and unintended, and occurs at doses normally used or tested in humans for the prophylaxis, diagnosis or therapy of disease, or for the modification of physiological function	5
Authorised representative	A person who can act on behalf of another person for the purposes of the My Health Record system. This could be for the person's child aged less than 14 years, or for an adult who lacks the capacity to manage their own record. An authorised representative may be a parent, carer, family member, legal guardian or someone with enduring power of attorney. An individual may have more than one authorised representative	Adapted from 3
Clinical incident	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. A clinical incident can be related to safety, usability, technical, privacy or security issues <i>For the purpose of these guidelines, guidance on clinical incidents and their management is limited to incidents directly associated with the My Health Record system. In the context of the My Health Record system, a clinical incident may relate to the system directly, or the behaviour of clinical software when interacting with the My Health Record system</i>	6
Clinical information system	A system used by a healthcare provider to manage patient and practice records. It may include a software component connected to the My Health Record system (e.g. pharmacy dispensing software)	3
Conformant software	Dispensing or other clinical software capable of interacting with the My Health Record system	7
Delegate	A non-clinical support worker (e.g. pharmacy technician) who has been granted access to the My Health Record system by a healthcare provider with an HPI-I (see Healthcare Provider Identifier—Individual [HPI-I], below), according to the healthcare organisation's My Health Record security and access policy	7
E-health literacy	Ability of people to use information and communication technologies to improve or enable health and health care	8
Event Summary	A clinical document that may be uploaded to a patient's My Health Record summarising one or more episodes of care	3
Health literacy	Skills, knowledge, motivation and capacity of a person to access, understand, appraise and apply information to make effective decisions about health and health care, and take appropriate action	9
Healthcare Identifiers Service (HI Service)	National system for uniquely identifying healthcare providers and individuals, which makes sure the right health information is associated with the right individual	3
Health Professional Online Services (HPOS)	A service provided by the Australian Government Department of Human Services to health professionals through a secure online channel. HPOS offers a range of services, including managing My Health Record registration and the ability for an HPI-O (see Healthcare Provider Identifier—Organisation [HPI-O], below) to link to a contracted service provider	3
Healthcare provider	A practitioner who provides services to individuals or communities to promote, maintain, monitor or restore health (such as a pharmacist, general practitioner, dentist, nurse, physiotherapist or case worker) Equivalent terms: health professional, healthcare practitioner, healthcare professional	5
Healthcare Provider Identifier—Individual (HPI-I)	A unique 16-digit number used to identify individual healthcare providers who deliver health care in the Australian healthcare setting	3
Healthcare Provider Identifier—Organisation (HPI-O)	A unique 16-digit number used to identify organisations that deliver health care in the Australian healthcare setting	3

Term	Definition	Source
Healthcare provider organisation	An entity, or a part of an entity, that has conducted, conducts, or will conduct, an enterprise that provides health care (e.g. community pharmacy, accredited pharmacist)	3
Home medicines review (HMR)	A systematic assessment of a patient's medications and the management of those medications by an accredited pharmacist in a community setting, with the aim of optimising consumer health outcomes and identifying potential medication-related issues to improve the quality use of medicines	10
Individual Healthcare Identifier (IHI)	A unique 16-digit number used to identify individuals who receive, or may receive, health care in the Australian healthcare setting	3
MedsCheck	A structured and collaborative clinical pharmacy service that takes place in the pharmacy to optimise the impact of medicines on patient health outcomes. It involves a review of patient medicines, a face-to-face consultation between the pharmacist and patient, development of a medication profile and an action plan, and a follow-up consultation	11
My Health Record	An electronic record of an individual's health information maintained by the Australian Government. My Health Record was formerly known as Personally Controlled Electronic Health Record (PCEHR)	3
My Health Record system	A system of managing health information online that will make it more accessible to Australians (except for those who indicate that they do not want a My Health Record) and healthcare providers	3
NASH PKI certificate	National Authentication Service for Health (NASH) is a secure and authenticated service for healthcare provider organisations and personnel to exchange sensitive My Health Record information. The service issues digital credentials, including digital certificates managed through the Public Key Infrastructure (PKI). The digital certificate authenticates a healthcare provider organisation to access the My Health Record system using conformant clinical software or securely share health information using software that meets Secure Message Delivery requirements	3
National Provider Portal (NPP)	A view-only, web-based interface through which healthcare provider organisations can access the My Health Record system without having to use a conformant clinical information system (e.g. dispensing software)	12
Network organisation	A healthcare provider organisation with an HPI-O (see Healthcare Provider Identifier—Organisation [HPI-O], above) that is part of a network hierarchy. A network organisation may be set up to work under a seed organisation. An HPI-O is assigned to the seed organisation. Network organisations can be used to represent different departments, sections or divisions within an organisation (e.g. departments within a hospital), or can be separate legal entities from the seed organisation	3
Nominated representative	A representative who is provided access to a My Health Record by the individual or the individual's authorised representative. A nominated representative can view the individual's health information. A nominated representative with read-only access is not required to provide any evidence of identity to the System Operator	3
Office of the Australian Information Commissioner (OAIC)	Key regulator for the My Health Record system that has the capacity to conduct audits, commence investigations, impose sanctions and accept enforceable undertakings	13
Organisation Maintenance Officer (OMO)	A person who undertakes the day-to-day administrative tasks in relation to the HI Service and the My Health Record system. An OMO needs to be someone who is familiar with the IT system used by the organisation. The OMO is responsible for understanding, implementing and compliance monitoring of the My Health Record security and access policy, and for maintaining the policy on behalf of the organisation. A healthcare provider organisation can have multiple OMOs	3
Patient	A person who uses, or is a potential user of, health services, including their family and carer(s) or agent Equivalent terms: consumer, healthcare recipient, client	5
Pharmacist	A provisionally or generally registered practising pharmacist registered with the Pharmacy Board of Australia within the Australian Health Practitioner Regulation Agency Equivalent terms: intern pharmacist, registered pharmacist	14
Pharmacist Shared Medicines List (PSML)	A list of reconciled medicines that the consumer was known to be taking at the time the list was created by a pharmacist. Medication reconciliation is a formal process of verifying a patient's medicines to obtain a complete and accurate list of their current medicines	15
Pharmacy organisation	Organisation or business providing pharmaceutical services to patients Equivalent terms: community pharmacy, pharmacy department, pharmacy business (e.g. accredited pharmacist)	7
Point of care	The location where care is provided (e.g. ambulance, general practice, patient's home, hospital, pharmacy)	16

Term	Definition	Source
Prescriber	A healthcare provider authorised to undertake prescribing within the scope of their practice Equivalent terms: doctor, dentist, general practitioner (GP), nurse practitioner, optometrist, other approved prescribers, specialist	17
Provider digital access (PRODA)	A method of authentication to provide users with access to government services online. This includes allowing a healthcare provider with an HPI-I (see Healthcare Provider Identifier—Individual [HPI-I], above) to access the My Health Record National Provider Portal for read-only purposes	3
Residential medication management review (RMMR)	A comprehensive medication review conducted in an aged care facility by an accredited pharmacist. It is resident focused, involving a systematic evaluation of the resident's complete medication regimen and management of that medicine	18
Responsible Officer (RO)	A person who has legal responsibility for understanding of, and compliance with, the My Health Record security and access policy and compliance with My Health Record legislation (e.g. pharmacy owner, pharmacist manager)	3
Seed organisation	A healthcare provider organisation with an HPI-O (see Healthcare Provider Identifier—Organisation [HPI-O], above) that is a legal entity and is the head of a network hierarchy, which may or may not include subordinate network organisations	3
Sensitive information	A particular type of personal information that, if disclosed or handled inappropriately, can leave an individual vulnerable to discrimination, mistreatment, humiliation or embarrassment. This includes health information about the person (e.g. genetic information, biometric information)	19
System Operator (SO)	The participant with responsibility for establishing and operating the My Health Record system. The System Operator is currently the Australian Digital Health Agency	3

About My Health Record

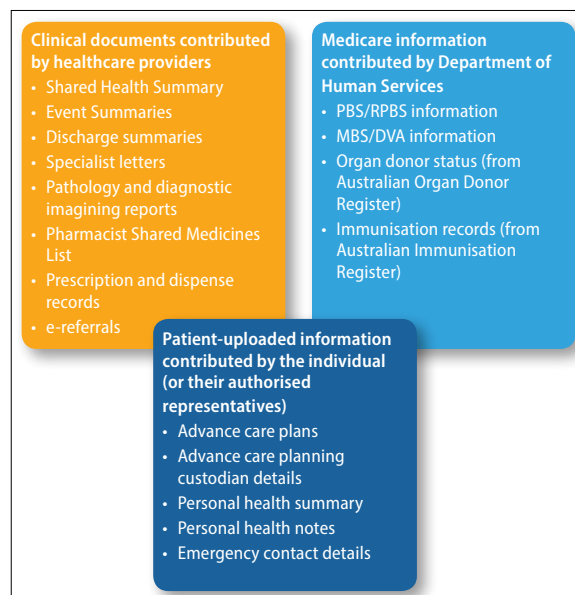
My Health Record is an electronic summary of an individual's key health information, contributed from their existing records and designed to be integrated into existing local clinical information systems.²⁰

Pharmacists can access a range of clinical information in a patient's My Health Record, including information about medicines, allergies and current medical conditions. Figure 1 outlines the clinical information sources contained in a My Health Record that pharmacists can use to provide patient care.

However, My Health Record should not be assumed to be a complete record, because it is a patient-controlled record, and not all healthcare providers use the My Health Record system or upload every clinical patient interaction.

Healthcare providers can upload different clinical documents to a patient's My Health Record (see Figure 2).

Figure 1. Clinical information sources for a My Health Record, as of May 2019



Reference: Australian Digital Health Agency¹

Figure 2. Documents that can be uploaded to a My Health Record



Reference: Australian Digital Health Agency²¹

System architecture

The My Health Record system is a national framework that enables key health information to be accessed by an individual and their healthcare providers.

The system has been designed to²²:

- allow patients to control the content of their record, including which healthcare provider organisations can access the record
- enable healthcare providers to access the patient's key health information, when internet connectivity allows, including at the point of care
- protect patient privacy by restricting access to healthcare providers (or delegates) who are authorised by their healthcare organisation, and who are providing health care to the patient. Patients can also opt to restrict access to specific documents or their entire My Health Record (see *Patient control*).

The My Health Record system does not replace direct sharing of health information (i.e. in person or via telephone) between healthcare providers or with patients. Information from a patient's My Health Record should be integrated with other information available to the pharmacist. The My Health Record should not be relied upon as the only source of patient health information.

Healthcare identifiers

The Healthcare Identifiers Service (HI Service) is a national system for uniquely identifying healthcare providers, healthcare organisations and patients receiving health care.³

To ensure the security of the information contained in the My Health Record system, organisations must register with the HI Service and obtain digital credentials (i.e. NASH PKI certificates) before accessing the My Health Record system. These certificates authenticate the identity of the organisation and registered healthcare providers (e.g. pharmacists) accessing the service²³ (see Appendix 1). Appendix 2 outlines the registration process to access the My Health Record system via the National Provider Portal.

Any access to a patient's My Health Record is linked to three healthcare identifiers (unique 16-digit numbers) that are allocated and managed by the HI Service²⁴:

- Healthcare Provider Identifier—Individual (HPI-I) for an individual (e.g. a pharmacist)
- Healthcare Provider Identifier—Organisation (HPI-O) for an organisation delivering health care (e.g. pharmacy or pharmacy department, general practice pharmacist or accredited pharmacist who holds an Australian Business Number)
- IHI—Individual Healthcare Identifier for a patient.

Healthcare identifiers can only be used for the purposes described in the *Healthcare Identifiers Act 2010* and *Healthcare Identifiers Regulations 2010*. These purposes

include communicating and managing health care, and cover documents and processes such as electronic referrals, discharge summaries and medication management.²⁴

Legislation

Interaction with the My Health Record system is protected by legislation and security mechanisms. The system is designed to uphold the highest grade of security and adheres to the Australian Government security frameworks.²⁵

Pharmacists using the system must comply with obligations outlined in the relevant legislation (see Box 1).^{26,27}

Box 1. My Health Record and related legislation

My Health Records Act 2012 establishes:

- the role and functions of the System Operator
- a registration framework for individuals, and entities such as healthcare provider organisations to participate in the system
- a privacy framework (aligned with the *Privacy Act 1988*) specifying which healthcare provider organisations can access and use information in the system, and the penalties that can be imposed for improper use of the information.

My Health Records Rule 2016 specifies the privacy and security requirements that healthcare provider organisations must comply with to be eligible to be registered, and to remain registered, under the My Health Record system.

My Health Records Regulation 2012 specifies additional information (e.g. identifying information and privacy laws) that continue to apply to the disclosure of sensitive information.

Healthcare Identifiers Act 2010 establishes the Healthcare Identifiers Service and regulates related matters.

Healthcare Identifiers Regulations 2010 provides additional detail and requirements regarding the operation of the Healthcare Identifiers Service.

Reference: Australian Digital Health Agency^{26,27}

Commonwealth, state and territory legislation forms the foundation on which pharmacist practice is based. Pharmacists must fulfil legal obligations at all times, and no part of these guidelines may be interpreted as permitting a breach of the law or discouraging compliance with legal requirements. If conflict arises between the legislation and these guidelines, legislative requirements must be adhered to.

The Pharmacy Board of Australia's *Code of Conduct for Pharmacists* also makes reference to the pharmacist's responsibilities in maintaining patients' health records. This may be applicable to use of the My Health Record system.

Pharmacy organisations must ensure that relevant policies and procedures are in place to inform the use of the My Health Record system by employees (see *Policies and procedures*).

Privacy

Patient privacy must be upheld by any pharmacist or authorised pharmacy staff member accessing the My Health Record system. All information in a patient's My Health Record is managed and protected in accordance with the *My Health Records Act 2012* and the *Privacy Act 1988*.²⁸ All patient information must also be managed in accordance with the *PSA Professional Practice Standards*, Standard 1: Fundamental Pharmacy Practice.⁵ Pharmacy organisations must have a privacy policy in place (see Appendix 3).

Data security design features of the My Health Record system include access histories, technology and data management controls, and security measures to minimise the likelihood of unauthorised access to information in a patient's record.²⁵

All patient health information, including information accessed from a patient's My Health Record, must be kept confidential and secure. Patient consent should be obtained before patient health information is disclosed to a carer or agent collecting a medicine on behalf of a patient.²⁹

For further information about privacy, see *Handling information in a My Health Record* by the Office of the Australian Information Commissioner (OAIC).

Consent

The legislative framework governing the My Health Record system allows a healthcare provider in a participating organisation to use or upload clinical information in a patient's My Health Record without obtaining consent from the individual, on the condition that they are providing care to that patient. There is also no requirement for a patient to review clinical information before it is uploaded.³⁰

The *My Health Records Act 2012* defines the term 'use' of health information in a My Health Record as:

- accessing the information
- viewing the information
- modifying the information
- deleting the information.

If the patient has registered for a My Health Record, they will have provided consent for registered healthcare providers involved in their care to access and upload information to their My Health Record.

Alternatively, if the patient has had a My Health Record created for them (e.g. as part of the transition to the opt-out participation model), the *My Health Records Act 2012* authorises registered healthcare providers involved in their care to access and upload information to their My Health Record.

This is subject to two important exceptions²⁸:

- A patient has asked that all records, a particular record or a specific class of records not be uploaded.

Prescribed state or territory law prohibits healthcare provider organisations from uploading the patient's record, or including particular information in a record without consent (see *Sensitive information*).

Regardless of consent requirements, it is good practice to advise patients how the pharmacy intends to interact with the My Health Record system and when it will upload information to their My Health Record (e.g. using communication tools to indicate that all dispense records will be uploaded to the patient's My Health Record unless the patient requests otherwise).

It is important to note that Pharmaceutical Benefits Scheme (PBS) and Repatriation Pharmaceutical Benefits Scheme (RPBS) claim information is automatically uploaded into a patient's My Health Record by Medicare, independent of pharmacies' dispense record upload. Box 2 provides information on how to manage Medicare information when patient consent is withdrawn.

Box 2. Managing Medicare information when a patient withdraws consent

PBS and RPBS claim information is uploaded into a patient's My Health Record by Medicare as a Medicare billing document. It does not contain the dosage instructions associated with a prescription. PBS and RPBS information is uploaded after pharmacy claims have been submitted for payment. Information may take up to 6 weeks to be uploaded to a patient's My Health Record.²⁰

Should a patient request that a dispense record not be uploaded, the pharmacist must comply with that request. It may be considered best practice to inform the patient that they will need to remove the corresponding PBS/RPBS entry themselves via the Consumer Portal.³¹

Sensitive information

Some existing state or territory legislation prohibits the disclosure of sensitive information (e.g. information relating to notifiable conditions, such as AIDS or HIV status) without the express consent^a of the individual.²⁸

Pharmacists should refer to state or territory legislation for further information about specific patient consent requirements before uploading dispense records to a patient's My Health Record (see Appendix 4), or contact their state or territory health department for specific guidance on jurisdictional requirements.

Some patients may have reservations about potentially sensitive information being uploaded to their My Health Record. For example, use of psychotropic medicines, antimicrobials for sexually transmissible infections or medicines for sexual dysfunction may be considered as sensitive by a patient. Pharmacists should proactively discuss particular sensitive information with the patient so that the patient can make an informed decision.

a Express consent is given explicitly, either orally or in writing. This could include a handwritten signature or an oral statement (such as a verbal agreement). Express consent can be withdrawn at any time.³⁸

Emergency situations

In certain emergency situations (e.g. the patient is unconscious), a pharmacist or their participating healthcare provider organisation is permitted to collect, use or disclose information in the patient's My Health Record if³²:

- it is unreasonable or impracticable to obtain consent from the patient or their authorised representative; and
- they reasonably believe that access to information in the My Health Record is necessary to lessen or prevent a serious threat to the patient or another individual's life, health or safety; or
- they reasonably believe that access to information in the My Health Record is necessary to lessen or prevent a serious threat to public health or safety.

In such situations, healthcare providers may use emergency access to bypass any access controls that have been set by the patient for their My Health Record.

Emergency access only needs to be invoked if the patient has set controls other than the default controls.

Emergency access provides the organisation with unrestricted access to the patient's My Health Record for 5 days. Under emergency access, all information in a My Health Record can be accessed, except for³²:

- records that have been effectively removed (i.e. permanently deleted) by the patient (this information can no longer be viewed, even in an emergency)
- information entered in the consumer-only notes section.

Unlawful use of the emergency access function is subject to civil and/or criminal penalties under the *My Health Records Act 2012*.

A healthcare provider **must not** use emergency access³²:

- to view their own My Health Record or a record of a family member
- to demonstrate how to use the emergency access function
- when a patient has forgotten the access code they have set^b (except where there is a serious threat to the person's life, health or safety)
- to check whether any restricted documents exist (except where there is a serious threat to the individual's life, health or safety and they are unable to provide consent, or to lessen or prevent a serious threat to public health or safety).

Emergency access is recorded in the access history of the My Health Record, which can be viewed by the patient and the System Operator. The patient can choose to be notified when anyone gains emergency access to their My Health Record.³² The System Operator audits use of the emergency access regularly and can request more information about the circumstances related to its use.³³ If a pharmacy organisation accesses a patient's My Health Record under these circumstances, details of the access should be recorded in the patient's local history (e.g. the patient's profile in the dispensing software or pharmacy record).

^b If a patient has forgotten the access code, they can contact the My Health Record helpline (1800 723 471) for assistance.

Using emergency access

Brendan, a 58-year-old male, has a seizure in Jin's pharmacy while on holiday. Brendan's travelling companions are not familiar with his medical history. While waiting for the ambulance, Jin is able to verify that Brendan has a My Health Record, but there is an access code on his record.

Since it is impractical to obtain consent from either Brendan or an authorised representative, Jin employs emergency access to view Brendan's record once the ambulance has been called. Upon accessing Brendan's My Health Record, Jin confirms that Brendan has type 1 diabetes, enabling the paramedics to treat Brendan for hypoglycaemia on their arrival.

Jin documents the details related to the emergency access in Brendan's profile in the dispensing software to ensure that sufficient information can be provided to the System Operator on request.

Authorised representatives

An authorised representative is a person who can act on behalf of another person for the purposes of the My Health Record system. This could be for their child aged less than 14 years, or for an adult who lacks the capacity to manage their own record.³⁴ An authorised representative may be a parent, carer, family member, legal guardian or someone with enduring power of attorney. However, if there is no-one with parental responsibility or legal authority, a person who is otherwise appropriate to act on behalf of the individual can be an authorised representative. An individual may have more than one authorised representative.³⁵

Authorised representatives can access, view and update the information in the individual's My Health Record, as well as add or remove nominated representatives. This control includes the ability to restrict which healthcare provider organisations have access to the record and which clinical documents they can see.³⁴

State or territory agencies or ministers can act as authorised representatives for children for whom they have parental or legal authority. This enables them to manage the record on behalf of an individual to support better health outcomes.³⁶

My Health Record and young people

Once an individual turns 14, they are permitted to manage their own My Health Record, and their parents or legal guardians are automatically removed as authorised representatives. If the individual would like their parents or legal guardians to continue to have access to their My Health Record, they can invite them to become nominated representatives. The individual can decide the level of access they give to their nominated representative(s).³⁷

If a young person does not take control of their My Health Record from the age of 14, clinical documents such as dispense records can still be uploaded and accessed, but the flow of Medicare information—including Medical Benefits Schedule (MBS), PBS and Australian Immunisation Register information—will be suspended. Once the person turns 18 and their My Health Record is accessed by a healthcare

provider or the individual, the flow of Medicare information will resume. Up to 2 years of MBS, PBS and Australian Organ Donor Register data, and all information from the Australian Immunisation Register will be transferred into the My Health Record.³⁸

Pharmacists should place the interests and wellbeing of the young person first when providing care to this age group.²⁹ Box 3 provides more information on considerations for care provision for young people with a My Health Record.

Box 3. Considerations when providing care to young people with a My Health Record

A young person's My Health Record does not indicate whether they have taken control of their record or have a nominated representative to manage their record. Therefore, pharmacists should:

- exercise professional judgement and consider other sources of clinical information when providing patient care under these circumstances (see *Viewing records*)
- take additional care in maintaining the privacy and confidentiality of patients in this age group (see *Privacy*)
- understand a young person's healthcare needs—for example, provide additional information and support when clinically appropriate.

Governance

Policies and procedures

As per the My Health Records Rule 2016, pharmacy organisations must have established policies and procedures to govern their use of the My Health Record system. The Responsible Officer (RO) and Organisation Maintenance Officer (OMO) are responsible for overseeing the implementation and use of the My Health Record system by the organisation, including compliance with policies and procedures.

Policies and procedures must meet legislative requirements and relevant professional practice standards. All My Health Record policies and procedures must be regularly reviewed and updated as required, as part of quality assurance and evaluation processes (see *Quality assurance*).

Pharmacy organisations should also be aware of resources that may assist in the safe and effective implementation and use of the My Health Record system, including the Australian Commission on Safety and Quality in Health Care *Electronic Medication Management Systems: a Guide to Safe Implementation* (3rd edition), *National Guidelines for On-Screen Display of Medicines Information* (2017) and *National Guidelines for On-Screen Presentation of Discharge Summaries* (2017).

Security and access

The My Health Records Rule 2016 sets out the privacy and security requirements that healthcare organisations must comply with to be eligible to be registered, and to remain registered, under the My Health Record system.³⁹

Under the Rule, pharmacy organisations must develop and maintain a robust security and access policy. See Appendix 3 for a template for a My Health Record security and access policy.

A My Health Record security and access policy should outline:

- My Health Record access and security procedures for the organisation
- how authorised people access the system
- training delivered to staff before they can access the My Health Record system
- physical and information security measures used by the organisation.

Organisations must review, update, maintain, enforce and promote to staff the policies that ensure that the My Health Record system is used safely and responsibly.

Pharmacy organisations have a responsibility to ensure that data security is considered, appropriate advice is sought and the necessary action is taken to minimise misuse of the My Health Record system. Ways to improve data security include the following:

- Screensaver mode is automatically activated when a computer desktop is inactive for more than 1 minute.
- Computer software is password protected.
- Strong and unique individual passwords are used, and changed regularly (e.g. every 3–6 months).
- Passwords are not shared with other staff (as per confidentiality and privacy policy).
- Administrative privileges in pharmacy dispensing software are restricted to designated staff (e.g. pharmacy manager), as per pharmacy policy.

There are penalties for the misuse (e.g. inappropriate collection of patient data, disclosure of patient data) of any information contained in a patient's My Health Record.⁴⁰

The following resources provide further information on cybersecurity, such as protecting computers, securing servers and common online threats:

- *Information Security Guide for Small Healthcare Businesses*
- *Security Behaviours: Encouraging Everyone to be Aware of Information Security*.

Managing clinical incidents

The pharmacy organisation's My Health Record security and access policy should include processes for managing clinical incidents related to use of the My Health Record system, according to the nature of the incident.

Pharmacists should follow the process for managing such clinical incidents documented in the organisation's My Health Record security and access policy. Some clinical incidents associated with use of the My Health Record system can be managed locally by the organisation. Pharmacists should consider the need to notify their professional indemnity insurer following a clinical incident. However, in the case of a data breach, the pharmacy organisation will need to notify a relevant third party, such as the System Operator, police or the OAIC (see Table 2).

The *My Health Records Act 2012* describes a My Health Record–related data breach as⁴¹:

- the unauthorised collection, use or disclosure of health information in an individual's My Health Record
- a) an event that has, or may have, occurred or b) any circumstances have, or may have, arisen that compromise, may compromise, have compromised or may have compromised, the security or integrity of the My Health Record system (whether or not involving a contravention of the *My Health Records Act 2012*).

For more information on data breach notification, refer to:

- the OAIC *Guide to Mandatory Data Breach Notification in the My Health Record System*
- the My Health Record website at: www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/data-breach-notification-steps

Pharmacists should review their policies and procedures to address factors contributing to clinical incidents as part of a quality assurance and improvement process. For further information, see Appendix 3.

Table 2. Managing clinical incidents

Incident	Action
Error in a document (e.g. dispense record) uploaded to a patient's My Health Record	<p>If you made the error:</p> <ol style="list-style-type: none"> 1. Delete the incorrect document (e.g. dispense record) from your dispensing system immediately and re-dispense 2. Upload the new, correct version 3. Record all actions in your own notes <p>If you are unable to delete the erroneous document, contact the System Operator via the My Health Record helpline (1800 723 471)</p> <p>Note: These actions relate to correcting dispensing errors in a patient's My Health Record. Appropriate follow-up, including replacing any incorrect medicine, referring the patient to the prescriber where necessary and notifying your indemnity insurer, must also occur as a priority</p> <p>If another healthcare provider made the error:</p> <ol style="list-style-type: none"> 1. Contact the patient and inform them that you have identified an error in their My Health Record 2. Encourage the patient to exercise their right to have the error corrected by the healthcare provider who uploaded the information, or offer to follow up with the healthcare provider yourself 3. Notify the System Operator via the My Health Record helpline (1800 723 471), if the healthcare provider cannot be contacted 4. Record your actions in your own notes
Upload of a document (e.g. dispense record) to a patient's My Health Record if consent has been withdrawn	<ol style="list-style-type: none"> 1. Delete the dispense record or document from the dispensing software, if possible. In some dispensing software, the consent or upload box may be unticked after dispensing, and this will remove the dispense record from the individual's My Health Record. Contact the software vendor or refer to the user manual to see if this feature is included 2. Advise the patient that they can permanently remove the document and the corresponding PBS/RPBS entry via the Consumer Portal. Refer them to the My Health Record helpline (1800 723 471), if necessary 3. If the issue is not resolved, contact the My Health Record helpline (1800 723 471)
Upload of a document (e.g. dispense record) to the wrong patient's My Health Record	<ol style="list-style-type: none"> 1. Delete the incorrect document (e.g. dispense record) from the dispensing software immediately and insert "incorrect identity" as the reason. If you are unable to delete, contact the My Health Record helpline (1800 723 471); they can do it on your behalf 2. Upload a new, corrected version to the correct patient's record 3. Record this action in your own notes
Suspected data breach	<ol style="list-style-type: none"> 1. Suspend/deactivate the user account 2. Change the password information for the account 3. Report the breach to the police and, if relevant: <ol style="list-style-type: none"> a. System Operator (1800 723 471) for any potential or actual data breaches that relate to (or may relate to) the My Health Record system b. Office of the Australian Information Commissioner (1300 363 992) for other data breaches that do not involve the My Health Record system—these may need to be handled in accordance with the <i>Privacy Act 1988</i>

Managing accidental access

Quyen, a previous patient at Gwen's pharmacy, phones to enquire about recent access to her My Health Record by the pharmacy. Quyen received an SMS notifying her that a new organisation, Gwen's pharmacy, has recently accessed her record. Quyen has not had a prescription dispensed at the pharmacy in the past few years, so wants to clarify who accessed her record and why.

Gwen accesses Quyen's patient profile in the dispensing system and confirms that there has been no dispensing in the previous 12 months. A patient history note in Quyen's profile documents accidental access to her My Health Record by another pharmacist, when attempting to view another patient's record. The note states that the error was identified before any clinical information was accessed.

Gwen provides this explanation and reassures Quyen that no security breach has occurred. Quyen is satisfied with this resolution.

Training

All pharmacy staff who will be accessing the My Health Record system must be trained before they access the system for the first time, or if new system functionality is introduced. Training should be included in staff orientation procedures if access to the system is part of a newly employed staff member's role. Training providers should consider using materials accredited by an accredited continuing professional development (CPD) organisation.

Refer to Box 4 for key information that should be included in My Health Record system training. All staff training should be documented.

Training resources are available on the My Health Record website.

Quality assurance

Pharmacy organisations have a responsibility to ensure that their interaction with the My Health Record system maintains the highest possible standard of care for each patient. To achieve this goal, a quality assurance process must be in place that outlines procedures for monitoring how the pharmacy organisation interacts with the My Health Record system, and strives for continuous quality improvement in the safety and quality of services.

To ensure that the quality of interaction with the My Health Record system is maintained, and any breaches are identified and addressed, pharmacy organisations must adhere to their My Health Record security and access policy (see Appendix 3).

To provide measurable quality improvement systems that will ensure quality delivery of services, the pharmacy organisation must be able to⁴²:

- identify and log any clinical incidents (including near misses)
- identify and log potential ways breaches of patient safety and security
- review work practices to prevent recurrence of clinical incidents
- implement safety and improvement strategies in response to clinical incidents, near-miss incidents or potential breaches
- provide ongoing staff training, especially when there have been changes to existing policies.

For further information, refer to the current edition of Australian Commission on Safety and Quality in Health Care *National Safety and Quality Health Service Standards*.

Box 4. My Health Record system training

System training should include:

- use of conformant software and/or the National Provider Portal to access the My Health Record system
- accurate and responsible access to a patient's My Health Record, including privacy issues (see *Privacy*)
- how to adjust the dispense record upload status in conformant software when patients withdraw consent
- processes to follow if there is a clinical incident or data breach involving a patient's My Health Record (see *Managing clinical incidents*)
- use of collaborative strategies to support optimal use of the My Health Record system (e.g. communication with general practitioners, allied health providers and Primary Health Networks)
- how to upload Event Summaries using conformant software (if relevant)
- how to apply preferred documentation standards when contributing information to a patient's My Health Record (e.g. SOAP, SBAR, accepted medical terminology, plain language—see Appendix 6)
- how to encourage patients to engage meaningfully with their My Health Record
- examples of language pharmacists should use to support patient use of My Health Record.



My Health Record and the pharmacist

The My Health Record system provides pharmacists with a platform to enhance provision of patient care through access to key patient health information and by contributing clinical records of care provision (e.g. dispense records).

However, a patient's My Health Record should not be considered as a complete source of patient health information. It does not replace direct sharing of health information (i.e. in person or via telephone) between healthcare providers or with patients.

Access to My Health Record

Pharmacists can access a patient's My Health Record through²⁰:

- conformant software that enables them to view records via their clinical information system, and upload relevant patient clinical information
- the National Provider Portal (NPP), which enables pharmacists without conformant software (e.g. accredited pharmacists practising independently) to search and view patient health records through their web browser. (Documents cannot be uploaded to a patient's My Health Record via the NPP.)

To upload information to a patient's My Health Record using conformant software, pharmacists need:

- an HPI-I that is linked to a registered organisation (i.e. a pharmacy or other healthcare provider organisation with an HPI-O)
- the relevant IHI for the patient who is receiving the healthcare service. An individual's IHI is linked to five identifiers: first name, surname, date of birth, Medicare number or Department of Veterans' Affairs (DVA) number, and gender (see Box 5).
- In addition, if pharmacists are using the NPP to view a patient's My Health Record, they will need to register for a PRODA (Provider Digital Access) account.⁴³ The process for setting up access to My Health Record via the NPP is outlined in Appendix 2.

For further information about registering with the HI Service and applying for healthcare identifiers, pharmacists should refer to the My Health Record website at: www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/register-your-organisation

Access by non-pharmacist staff

The electronic record of supply of a medicine to a patient should accurately record the pharmacist who is responsible for dispensing the medicine. This ensures that all dispensing records uploaded to the patient's My Health Record have been authored by a registered pharmacist with a HPI-I.

Non-pharmacist staff do not hold an HPI-I, and can only use the My Health Record system if they are authorised by the pharmacy organisation to access the system and provide health care to an individual. Pharmacists should determine the need for non-pharmacist staff to use the My Health Record system based on their position description and role. Access to the My Health Record system by non-pharmacist staff must be clearly defined in the organisation's security and access policy (see Appendix 3).

Pharmacy organisations must be able to identify each person who accesses an individual's My Health Record and provide that information to the System Operator when requested. Any access to the My Health Record system by a non-pharmacist will be recorded in the access history of the patient's My Health Record under the pharmacy's HPI-O. However, staff will be provided with a unique user account to access the My Health Record System via conformant software so that their access can be identified.

Box 5. Patient records, healthcare identifiers and My Health Record access

Patient records in the clinical information system need to be complete and accurate before pharmacists access a patient's My Health Record.

Correct patient information will assist the pharmacist to search and match against information held by the Healthcare Identifiers Service, including:

- first name
- surname
- date of birth
- gender

Medicare number (including individual reference number) or Department of Veterans' Affairs (DVA) number.

Pharmacy workflows must ensure that patient information, including date of birth and gender, is captured in the dispensing software to enable the validation of the patient's IHI and upload of dispensing information to the patient's My Health Record.

Electronic Transfer of Prescriptions (eTP)-enabled pharmacies may record the five patient identifiers in the dispensing software efficiently by scanning all available electronic prescription barcodes.

Pharmacists are responsible for the quality of the data contained in their clinical information system, and should consider the need for data cleaning (e.g. to correct any inaccurate information in a patient record in the dispensing software).

The delegating pharmacist will be accountable for the actions of non-pharmacist staff, including use of the My Health Record system. A pharmacist's responsibility is to ensure that non-pharmacist staff who access the My Health Record system are directly supervised, and have the appropriate training and experience, in accordance with the pharmacy's My Health Record security and access policy.

For more information on how to integrate use of the My Health Record system into the pharmacy's dispensing workflow, see the latest version of the *PSA Dispensing Practice Guidelines*.

Pharmacy workflow considerations

Pharmacists have a responsibility to protect and promote the health of patients.²⁹ Changes to work practices or workflows may be required to ensure that information uploaded to a patient's My Health Record is accurate and complete. Some of the workflow considerations are as follows:

- Use a 'script-in' procedure to ensure that patient information, including date of birth and gender, is collected and recorded in the dispensing software.
- Consider how patients' requests not to upload to their My Health Record are passed on to a pharmacist so that the implications of not sharing key pieces of their health information is discussed with the patient (see *Patient support*).
- Ensure that dispense record upload status in conformant software is adjusted accordingly when patients withdraw consent.
- Document in the patient's profile when they requested the dispense record of a particular medicine not to be uploaded.
- Ensure that the dispensing or responsible pharmacist's initials are recorded in the dispensing software, so that all dispense records are uploaded to a patient's My Health Record.
- Consider whether or not to upload a dispense record with incomplete information (e.g. some dispensing software does not have the capability to display ingredients of a compounded product).

Specific My Health Record-related workflow and local procedures should be documented in the organisation's security and access policy (see Appendix 3).

Viewing records

Pharmacists have a professional obligation to ensure that they have sufficient patient information to optimise the professional services they provide and ensure a safe dispensing process.⁵ They should use professional judgement to determine whether they have sufficient information or if further clinical information is required, based on the episode of care being provided.

It is important to note that My Health Record is only one of a number of potential sources of patient health information, and should not be assumed to be a complete record. Pharmacists should consider the need to consult other appropriate sources of information (e.g. the patient or carer, or the prescriber) in addition to, or instead of, a patient's My Health Record

- Assist with reconciliation of patient medicines to produce an accurate medication profile
- Access patient information, including allergies, adverse reactions and non-prescription medicines
- Access clinical information, such as discharge summaries, medication summaries and laboratory results, in a timely manner
- Enhance continuity of care between different healthcare settings
- Confirm appropriateness of treatment based on medical history
- Access immunisation records and child health check summaries

Health Record, to enable safe and appropriate patient care. Pharmacists should ensure that reasonable attempts are made to access information required to inform appropriate clinical decisions.

The My Health Record system provides pharmacists with an accessible source of information that may assist them to meet professional obligations. Pharmacists should only access a patient's My Health Record in the course of providing care to that patient, and should only view documents in the record that they reasonably believe will assist them to provide better patient care (e.g. enhance clinical decision making when a clinical issue or problem has been identified). See Box 6 for examples of reasons for accessing a patient's My Health Record. Appendix 5 provides access scenarios that support patient care.

There is no requirement for the patient to be present when the pharmacist is viewing their record, provided that the above requirements are met.³⁰

When using information from a patient's My Health Record to make clinical decisions, pharmacists should consider the information's:

- **currency**—depending on the type of document, in certain circumstances the information in a patient's My Health Record may not reflect current patient care^c

- **accuracy and completeness**—information contained in a patient's My Health Record must be reconciled with information from other available sources (including a pharmacist-led interview with the patient to obtain a relevant history) and its accuracy assessed within the patient context^d
- **clinical significance**—professional judgement must be used to determine whether a document is clinically relevant to the care the pharmacist is providing
- **source**—the source of any document should be reviewed for appropriateness, because all healthcare providers with an HPI-I who have registered with the My Health Record system can upload information to a patient's My Health Record.

It is good practice to document the clinical information accessed through a patient's My Health Record in the patient profile in the dispensing software or the pharmacy's documentation system, because patients can permanently remove a clinical document, or have their My Health Record permanently deleted if they choose to cancel the record.

Documents in My Health Record

The following clinical documents may be available in a patient's My Health Record¹:

- **Shared Health Summary**—a summary of a patient's medical history, medicines, allergies, adverse drug reactions and immunisations created by their general practitioner or other nominated healthcare provider.
- **Discharge summary**—a record of a patient's hospital stay and any follow-up treatment that is required. It may include a clinical synopsis of the reason for admission and any diagnoses or medication changes made during the admission.
- **Specialist letter**—a document used by a treating specialist to communicate to the referring general practitioner (GP) patient information, treatment plan and follow-up required.
- **Event Summary**—a document that details key health information about a significant healthcare event that is relevant to the ongoing care of the patient (e.g. clinical intervention, improvement in a condition, treatment that has been started or completed). Generally, an Event Summary is used when it is not appropriate to upload the information as a Shared Health Summary, discharge summary or specialist letter.
- **Pathology and diagnostic imaging reports**—reports providing outcomes of pathology tests or diagnostic imaging examinations.

c For example, in oncology settings (e.g. on wards, in clinics), it is not unusual for patients to be dosed from medication charts, with prescriptions reconciled at a later date. Changes to treatment regimens may not be immediately reflected in dispensing information uploaded to the record.

d For example, some information (e.g. S100 Remote Area Aboriginal Health Service dispensing information) may not be patient linked, and therefore may be absent from the patient's My Health Record.

Clinical documents case scenarios

Using a Shared Health Summary

Mrs Wood, 57 years old, has diabetes, and chronic lower back pain associated with a motor vehicle accident about 10 years ago. She goes into Ramya's pharmacy quite regularly for her prescriptions for metformin, ramipril and morphine. She also takes occasional paracetamol for pain. Ramya is concerned about Mrs Wood's pain management as she is always commenting that her pain is not under control and she seems depressed. In response, Ramya offers her a MedsCheck.

During the MedsCheck interview, Ramya accesses Mrs Wood's My Health Record and views her Shared Health Summary. A number of other medical conditions are listed, including depression and an allergy to aspirin. When Ramya talks to Mrs Wood about these additional medical conditions, Mrs Wood acknowledges that she should be taking something for her mood. Ramya views the Medicines Information View in Mrs Wood's My Health Record, which shows that sertraline has been prescribed for her but never dispensed.

Ramya encourages Mrs Wood to talk to her GP about her depression and her pain management. She details this in the action plan, which is provided to Mrs Wood and her GP via secure electronic messaging.

Using a patient's discharge summary

Mrs Nguyen is an 82-year-old woman who has multiple medical conditions and hospital admissions. She has regular changes to her medicines because of problems associated with diabetes, heart failure and pain. She comes into the pharmacy on Friday afternoon after having been discharged from hospital earlier in the week. She has lost her new medicines list given to her on discharge and is confused about the medication changes. Mrs Nguyen thinks her pain medicine and fluid tablets have changed but is unsure. She also thinks her 'sugar pills' may have changed.

Andrew, the pharmacist, accesses Mrs Nguyen's My Health Record. He views her most recent discharge summary and identifies the medicines she was prescribed on discharge. With this additional information, Andrew is able to reconcile her medicines and update her medication profile.

Using immunisation information

Sergio is a consultant pharmacist at the Aboriginal Health Service. He is conducting a home medicines review (HMR) for Tracey, 49 years old, who is new to the area. Tracey was diagnosed with type 2 diabetes 3 years ago and also has osteoarthritis. Sergio asks Tracey if her influenza and pneumococcal immunisations are up to date, but she is unsure.

As Tracey is considered 'medically at risk', Sergio accesses her My Health Record to check her immunisations. He can see that Tracey received influenza and pneumococcal vaccinations 3 years earlier, but there is no record of her receiving an annual influenza vaccine since. Sergio discusses the benefits of immunisation with Tracey, who tells him she didn't realise she needed a vaccination every year. Sergio notes in the HMR report that Tracey is due for an annual influenza vaccination.

Using pathology information

Colin, 34 years old, presents at Ahmed's pharmacy to have his clozapine dispensed. Before supplying clozapine, Ahmed must check and enter Colin's pathology results into the clozapine patient monitoring database. However, Colin has misplaced the printout of his latest pathology results from his doctor.

Colin's My Health Record contains his most recent pathology report. Ahmed accesses Colin's My Health Record and confirms from the pathology report that Colin's white cell count and absolute neutrophil count results are within appropriate parameters, and proceeds to dispense the prescription.

Creating and uploading a Pharmacist Shared Medicines List (PSML)

David, 70 years old, receives a dose administration aid (DAA) service from Ying's pharmacy. David presents to the pharmacy with a few new prescriptions. Ying contacts David's GP to clarify the changes made to his medications and later receives a written confirmation.

Ying reconciles David's medication, documents the changes in the DAA packing record and updates the DAA medication profile in the local software. Ying then packs a new DAA for David. Based on the new DAA medication profile, Ying creates a PSML and uploads the document to David's My Health Record.

Using a Shared Health Summary

Mrs Wood, 57 years old, has diabetes, and chronic lower back pain associated with a motor vehicle accident about 10 years ago. She goes into Ramya's pharmacy quite regularly for her prescriptions for metformin, ramipril and morphine. She also takes occasional paracetamol for pain. Ramya is concerned about Mrs Wood's pain management as she is always commenting that her pain is not under control and she seems depressed. In response, Ramya offers her a MedsCheck.

During the MedsCheck interview, Ramya accesses Mrs Wood's My Health Record and views her Shared Health Summary. A number of other medical conditions are listed, including depression and an allergy to aspirin. When Ramya talks to Mrs Wood about these additional medical conditions, Mrs Wood acknowledges that she should be taking something for her mood. Ramya views the Medicines Information View in Mrs Wood's My Health Record, which shows that sertraline has been prescribed for her but never dispensed.

Ramya encourages Mrs Wood to talk to her GP about her depression and her pain management. She details this in the action plan, which is provided to Mrs Wood and her GP via secure electronic messaging.

- **Pharmacist Shared Medicines List (PSML)**^e—a list of reconciled medicines that the consumer was known to be taking at the time the list was created by a pharmacist. A pharmacist can upload a PSML based on a reconciled hospital discharge medicines list or dose administration aid medicines list, and after providing a pharmacist professional service, such as MedsCheck, home medicines review (HMR) or residential medication management review (RMMR).
- **Prescription records**—documents containing information about the medications (PBS, RPBS and private) prescribed to a patient, including brand name, active ingredients, strength, dosage instructions, maximum number of repeats, date of prescribing, prescription expiry date, the healthcare provider who prescribed the medication and the healthcare provider organisation that the patient visited.
- **Dispense records**—documents containing information about the medications (PBS, RPBS and private) dispensed to a patient, including brand name, active ingredients, strength, dosage instructions, number of repeats dispensed and remaining, where it was dispensed and the date of last dispensing.
- **eReferral**—a document that communicates significant patient information from one treating healthcare provider to another.

Medicines Information View

The Medicines Information View in the My Health Record system can quickly sort and display medicines information held in a patient's My Health Record in date or alphabetical order. The medicines information is gathered from the⁴⁴:

- patient's most recent (and up to 2 years) prescription and dispense records, and other PBS claims information
- patient's most recent Shared Health Summary and discharge summary
- patient's most recent PSML
- recent Event Summaries, specialist letters and eReferral notes uploaded to the patient's record since their latest Shared Health Summary
- patient's personal health summary, which may include allergies, adverse reactions and other key information.

Prescription and Dispense View

The Prescription and Dispense View in the My Health Record system allows patients and their healthcare providers to easily view details of their prescribed and dispensed medications in one place. Over time, the view will capture the history of a patient's medication details.⁴⁵

The view displays⁴⁵:

- the name of the medication (both the brand name and the active ingredients), and the date it was prescribed and dispensed
- the strength and form of the medication
- directions for use.

^e PSML is a new clinical document planned to be implemented later in 2019. A small number of software vendors have made changes in their products so that pharmacists can upload PSMLs in clinical practice. It is expected that these capabilities will be progressively rolled out throughout the 2019–20 financial year.

Using the Prescription and Dispense View

Ms Smith, a 23-year-old woman, comes into Sung-Hee's pharmacy on a Sunday morning after visiting the after-hours medical clinic. She has been prescribed cefalexin 500 mg three times a day for a presumed urinary tract infection. During counselling, Sung-Hee learns that Ms Smith developed a rash when taking an antibiotic about 12 months ago, but she cannot remember the name of the antibiotic. The antibiotic was prescribed by her regular GP, whose practice is closed today. Sung-Hee does not have any dispensing history for Ms Smith.

Sung-Hee accesses Ms Smith's My Health Record and opens the Prescription and Dispense View, and identifies that the previous antibiotic was cefalexin. Ms Smith does not want to take this antibiotic if it is the same one that caused the rash. Sung-Hee calls the doctor at the after-hours medical clinic to discuss. The doctor changes the prescription to trimethoprim 300 mg daily for 3 days. Sung-Hee advises Ms Smith that she has updated the allergy information in the pharmacy's dispensing system and uploaded it to her My Health Record. Sung-Hee also records this event as a clinical intervention.

Contributing clinical information

Pharmacists can upload dispensing information to a patient's My Health Record. They should ensure that any uploaded clinical information is complete, relevant, accurate and current at the time of uploading. Information should be presented in an appropriate format to ensure its relevancy (see *Standards of documentation*).

Pharmacists should check that the correct patient is selected in their dispensing software to ensure that any information is uploaded to the correct patient's My Health Record.

Patients may request that a document is not included in their My Health Record. The pharmacist must adhere to the wishes of the patient and should document the request in the patient's history in the dispensing software or pharmacy record.

Pharmacists should be aware of additional consent requirements associated with uploading sensitive health information (see *Consent*).

Dispensing information

For pharmacies using conformant software, dispense records will be uploaded either directly or via prescription exchanges. However, only prescriptions dispensed using the credentials of an authorised user (e.g. a pharmacist with an HPI-I and granted access by their organisation) will be uploaded.

Dispensing information will only be uploaded if the pharmacy is registered and connected to the My Health Record system, and the patient has not withdrawn consent (see Figure 3).

Right medicine, right patient, wrong record

David, the pharmacist, has suggested to George Whyte (aged 85) that he would benefit from having his medicines packed in a dose administration aid (DAA). Mr Whyte is being treated for high cholesterol, cardiac failure, lower back pain and peptic ulcer disease. Before packing Mr Whyte's DAA, David reconciles his medicines to create an accurate medication profile.

During the reconciliation process, David accesses Mr Whyte's My Health Record and opens the Medicines Information View. He notices that there is a dispensing record for metformin. To confirm the appropriateness of treatment based on the patient's medical history, David reviews Mr Whyte's most recent Shared Health Summary and cannot find any report of a diagnosis of diabetes or prescribing of metformin.

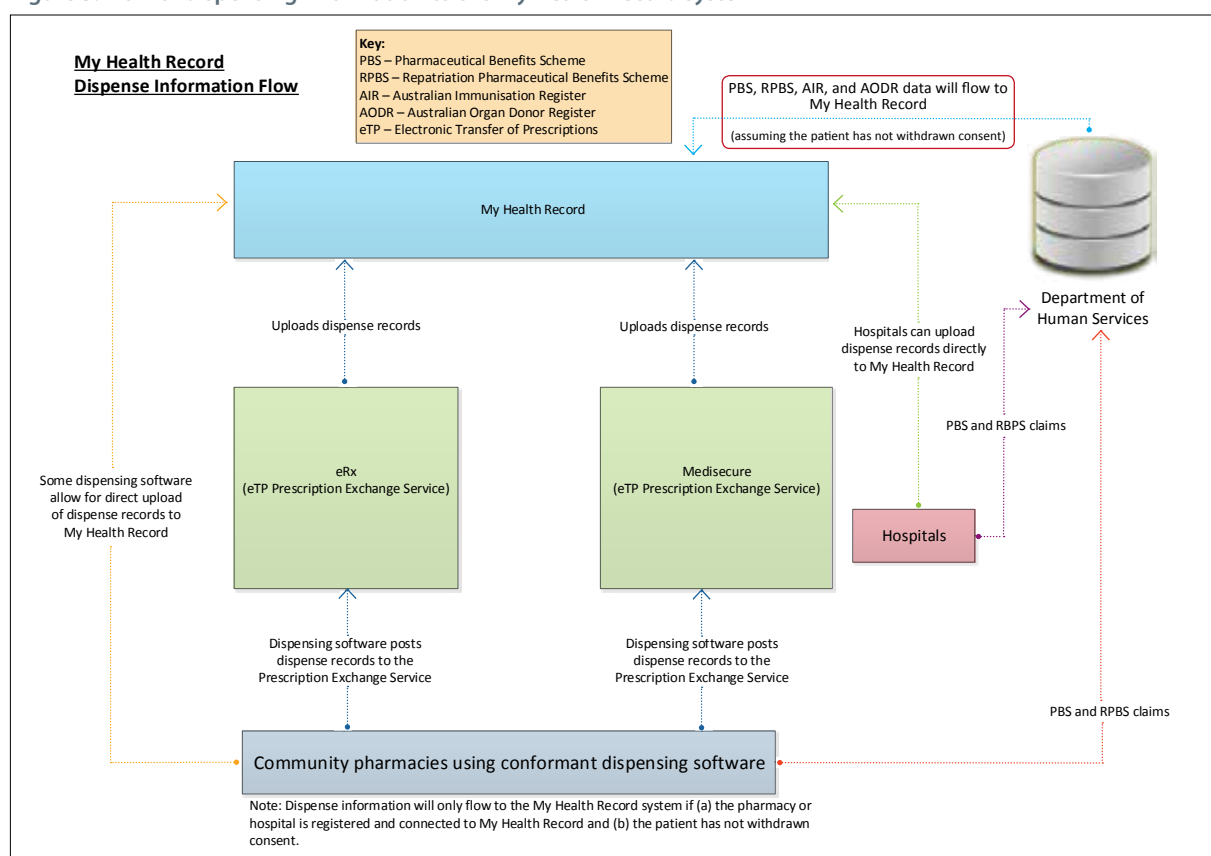
David contacts Mr Whyte's GP, and confirms that he has not been prescribed metformin and does not have diabetes. David asks Mr Whyte if he sees any other doctors or specialists, and he says that he only sees the one doctor.

David has identified a clinical incident resulting from an error in the dispensing information upload by another pharmacy. He informs Mr Whyte of the error and contacts the other pharmacy to amend Mr Whyte's record, according to the pharmacy's process for managing clinical incidents.

The other pharmacy confirms that they received a prescription for metformin from a Mr George White, but the incorrect patient, Mr George Whyte, was selected in their dispensing system. David records his actions in Mr Whyte's patient notes in the pharmacy's clinical information system.

This scenario highlights the importance of confirming all five patient identifiers to ensure that the correct patient is selected in dispensing software, and consequently the dispense record is uploaded to the correct patient's My Health Record.

Figure 3. Flow of dispensing information to the My Health Record system



Reference: Australian Digital Health Agency⁴⁶

For dispensing software-specific information, pharmacists should refer to their software manual or consult the software vendor.

Dispense information from PBS and RPBS claims will flow automatically to a patient's My Health Record, regardless of whether the pharmacy organisation is connected to the My Health Record system. There can be a delay of up to 6 weeks for information to be uploaded. If a patient withdraws consent for a dispense record to be uploaded, they can stem the flow of PBS/RPBS information to their record, and restrict access to, or remove, particular claims information, via the Consumer Portal.

Using prescribing information

Mr Brown is a 68-year-old man with hypertension, diabetes, osteoarthritis and hyperlipidaemia. Last month, his specialist changed his blood pressure medicine from perindopril to another tablet. Mr Brown cannot remember the name of his new tablet, which he has now run out of. He had the new medication previously dispensed by the pharmacy next to his specialists' rooms.

At his GP appointment today, he received a prescription for perindopril, rather than the new medicine.

Mai, the pharmacist, accesses Mr Brown's My Health Record to confirm the name of his newly prescribed medicine via information in:

- the Medicines Information View, which details dispense and PBS information
- prescribing information (available if the specialist was using a health information exchange service such as eRx)
- PBS administrative information, to identify what medication was dispensed recently.

There is no PBS record of the new medicine in Mr Brown's My Health Record yet. However, Mai sees that olmesartan was prescribed by the specialist. She calls Mr Brown's GP to notify them of the change. The GP gives a verbal authorisation for the pharmacist to dispense olmesartan, and confirms they will provide a prescription the next day.

Pharmacist Shared Medicines List

Pharmacists can create and upload an accurate and up-to-date reconciled medicines list to a patient's My Health Record to support the care of the patient. Before creating a PSML, pharmacists should consider whether the document would benefit the patient (e.g. patients with multiple comorbidities and frequent hospital admissions) and how other healthcare providers would benefit from the information in the PSML.

A PSML should be as accurate as practicable. It should include all prescription, non-prescription, complementary and alternative medicines that the patient takes at a point in time. Where possible, pharmacists should use information from at least two sources to inform the medication reconciliation process.⁴⁷ These sources may include other healthcare providers, the patient and their My Health Record.

Box 7. Considerations when uploading clinical information via Event Summaries

The decision to upload clinical information in an Event Summary to a patient's My Health Record should be informed by:

- the complexity of the patient's care requiring coordination between a variety of healthcare providers
- the likelihood that the patient will present to other healthcare providers who may benefit from the information
- the clinical relevance of the information to the patient's current management
- the potential for the information to contribute to the clinical assessment of future patient presentations
- the sensitivity of the information.

PSMLs can be created based on a reconciled hospital discharge medicines list or dose administration aid medicines list, and after providing a pharmacist professional service (e.g. MedsCheck, HMR or RMMR). Where clinically appropriate, a new PSML should be created and uploaded to a patient's My Health Record whenever changes are made to a patient's medicines.

Event Summaries

Pharmacists can contribute patient allergy information to a My Health Record as an Event Summary, by adding patient allergies to their clinical information system. Pharmacists should consult their software vendors for advice on uploading allergy information to a My Health Record. This functionality may not be available in all conformant software systems.

In future, pharmacists may be able to add other significant patient health information to a My Health Record as an Event Summary, so that they can document meaningful clinical information associated with the provision of professional services (i.e. MedsChecks, HMR, dose administration aids, clinical interventions and Staged Supply).

Event Summaries should only be used to share patient clinical information that is of benefit to other treating healthcare providers (see Box 7).

Editing or deleting clinical documents

If a clinical document (e.g. dispense record, PSML, Event Summary) has been uploaded in error or contains a mistake, the author of that document can delete it from their local system, which will remove it from the patient's My Health Record. Clinical documents cannot be edited in the My Health Record system.

In the event of an error or mistake, the authoring pharmacist can replace the clinical document or dispense record by editing it in the pharmacy dispensing software or other clinical information software. The edited version is then uploaded and supersedes the original.²⁰

If a pharmacist identifies an error in a document uploaded by another organisation, they should notify the author and organisation that created the record. If the author cannot be contacted, the pharmacist should contact the System Operator via the My Health Record helpline (1800 723 471), to amend the record. Pharmacists cannot delete or replace a document they did not upload (see *Managing clinical incidents*).

If patient records in the dispensing software need to be merged, it is important to ensure that the patient's My Health Record is updated correctly. Contact dispensing software vendors for information on the merge function and its impact on a patient's My Health Record.

Standards of documentation

Pharmacists have a responsibility to ensure that all clinical documents uploaded to a patient's My Health Record are of a sufficient standard that they could provide clinical benefit to the patient if accessed by other treating healthcare providers.

In future, pharmacists will be able to upload an Event Summary to a patient's My Health Record, which could be accessed by a broad range of treating healthcare providers.

Clinical documents, such as an Event Summary, should be written in such a way as to avoid any ambiguity about the patient, the author and what occurred. They should contain sufficient information to allow other healthcare providers to provide care to the patient. Only information that is relevant to the care provided should be included.⁴⁸

Clinical documents uploaded to a patient's My Health Record should contain^{48,49}:

- the date of consultation
- the author's printed name, designation and place of practice
- accurate statements of clinical interactions between the pharmacist and the patient and/or their carer
- objective information that is clinically useful to other healthcare providers
- detailed management strategies, including
 - the care and services provided, and any outcomes
 - professional advice sought and provided
 - observations taken and results.

For further information, see Appendix 6.

Abbreviations and symbols used in clinical documents uploaded to a patient's My Health Record should be approved (see the *Australian Pharmaceutical Formulary and Handbook*, 24th edition (APF24), *Medical abbreviations chapter*, and the *Australian Commission on Safety and Quality in Health Care (ACSQH) abbreviations*⁵⁰).

Pharmacists should refer to resources such as *National Guidelines for On-Screen Display of Medicines Information* (2017) and *National Guidelines for On-Screen Presentation of Discharge Summaries* (2017) for information about the on-screen display of medicines information.

Access history

Any activity on the My Health Record system, including viewing and uploading information, is recorded under the access history. This log of activities can be viewed by the System Operator and the patient. Pharmacists can view a record of their own activity. The access history displays⁵¹:

- the name of the healthcare provider organisation that accessed the patient's My Health Record
- the time the record was accessed
- the type of activity (i.e. view or upload).

Pharmacists should only view a patient's My Health Record for the purpose of providing care. If a pharmacist inadvertently accesses a document or record, this access should be noted in the patient history in the pharmacist's clinical information system to enable follow-up, if required.



My Health Record and the patient

Pharmacists should ensure that patients fully understand how the pharmacy intends to interact with the My Health Record system, why their health information and activities are uploaded in their My Health Record, and why their My Health Record is accessed by pharmacists and pharmacy staff.

When communicating with patients about My Health Record, pharmacists should consider the patient's health and e-health literacy, cognition, culture and beliefs, and the need to involve other primary healthcare team members, family and carers, and/or translators.⁵²

Patient control

The My Health Record system has been designed to enable the patient to control the content of their record, and who can access their health information. The patient can^{27,28}:

- cancel their record and have it permanently deleted at any time
- register for a record at any time, or re-register for a record if they have cancelled their previous record
- request that a document is not uploaded to their My Health Record by their healthcare provider
- request that no Medicare information is uploaded to their record by the Department of Human Services
- choose to receive an email or SMS notification when a healthcare provider accesses their record for the first time or in an emergency

- choose to restrict access to, hide from view, or permanently remove, specific documents in their My Health Record
- choose which healthcare provider organisations can access their My Health Record.

Patients can limit access to their entire record (using a Record Access Code) or to particular documents (using a Limited Document Access Code).^f Restrictions can be applied to all organisations, or a specific organisation when that organisation has previously accessed the patient's My Health Record.

A healthcare provider will be prompted by their clinical information system if an access code is required. The patient will need to provide the access code to the healthcare provider to enable access to their My Health Record.¹ Pharmacists should acknowledge the patient's right to control access to information in their My Health Record and discuss why they need access to the information restricted by an access code.

In an emergency, a healthcare provider can use the emergency access functionality to override the existing access controls (see *Consent*).

Patient support

Patients should be supported to make informed decisions about managing their My Health Record. Pharmacists should discuss the My Health Record system with their patients, including details of the types of information that patients can share using their My Health Record and the implications of not sharing key pieces of health information.

^f Although the My Health Record system enables this functionality, results from the My Health Record participation trials in 2017 indicate that most patients do not invoke access controls.⁵⁷

Patients should be informed about the security of their health information in their My Health Record, and the measures in place to prevent unauthorised access.

Consumer guides are available on the My Health Record website, which could be used by pharmacists to offer patient support.

Supporting informed decision making

Joe (aged 54), a regular patient at Gary's pharmacy, presents with a prescription for vardenafil. Joe specifically asks that Gary does not upload the vardenafil dispense record to his My Health Record. He works as an administrator in a hospital and doesn't want his colleagues to find out that he has erectile dysfunction.

Gary first assures Joe of the security measures in place to prevent unauthorised access to his My Health Record, including by his colleagues at the hospital. Healthcare providers are only permitted to access the records of patients in their care, and need patient details, including first name, surname, date of birth, Medicare number and gender, to access a record. Joe can also view who has accessed his record, so would be alerted to any unauthorised access should it occur.

Gary also explains to Joe the implications of not including a record of the medicine in his My Health Record. Vardenafil can interact with other medicines, including some given in emergency situations, so it may be important for his treating healthcare providers to be aware of his treatment.

Finally, Gary outlines controls Joe can place on his record if he is still worried about unauthorised access, including a Record Access Code, and a Limited Document Access Code. After talking to Gary, Joe decides to allow the dispense record to be included in his My Health Record without applying an access code.

Health literacy and e-health literacy

Health literacy is important to the safety, quality and effectiveness of health care. If patients do not understand the information and services they are provided, they may be at higher risk of experiencing poor health outcomes. Health literacy affects e-health literacy. Patient engagement with the My Health Record system relies on their e-health literacy, as well their level of social support, and the responsiveness of healthcare providers and the health system.⁵³

About 60% of patients do not have adequate health literacy to make well-informed health decisions and act on them. By responding to a patient's health literacy and providing support, healthcare providers can forge effective partnerships with the patient, building the patient's capacity to make informed healthcare decisions (see Box 8).⁵³

Both health literacy and e-health literacy are dynamic and influenced by context (e.g. illness, hospitalisation). Pharmacists should consider their patient's health literacy and e-health literacy so that they provide tailored support and promote engagement with the My Health Record system.⁵³

For further information about health literacy, see: www.safetyandquality.gov.au/our-work/patient-and-consumer-centred-care/health-literacy

Box 8. Ways to support patient health literacy

Pharmacists can support the delivery of effective healthcare messages by:

- identifying the needs and preferences of individual patients, and tailoring communication style to their situation
- assuming that most people will have difficulty understanding and applying complex health information and concepts
- using a range of interpersonal communication strategies to confirm that information has been delivered and received effectively
- encouraging people to speak up if they have difficulty understanding the information provided
- using effective ways of communicating risk information about treatment options.

Reference: Adapted from ASCQHC⁵³

Appendix 1 - Accessing My Health Record via conformant software

My Health Record - Healthcare Provider Registration

Access via conformant software

Step 1 – Register for a PRODA account

PRODA (Provider Digital Access) is a method of authentication to provide users with access to government services online - <https://proda.humanservices.gov.au>

PRODA registration requires three forms of identification from the following list.

- ♦ Australian passport
- ♦ Medicare card
- ♦ Australian driver's licence
- ♦ ImmiCard
- ♦ Australian birth certificate
- ♦ Australian Visa and foreign passport
- ♦ Citizenship certificate
- ♦ Certificate of registration by descent

Password hint: cannot include more than one special character.

Complete the registration and log in.

Step 2 – My Health Record Seed Organisation Registration

Healthcare providers and administrators can manage the My Health Record registration process via Health Professional Online Services (HPOS). Once you are logged into PRODA, click **Health Professional Online Services (HPOS)** from the list of services.

If this is your first time using PRODA...

You will be prompted to enter your healthcare identifier (i.e. AHPRA registration, HPI-I, HPI-O or RO/OMO number).

You will then be prompted to accept the terms and conditions, set your email address, and set your notification preferences. It is recommended that you select **Immediate notification for each new correspondence**.

Once your PRODA and HPOS are linked...

From within the **Health Professional Online Services** tile, choose either **Link Identifiers** to link your PRODA account to the HI service or **Go to Service** to register your organisation. Follow the prompts.

If you are not listed on your organisation's Australian Business Register record, you may need to upload evidence to your online application.

The following documents may be uploaded. A full list of documents is included in the **Organisation Details** tab of the online application.

- ♦ Certificate of company registration from ASIC
- ♦ Notice by registrar of Australian Business Register
- ♦ Business bank statement
- ♦ Lease agreement or Rates notice
- ♦ Other document (i.e. a statutory declaration)

Submit the form, your process will end with a Pending status. The **HPOS Mail Centre** will notify you when the registration is complete.

Step 3 – Request a NASH Certificate

Once your HPI-O has been issued, click **My Programs** and then **Healthcare Identifiers**. Select **My organisation details** and select your organisation.

From the **Organisation snapshot** screen, click the last tab **Certificates** and then **Request a NASH PKI site certificate** at the bottom of the screen.

Complete the **Mobile Number** and other required fields, click **Save changes**. You will receive an SMS when the certificate is ready for download from HPOS (from the **Certificates** tab).

Step 4 – Link your existing PKI certificate

From the HPOS **Organisation snapshot** screen, click the last tab **Certificates** and then **Link existing PKI certificate** near the bottom of the screen. Identify the correct PKI certificate to link to your HPI-O.

Need Help?

PRODA: 1800 700 199
(Mon – Fri 8am to 5pm AWST)

HPOS: 13 21 50
(Mon – Fri 8am to 5pm AWST)

Certificates: 1800 700 199
(Mon – Fri 8am to 5pm AEST)

My Health Record Help line:
1800 723 471
(24 hours, 7 days a week)



Appendix 2 - Accessing My Health Record via the National Provider Portal

My Health Record - Healthcare Provider Registration Access via the National Provider Portal (NPP)

Step 1 – Register for a PRODA account

PRODA (Provider Digital Access) is a method of authentication to provide users with access to government services online - <https://proda.humanservices.gov.au>

PRODA registration requires three forms of identification from the following list.

- ♦ Australian passport
- ♦ Medicare card
- ♦ Australian driver's licence
- ♦ ImmiCard
- ♦ Australian birth certificate
- ♦ Australian Visa and foreign passport
- ♦ Citizenship certificate
- ♦ Certificate of registration by descent

Password hint: cannot include more than one special character.
Complete the registration and log in.

Step 2 – My Health Record Seed Organisation Registration

Healthcare providers and administrators can manage the My Health Record registration process via HPOS (Health Professional Online Services). Once you are logged into PRODA, click **Health Professional Online Services (HPOS)** from the list of services.

If this is your first time using PRODA...

You will be prompted to enter your healthcare identifier (i.e. AHPRA registration, HPI-I, HPI-O or RO/OMO number).

You will then be prompted to accept the terms and conditions, set your email address, and set your notification preferences. It is recommended that you select **Immediate notification for each new correspondence**.

Once your PRODA and HPOS are linked...

From within the **Health Professional Online Services** tile, choose either **Link Identifiers** to link your PRODA account to the HI service or **Go to Service** to register your organisation. Follow the prompts.

The first two tabs identify the organisation and your details. The third tab allows you to nominate an Organisation Maintenance Officer (OMO).

If you are not listed on your organisation's Australian Business Register record, you may need to upload evidence to your online application. The following documents may be uploaded. A full list of documents is included in the **Organisation Details** tab of the online application.

- ♦ Certificate of company registration from ASIC
- ♦ Notice by registrar of Australian Business Register
- ♦ Business bank statement
- ♦ Lease agreement or Rates notice
- ♦ Other document (i.e. a statutory declaration)

Submit the form, your process will end with a Pending status. The **HPOS Mail Centre** will notify you when the registration is complete.

Step 3 – Link your Healthcare provider individuals

Once your HPI-O has been issued, click **My Programs** and then **My Health Record System - Organisation Registration**. Select **Manage Authorisation Links** and **Add/Update** your organisation.

Add healthcare providers' HPI-Is in the **Enter HPI-I Number** field and select **Search**. The HPI-I must match exactly.

Providers can locate their HPI-I by accessing their account on the AHPRA website - <https://www.ahpra.gov.au>

Your healthcare providers can now access the National Provider Portal by clicking the My Health Record tile in their PRODA account.

Need Help?

PRODA: 1800 700 199
(Mon – Fri 8am to 5pm AWST)

HPOS: 13 21 50
(Mon – Fri 8am to 5pm AWST)

My Health Record Help line:
1800 723 471
(24 hours, 7 days a week)



Appendix 3 - My Health Record security and access policy

My Health Record security and access policy (this policy should be reviewed and maintained regularly)		
Organisation name:	Version Number:	Date version was enacted:
Governance		
Responsible Officer (RO)		
Organisation Maintenance Officer/s (OMO)	1.	
	2.	
	3.	
	4.	
Access		
Authorised staff will access the My Health Record system via:		
An up-to-date list of individual healthcare providers authorised to access the Provider Portal will be provided to the System Operator (SO) by:		
Authorised staff will be provided with a unique user account to access the My Health Record system via conformant software by:		
The level of access granted to individual staff will be determined and documented by:		
Access flags will be assigned by:		
Access records will be maintained by:		
Security		
User account information and access will be managed by:		
Account passwords will be changed by users every:		
Staff will report any suspected security breach to:		
Confirmed security breaches will be reported to the relevant authority by:		
A log of security breaches including date and time of the breach, user account involved, patient information accessed (if known), and mitigation strategies employed will be maintained by:		
A risk assessment of information and communications technology (ICT) systems to identify and mitigate potential privacy and security risks associated with My Health Record system access is conducted every:		
Training		
My Health Record system training will be organised for all authorised staff before they first access the system by:		
A register of staff training including the names of those who have completed training and the date training was completed will be maintained by:		
Training will be reviewed to ensure currency and updated as required (i.e. if new functionality is introduced into the system) every:		
Clinical incidents		
Clinical incidents will be reported to the relevant party by:		
A log of reported clinical incidents will be maintained by:		
Clinical incident management is the responsibility of:		
Patient complaints		
Patient complaints regarding My Health Record will be redirected to the My Health Record Helpline (1800 723 471) or will be referred to:		
Local procedures related to My Health Record use		

Explanatory notes

Governance

Responsible Officer (RO): has legal responsibility for understanding of, and compliance with, this policy, and compliance with the My Health Record (MHR) legislation (e.g. pharmacy owner, pharmacist manager).

Organisation Maintenance Officer (OMO): undertakes the day-to-day administrative tasks in relation to the HI Service and the MHR system. An OMO needs to be someone who is familiar with the IT system used by [insert organisation name]. The OMO is responsible for understanding, implementation and compliance monitoring of the MHR system security and access policy, and for maintenance of the policy on behalf of [insert organisation name]. A healthcare provider organisation can have multiple OMOs. The OMO has different responsibilities to the RO; it is recommended that these two roles are not performed by the same person.

Access

Authorised staff: Staff are only authorised to access the MHR system where access is required for the provision of patient care. The OMO will maintain a record of authorised Healthcare Provider Identifier—Individual (HPI-I) numbers, and the level of access granted, in the clinical software and in the organisation's internal records.

National Provider Portal: means the portal provided by the System Operator that allows identified healthcare providers from participating healthcare provider organisations to access the MHR system without having to use a conformant clinical information system. Where individual healthcare providers are authorised to access the MHR system using the National Provider Portal, the OMO will establish and maintain an accurate and up-to-date list of individuals with the System Operator. If an individual healthcare provider is no longer authorised to access the National Provider Portal on behalf of the organisation, the OMO will ensure that the System Operator is informed and the individual removed from the list of authorised users.

System Operator: means the Australian Digital Health Agency. To contact the agency about issues with the MHR system, phone the MHR helpline (1800 723 471).

Unique user account: The pharmacy dispensing software (or clinical information software) will be used to assign and record unique internal staff member identification codes. The unique identification code will be recorded by the clinical software against any MHR system access. Staff will use their individual user accounts to access the MHR system at all times.

Level of access: It is a criminal offence for anyone other than a registered clinical professional to access a patient's MHR. Staff may be granted full access (i.e. ability to view and upload records) or view-only access as determined by the duties of their role. Dispensary or pharmacy assistants may be granted a view-only access to the MHR system to assist pharmacists in performing certain tasks.

Access flags: means an information technology mechanism made available by the System Operator to define access to a consumer's digital health record. Where appropriate to the size and complexity of the healthcare organisation, the RO/OMO will define an appropriate network hierarchy for the organisation and assign access flags appropriately for the structure of the organisation. The network hierarchy will define the seed organisation, the network organisations that fall under the seed organisation and the network organisations for whom access flags are appropriate.

In setting and maintaining access flags, the RO/OMO will ensure that:

- healthcare recipients are able to determine and control access to their MHR in a way that meets reasonable public expectations. Network organisations that would not be expected by healthcare recipients to be connected will thus have their own access flags
- the organisation is able to share health information internally in an appropriate manner that prevents security breaches.

The RO/OMO will undertake reviews of the network structure and access flag assignments when the structure changes, or a System Operator or healthcare recipient query reveals potential structural issues. The organisation commits to making reasonable changes in line with requests from the System Operator.

Access records: means records that enable identification of the user who accessed the system via conformant software on a particular day. The OMO will determine whether the practice management software keeps a record of the individual staff members assigned to a particular user account. If not, the OMO will create and maintain a separate record that details the links between user accounts and individual staff. These records must be maintained to allow audits to be conducted by the System Operator at their discretion or as part of clinical incident management.

Security

Data breach: means instances of unauthorised collection, use or disclosure of health information included in a healthcare recipient's MHR—for example, when a staff member with access to the MHR system discovers that someone else may have gained access to their user account.

Relevant authority: If a security breach is confirmed, the breach will be reported to the relevant authority. The police will be notified of all security breaches. If patient data are compromised, the Office of the Australian Information Commissioner will be notified. If the breach involved the MHR system, the System Operator will be notified.

Mitigation strategies: In the event of a security breach, the RO/OMO will undertake appropriate mitigation strategies, including:

- suspending/deactivating the user account
- changing the password information for the account
- reporting the breach to the police, and the System Operator and the Office of the Australian Information Commissioner, as relevant.

Risk assessment: includes assessment of:

- potential for unauthorised access to the MHR system using the clinical information system, and associated mitigation strategies, if required.
- potential for misuse or unauthorised disclosure of information from a consumer's MHR by persons authorised to access the MHR system, and associated mitigation strategies, if required
- potential for accidental disclosure of information contained in a consumer's MHR, and associated mitigation strategies, if required
- increasing risks and potential impact of the changing threat landscape (e.g. newer types of security threats such as ransomware), and associated mitigation strategies, if required
- any relevant legal or regulatory changes that have occurred since the last review, and associated mitigation strategies, if required.

Training

MHR system training: Staff training will provide information about how to use the conformant software, and/or the MHR system National Provider Portal, so that staff can access the My Health Record system accurately and responsibly. It will include privacy training. Training will use materials approved by the Australian Digital Health Agency, the Pharmaceutical Society of Australia, the Pharmacy Guild of Australia or the Society of Hospital Pharmacists of Australia (i.e. MHR training modules or MHR CPD modules).

New functionality: As a general rule, when new functionality is introduced into the MHR system, there is a version upgrade and release to pharmacy dispensing software. Training material produced by the Australian Digital Health Agency and/or material from peak organisations will be updated to reflect new functionalities as they become available and published for public use. Additional training may need to be provided to staff with authorised access, using the updated training material.

Clinical incidents

Clinical incident: means 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. A clinical incident can be related to safety, usability, technical, privacy or security issues. The incident may relate to the MHR system directly, or the behaviour of clinical software when interacting with the MHR system.

Relevant party: Clinical incidents will be reported to the relevant party at the time of occurrence. In the first instance, the relevant party is the System Operator who can be contacted via the MHR helpline (1800 723 471). The System Operator will triage the clinical incident and refer it as necessary.

Clinical incidents management

Incident	Action
Error in a document (e.g. dispense record) uploaded to a patient's My Health Record	<p>If you made the error:</p> <ol style="list-style-type: none"> 1. Delete the incorrect document (e.g. dispense record) from your dispensing system immediately and re-dispense 2. Upload the new, correct version 3. Record all actions in your own notes <p>If you are unable to delete the erroneous document, contact the System Operator via the My Health Record helpline (1800 723 471)</p> <p><i>Note: These actions relate to correcting dispensing errors in a patient's My Health Record. Appropriate follow-up, including replacing any incorrect medicine, referring the patient to the prescriber where necessary and notifying your indemnity insurer, must also occur as a priority</i></p> <p>If another healthcare provider made the error:</p> <ol style="list-style-type: none"> 1. Contact the patient and inform them that you have identified an error in their My Health Record 2. Encourage the patient to exercise their right to have the error corrected by the healthcare provider who uploaded the information, or offer to follow up with the healthcare provider yourself 3. Notify the System Operator via the My Health Record helpline (1800 723 471), if the healthcare provider cannot be contacted 4. Record your actions in your own notes
Upload of a document (e.g. dispense record) to a patient's My Health Record if consent has been withdrawn	<ol style="list-style-type: none"> 1. Delete the dispense record or document from the dispensing software, if possible. In some dispensing software, the consent or upload box may be unticked after dispensing, and this will remove the dispense record from the individual's My Health Record. Contact the software vendor or refer to the user manual to see if this feature is included 2. Advise the patient that they can permanently remove the document and the corresponding PBS/RPBS entry via the Consumer Portal. Refer them to the My Health Record helpline (1800 723 471), if necessary 3. If the issue is not resolved, contact the My Health Record helpline (1800 723 471)
Upload of a document (e.g. dispense record) to the wrong patient's My Health Record	<ol style="list-style-type: none"> 1. Delete the incorrect document (e.g. dispense record) from the dispensing software immediately and insert "incorrect identity" as the reason. If you are unable to delete, contact the My Health Record helpline (1800 723 471); they can do it on your behalf 2. Upload a new, corrected version to the correct patient's record 3. Record this action in your own notes
Suspected data breach	<ol style="list-style-type: none"> 1. Suspend/deactivate the user account 2. Change the password information for the account 3. Report the breach to the police and, if relevant: <ol style="list-style-type: none"> a. System Operator (1800 723 471) for any potential or actual data breaches that relate to (or may relate to) the My Health Record system b. Office of the Australian Information Commissioner (1300 363 992) for other data breaches that do not involve the My Health Record system—these may need to be handled in accordance with the Privacy Act 1988

Patient complaints

Patient complaints: Healthcare recipients will be made aware of the process for raising issues or complaints. Patient complaints raised in relation to unauthorised access to their My Health Record will be investigated. Unauthorised access will be managed through complaint management and staff performance management processes. If the unauthorised access is found to be by someone other than an employee, the healthcare recipient and the complaint will be referred to the management of that service and/or the Office of the Australian Information Commissioner. Where a healthcare recipient ask for a document to be removed or amended, the request will be logged with the OMO and the document removed, or a new amended document uploaded, within 7 days. If amendment or removal is not considered appropriate, the healthcare recipient will be directed to exercise their personal controls over the document.

Local procedures related to My Health Record use

As each pharmacy's workflow varies, specify local procedures such as:

- My Health Record access by non-pharmacist staff
- upload of 'owing' prescriptions or dispense records with incomplete information (e.g. incomplete product name of a compounded product)
- how patients' requests not to upload to their My Health Record are passed on to a pharmacist.

Policy Manager:

Contact: Tel: Email:

Approval authority: Latest review date:

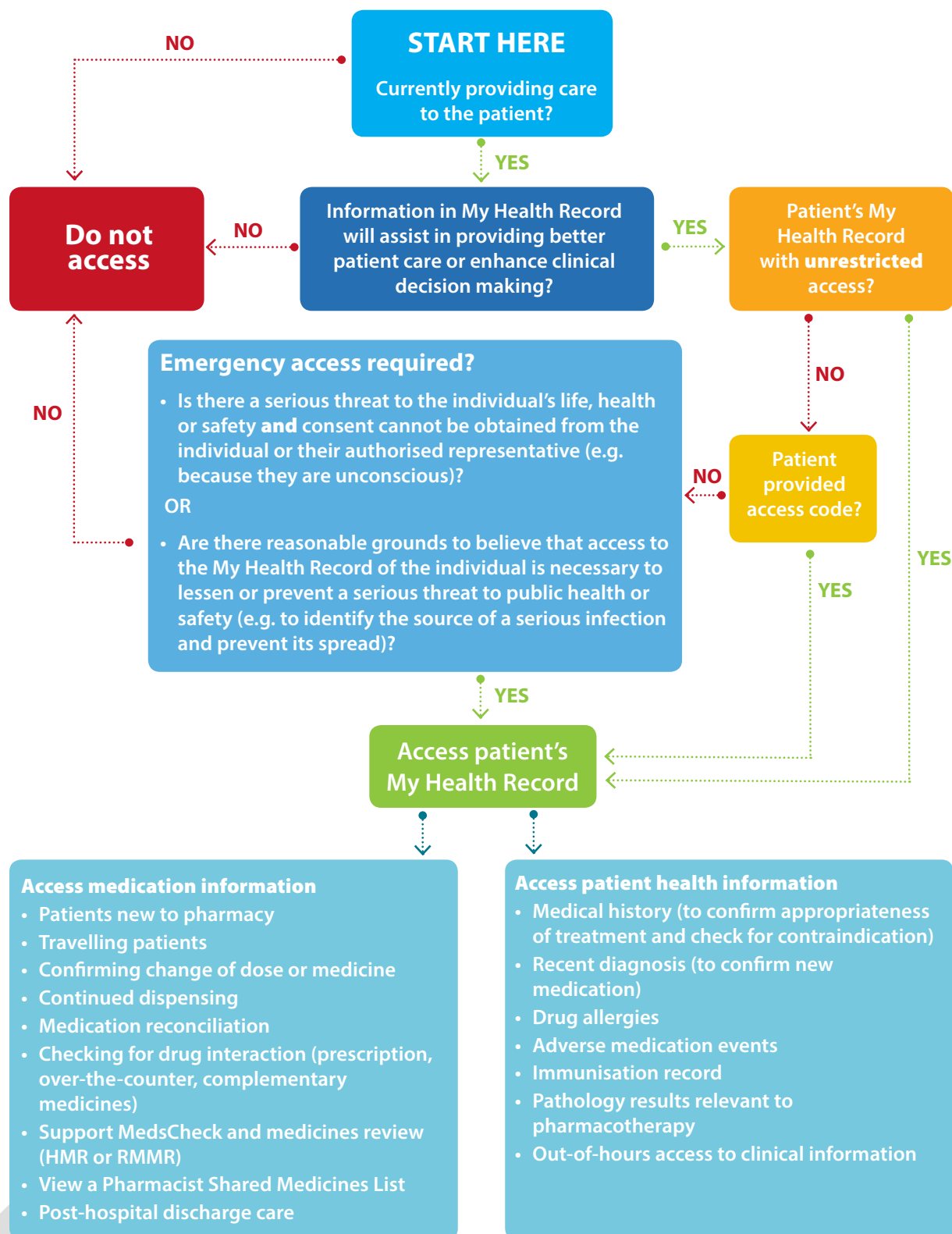
Appendix 4 - Sensitive information

Legislation in some states and territories prevents the disclosure of certain sensitive information unless express or written consent is provided.²⁸ Uploading such information to a patient's My Health Record would be considered disclosure. State and territory-specific information is provided in the following table.

State and territory legislation relevant to uploading sensitive information to the My Health Record system⁵⁴

State or territory	Act	Section
Australian Capital Territory	<i>Public Health Act 1997</i>	Sections 110 and 111 https://www.legislation.act.gov.au/a/1997-69/current/pdf/1997-69.pdf
New South Wales	<i>Public Health Act 2010</i>	Section 56 https://www.legislation.nsw.gov.au/#/view/act/2010/127/part4/div3/sec56
Northern Territory	No specific requirements apply	
Queensland	<i>Public Health Act 2005</i>	Section 55 https://www.legislation.qld.gov.au/view/html/inforce/2018-01-01/act-2005-048#sec.55 Sections 77–79 https://www.legislation.qld.gov.au/view/html/inforce/2018-01-01/act-2005-048#sec.77 Sections 105–107 https://www.legislation.qld.gov.au/view/html/inforce/2018-01-01/act-2005-048#sec.105 Sections 175–177 https://www.legislation.qld.gov.au/view/html/inforce/2018-01-01/act-2005-048#sec.175 Sections 220–222 https://www.legislation.qld.gov.au/view/html/inforce/2018-01-01/act-2005-048#sec.220 Sections 238–240 https://www.legislation.qld.gov.au/view/html/inforce/2018-01-01/act-2005-048#sec.238 Sections 266–268 https://www.legislation.qld.gov.au/view/html/inforce/2018-01-01/act-2005-048#sec.266
South Australia	No specific requirements apply	
Tasmania	No specific requirements apply	
Victoria	No specific requirements apply	
Western Australia	No specific requirements apply	

Appendix 5 - My Health Record decision tool—appropriate access scenarios



Appendix 6 - Standards of documentation

Documentation between healthcare providers must be clear, concise and unambiguous to ensure continuity of patient care.⁵⁵

Two documentation methods commonly used by healthcare providers are:

- SOAP (Subjective, Objective, Assessment, Plan) method
- SBAR (Situation, Background, Assessment, Recommendation) communication technique.

SOAP method

The SOAP method helps to structure documentation in a clear and consistent manner.

There are four distinct sections in this method⁵⁵:

- **Subjective.** Describe the patient's current condition in a narrative form. Include the patient's chief complaints: onset, chronology, quality and severity. Use quotations to document what the patient tells you about how they are feeling, in their own words.
- **Objective.** Document objective, repeatable and measurable facts about the patient's status. Include objective observations about how the patient appears—for example, "Patient appears pale and in discomfort". Include observations and vital signs, findings from physical examination, laboratory results and other measurements (e.g. age, weight, blood pressure).
- **Assessment.** Summarise the most important points and the primary medical diagnosis. If the diagnosis has already been made, comment on whether the patient is clinically improving or deteriorating—for example, "Impression: resolving pneumonia". A complete list of all diagnoses and issues should ideally be created and updated as new issues arise.
- **Plan.** Document a clear plan, further investigations, referrals, procedures, new medications to be charted and estimated follow-up date.

See the SOAP template below.

SBAR communication technique

SBAR is another accepted tool for clinical communication that aims to standardise clinical reporting between healthcare providers in a concise and accurate manner⁵⁶:

- **Situation.** What is the problem? Provide a concise statement of the problem.
- **Background.** What is the background information? Briefly outline the most relevant information related to the situation.
- **Assessment.** What is your assessment of the problem? Analyse and consider what has been found and what you think.
- **Recommendation.** What action/response do you propose? Recommend what action you want to happen.

For further information on SBAR, see the Institute for Healthcare Improvement SBAR toolkit.

SOAP template

Subjective/ Objective		Assessment	Plan		Goals and monitoring parameters	Patient education
Problem: Subjective and objective evidence	Current medicines	Aetiology	Evaluate need for therapy Evaluate current or new therapy Treatment options	Recommended drug treatment Drugs to avoid Follow up		
Subjective evidence: Listen to what the patient is saying about how he/she feels. Observe the patient. Note observations of others.	<ul style="list-style-type: none"> What medicine is the patient taking for the specific problem? All medicines being taken by a patient should correspond to a problem. If not, the problem list is incomplete. Note: some medicines may treat more than one problem 	<ul style="list-style-type: none"> What is the cause of the problem? Does the patient have any risk factors? Is this a medicine-induced disease? 	Need for therapy: Is the problem mild, moderate or severe; stable or progressive; acute or chronic? What would be the outcome if the patient is not treated? Current/recommended therapy: Are all current medicines necessary? State the reason why the regimen (current or recommended) is or is not the BEST regimen for this patient considering other problems and factors (e.g. age, gender, organ function, convenience, cost, etc.) Is the dose, dosage form, route and duration appropriate? Is the patient responding appropriately? Is the patient exhibiting adverse effects? Has the patient been taking the medicine as prescribed? Treatment options: What are all of the options available to manage this problem?	Recommend treatment: <ul style="list-style-type: none"> Continue treatment Discontinue medication—reasons for discontinuation Recommend medicine, dose, dosage form, route, schedule, and duration Begin full dose or titrate Reasons why chosen (stated under Evaluate) Drugs to avoid: Are there reasons why specific medicines are not being used to treat this problem? Why? Should any medicines be specifically avoided in this patient? Why?	Goal: What are the goals for this problem? (e.g. cure, prevent morbidity or mortality, reduce symptoms, return an abnormal lab test to normal, avoid an adverse effect or interaction). Monitoring therapeutic: What are the subjective and objective parameters used to determine if the goals are met? How often should they be performed? How will you know the endpoint has been reached? Monitoring toxic: What are the subjective and objective parameters used to determine if toxic or adverse effects are occurring? How often should they be performed? How will it be determined if they are medication-related? How will the reaction or effect be managed?	<ul style="list-style-type: none"> Use of medicine Administration guidelines Precautions What to do if a dose is missed Storage Anticipated side effects and management Preventative measures and lifestyle changes that may be recommended Education about disease state Improving adherence

Adapted from: <https://pharmacy.ucsd.edu/sites/pharmacy.ucsd.edu/files/docs/faculty-residents/Ambulatory-Care-Sample-Format.pdf>

References

- 1 Australian Digital Health Agency. View a My Health Record. At: www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/view-my-health-record
- 2 Australian Digital Health Agency. What is digital health? At: www.digitalhealth.gov.au/get-started-with-digital-health/what-is-digital-health
- 3 Australian Digital Health Agency. Glossary. At: www.myhealthrecord.gov.au/glossary
- 4 Australian Pharmacy Council. Accredited CPD organisations. 2017. At: www.pharmacycouncil.org.au/our-services/education-providers/accredited-providers/acc_cpd_orgs.pdf
- 5 Pharmaceutical Society of Australia. Professional practice standards. Version 5. Canberra: PSA; 2017.
- 6 Australian Digital Health Agency. Report a clinical incident or issue. At: www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/report-clinical-incident-or-issue
- 7 Pharmaceutical Society of Australia. Definition agreed by the Digital Health Project Advisory Group for the My Health Record guidelines for pharmacists. Canberra: PSA; 2018.
- 8 Neter E, Brainin E. eHealth literacy: extending the digital divide to the realm of health information. *J Med Internet Res* 2012;14(1):e19.
- 9 World Health Organization. The WHO health promotion glossary. Geneva: WHO; 1998. At: www.who.int/healthpromotion/about/HPG/en
- 10 Pharmaceutical Society of Australia. Guidelines for pharmacists providing Home Medicines Review (HMR) services. Canberra: PSA; 2011.
- 11 Pharmaceutical Society of Australia. Guidelines for pharmacists providing MedsCheck and Diabetes MedsCheck services. Canberra: PSA; 2017.
- 12 Australian Digital Health Agency. Access My Health Record using the Provider Portal. At: www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/access-my-health-record-using-provider-portal
- 13 Office of the Australian Information Commissioner. About us. At: www.oaic.gov.au/about-us
- 14 Pharmacy Board of Australia. Provisional to general registration: pharmacy frequently asked questions. 2019. At: www.pharmacyboard.gov.au/Registration/Provisional-to-General-Registration.aspx
- 15 Western Australian Department of Health. Medication reconciliation. At: ww2.health.wa.gov.au/Articles/J_M/Medication-reconciliation
- 16 Australian Government Department of Health. Definitions: point-of-care-testing. 2013. At: www.health.gov.au/internet/publications/publishing.nsf/Content/qupp-review-qupp-definitions
- 17 National Prescribing Service Limited. Better choices, Better health. Competencies required to prescribe medicines: putting quality use of medicines into practice. Sydney: National Prescribing Service Limited; 2012.
- 18 Pharmaceutical Society of Australia. Guidelines for pharmacists providing residential medication management review (RMMR) and quality use of medicines (QUM) services. Canberra: PSA; 2017.
- 19 Office of the Australian Information Commissioner. Australian privacy principles. At: www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles
- 20 Australian Digital Health Agency. Community pharmacy FAQs. 2019. At: www.myhealthrecord.gov.au/sites/default/files/hd173_pharmacyqa_v0.10_20190201_wr.pdf?v=1548994084
- 21 Australian Digital Health Agency. What is in a My Health Record? At: www.myhealthrecord.gov.au/for-healthcare-professionals/what-is-in-my-health-record
- 22 Australian Digital Health Agency. What is My Health Record? At: www.myhealthrecord.gov.au/for-healthcare-professionals/what-is-my-health-record
- 23 Australian Digital Health Agency. Access My Health Record using your clinical information system. At: www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/access-my-health-record-using-your-clinical-information-system
- 24 Office of the Australian Information Commissioner. Healthcare identifiers. At: www.oaic.gov.au/privacy-law/other-legislation/healthcare-identifiers
- 25 Australian Digital Health Agency. My Health Record system security. At: www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/my-health-record-system-security
- 26 Australian Digital Health Agency. Legislation and governance. At: www.myhealthrecord.gov.au/about/legislation-and-governance
- 27 Australian Digital Health Agency. Stronger My Health Record privacy laws. At: www.myhealthrecord.gov.au/about/legislation-and-governance/summary-privacy-protections
- 28 Office of the Australian Information Commissioner. My Health Record access controls. At: www.oaic.gov.au/agencies-and-organisations/my-health-record/my-health-record-access-controls
- 29 Pharmacy Board of Australia. Code of conduct. 2014. At: www.pharmacyboard.gov.au/codes-guidelines/code-of-conduct.aspx
- 30 Australian Digital Health Agency. Understand when you can view and upload information. At: www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/understand-when-you-can-view-and-upload-information
- 31 Australian Digital Health Agency. Remove information. At: www.myhealthrecord.gov.au/for-you-your-family/howtos/remove-information
- 32 Australian Digital Health Agency. Emergency access. At: www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/emergency-access
- 33 Australian Government. Federal Register of Legislation. My Health Records Rule 2016. At: www.legislation.gov.au/Details/F2016C00607
- 34 Australian Digital Health Agency. Authorised representatives. At: www.myhealthrecord.gov.au/for-you-your-family/howtos/authorised-representatives
- 35 Australian Digital Health Agency. Become an authorised representative. At: www.myhealthrecord.gov.au/for-you-your-family/howtos/become-an-authorised-representative
- 36 Authorised representative information provided by the Australian Digital Health Agency Policy & Privacy team via email correspondence, 5 Feb 2019.
- 37 Australian Digital Health Agency. Manage your record from age 14. At: www.myhealthrecord.gov.au/for-you-your-family/howtos/manage-your-record-from-age-14
- 38 Australian Digital Health Agency. Young people and My Health Record. Webinar. 2019.
- 39 Australian Digital Health Agency. Recognise your privacy and security obligations. At: www.digitalhealth.gov.au/using-the-my-health-record-system/maintaining-digital-health-in-your-practice/privacy-and-security-for-digital-health
- 40 Australian Digital Health Agency. Penalties for misuse of health information. At: www.myhealthrecord.gov.au/about/legislation-and-governance/penalties-for-misuse-health-information
- 41 Australian Digital Health Agency. Manage a data breach. At: www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/manage-data-breach
- 42 Australian Commission on Safety and Quality in Health Care. National safety and quality health service standards. Sydney: ACSQHC; 2017. At: www.safetyandquality.gov.au/our-work/assessment-to-the-nsqhs-standards/nsqhs-standards-second-edition
- 43 Australian Digital Health Agency. Access My Health Record using the Provider Portal. At: www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/access-my-health-record-using-provider-portal
- 44 Australian Digital Health Agency. Medicines information view. At: www.myhealthrecord.gov.au/for-healthcare-professionals/howtos/medicines-information-view
- 45 Australian Digital Health Agency. eMedication management. At: www.digitalhealth.gov.au/get-started-with-digital-health/what-is-digital-health/features-of-the-my-health-record-system/emedication-management
- 46 Image agreed by the Digital Health Project Advisory Group for My Health Record Guidelines for Pharmacists, 2018.
- 47 Australian Commission on Safety and Quality in Health Care. Medication reconciliation. 2016. At: www.safetyandquality.gov.au/our-work/medication-safety/medication-reconciliation
- 48 Royal Australian College of General Practitioners. Standard 1.6. In: Standards for general practices. 4th edn. Melbourne: RACGP; 2015. At: www.racgp.org.au/FSDEDEV/media/documents/Running%20a%20practice/Practice%20standards/4th%20edition/Standards-4th-edition.pdf
- 49 NSW Government. Health care records: documentation and management. 2012. At: www1.health.nsw.gov.au/pds/ActivePDSDocuments/PD2012_069.pdf
- 50 Australian Commission on Safety and Quality in Health Care. Recommendations for terminology, abbreviations and symbols used in medicines documentation. Sydney: ACSQHC; 2016. At: www.safetyandquality.gov.au/our-work/Medication-safety/Safer-naming-labelling-and-packaging-of-medicines/Recommendation-for-Terminology-Abbreviations-and-Symbols-used-in-Medicines-Documentation
- 51 Australian Digital Health Agency. See who has accessed your record. At: www.myhealthrecord.gov.au/for-you-your-family/howtos/see-who-has-accessed-your-record
- 52 Digital health. In: Sansom LN ed. Australian pharmaceutical formulary and handbook. 24th edn. Canberra: Pharmaceutical Society of Australia; 2018.
- 53 Australian Commission on Safety and Quality in Health Care. National statement on health literacy. Sydney: ACSQHC; 2014. At: www.safetyandquality.gov.au/publications/health-literacy-national-statement
- 54 Australian Government. My Health Records Regulation 2012. At: www.legislation.gov.au/Details/F2016C00766
- 55 Syed S. Onthewards. How to document well. 2017. At: <https://onthewards.org/how-to-document-well>
- 56 Institute for Healthcare Improvement. SBAR tool: situation-background-assessment-recommendation. 2018. At: www.ihl.org/resources/Pages/Tools/sbartoolkit.aspx
- 57 Siggins Miller. Evaluation of the participation trials for the My Health Record: final report. Canberra: Australian Government Department of Health; 2017. At: www.health.gov.au/internet/main/publishing.nsf/content/health-evaluation-trials
- 58 Office of the Australian Information Commissioner. Privacy business resource 24: health service providers' communications with patients. At: www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-24-health-service-providers-communications-with-patients

PHARMACEUTICAL SOCIETY OF AUSTRALIA LTD.

ABN 49 008 532 072

NATIONAL OFFICE

Level 1, Pharmacy House
17 Denison Street
Deakin ACT 2600
PO Box 42
Deakin West ACT 2600

P: 02 6283 4777
F: 02 6285 2869
E: psa.nat@psa.org.au

BRANCH CONTACT DETAILS

P: 1300 369 772
F: 1300 369 771

AUSTRALIAN

CAPITAL TERRITORY

Level 1, Pharmacy House
17 Denison Street
Deakin ACT 2600

PO Box 42
Deakin West ACT 2600
E: act.branch@psa.org.au

NEW SOUTH WALES

32 Ridge Street
North Sydney NSW 2060
PO Box 162
St Leonards NSW 1590

E: nsw.branch@psa.org.au

QUEENSLAND

Level 2, 225 Montague Road
West End QLD 4101

PO Box 6120
Woolloongabba QLD 4102
E: qld.branch@psa.org.au

SOUTH AUSTRALIA

Suite 7/102
Greenhill Road
Unley SA 5061
E: sa.branch@psa.org.au

TASMANIA

161 Campbell Street
Hobart TAS 7000
E: tas.branch@psa.org.au

VICTORIA

Level 1, 381 Royal Parade
Parkville VIC 3052
E: vic.branch@psa.org.au

WESTERN AUSTRALIA

21 Hamilton Street
Subiaco WA 6008
E: wa.branch@psa.org.au