My Health Record
Guidelines for Pharmacists

Australian Government
Australian Digital Health Agency

PSA Australia’s peak body for pharmacists
## Contents

- Executive summary 4
- Acknowledgements 4
- Introduction 5
- Terminology 6
- About the My Health Record 9
  - System architecture 10
  - Healthcare identifiers 10
  - Legislation 10
  - Privacy 11
  - Consent 11
  - Governance 12
    - Policies and procedures 12
    - Quality assurance 14
- My Health Record and the pharmacist 15
  - Access to the My Health Record 15
    - Access by non-pharmacist staff 16
    - Viewing records 16
    - Documents in the My Health Record 17
    - Medicines Information view 18
    - Prescription and Dispense view 18
  - Contributing clinical information 18
    - Dispensing information 18
    - Event Summaries 19
    - Editing or deleting clinical documents 20
    - Standards of documentation 20
  - Access history 21
- My Health Record and the patient 22
  - Patient control 22
  - Patient support 22
    - Health literacy and eHealth literacy 23
- Appendix 1 – My Health Record system registration flow chart 24
- Appendix 2 - My Health Record Security and access policy 25
- Appendix 3 – Standards of documentation 28
- References 30
Executive summary

The My Health Record system has been designed to allow the secure sharing of patient health information via an electronic platform.\(^1\)

For the pharmacist, greater access to patient health information in this way may:
- enable more efficient and effective medication reconciliation
- enhance their contribution to the quality use of medicines
- improve continuity of patient care.

The ability for pharmacists to contribute patient health information to the My Health Record (e.g. dispense records, immunisation records) may also enhance communication with other healthcare providers caring for their patients, and improve health outcomes.

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

Acknowledgements

The development of the *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**

Shane Jackson, Chair  
Richard Brightwell, Consumers Health Forum  
Allan Groth, Indigenous Allied Health Australia  
Helen Dowling, Medicines Safety Program Steering Group  
Vicki Ibrahim, Australian Digital Health Agency  
William Kelly, Pharmacy Board of Australia  
Grant Martin, Australian Association of Consultant Pharmacy  
Andrew Matthews, Society of Hospital Pharmacists of Australia  
Vincent O’Sullivan, Pharmacy Guild of Australia  
Mike Stephens, National Aboriginal Community Controlled Health Organisation  
Sam Turner, Pharmaceutical Society of Australia  
Gilbert Yeates, Pharmaceutical Defence Limited

*With thanks also to Dr Steve Hambleton for his contribution.*

**Project Working Group**

Chris Campbell, Chair  
Leonie Abbott  
Travis Bailey  
Samantha Bowen  
Rachel Dienaar  
Robert Farrier  
Kenneth Lee  
Irwin Lowe  
Juliet Richards  
Angela Stathopoulos

**Project Team**

Anna Ezzy  
Jill Malek  
Rose Nash  
Jan Ridd
Introduction

The My Health Record provides electronic access to a patient’s key health information including medicines, allergies, medical conditions and test results, and supports improvements in the safety, quality and efficiency of Australia’s healthcare system.²

The need to create a repository to consolidate patient health information has come about in part due to increasing volumes of patient health data, which is 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 expansion program, all Australians will have a record by the end of 2018 unless they choose not to have one. The My Health Record will support timely access to important health information by patients (and their carers, where appropriate) and their treating healthcare providers.

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 and Event Summaries (allergies), contributed to patient records by pharmacists, will help 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 display a sign to advise their patients of their use of, or decision not to use, the My Health Record system.
## Terminology

Please see the table below for definitions of terms commonly appearing in the Guidelines.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Equivalent or related term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access history</td>
<td>An audit trail of all activity related to a patient’s My Health Record detailing when it has been accessed, and when a document has been changed or removed.</td>
<td></td>
</tr>
<tr>
<td>Accredited continuing professional development (CPD) organisation</td>
<td>An organisation able to accredit continuing professional development (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, NPS MedicineWise</td>
<td></td>
</tr>
<tr>
<td>Adverse drug reaction</td>
<td>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.</td>
<td>ADR</td>
</tr>
<tr>
<td>Authorised representative</td>
<td>A person who can participate in and make healthcare decisions for another individual. For the purposes of these guidelines, an authorised representative is someone who has parental responsibility for a person under 18; or has legal authority (i.e. enduring power of attorney or guardianship) to act on behalf of a person who is at least 18 and is not capable of making their own decisions. If no-one has 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 can have more than one authorised representative.</td>
<td></td>
</tr>
<tr>
<td>Clinical incident</td>
<td>A clinical incident is 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 and/or security issues. 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.</td>
<td></td>
</tr>
<tr>
<td>Clinical information system</td>
<td>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 computer system).</td>
<td></td>
</tr>
<tr>
<td>Conformant software</td>
<td>Dispensing or other clinical software capable of interacting with the My Health Record system.</td>
<td></td>
</tr>
<tr>
<td>Delegate</td>
<td>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, according to the healthcare organisation’s My Health Record Security and access policy.</td>
<td></td>
</tr>
<tr>
<td>eHealth literacy</td>
<td>Ability of people to use information and communication technologies to improve or enable health and health care.</td>
<td></td>
</tr>
<tr>
<td>Event Summary</td>
<td>A clinical document that may be uploaded to a patient’s My Health Record summarising one or more episode of care.</td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
<td>Equivalent or related term</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Health literacy</td>
<td>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</td>
<td>HPO</td>
</tr>
<tr>
<td>Healthcare Identifiers service</td>
<td>National system for uniquely identifying healthcare providers and individuals, which makes sure the right health information is associated with the right individual</td>
<td>HI service</td>
</tr>
<tr>
<td>Healthcare provider</td>
<td>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)</td>
<td>Health professional, healthcare practitioner, healthcare professional</td>
</tr>
<tr>
<td>Healthcare provider organisation</td>
<td>An entity, or a part of an entity, that has conducted, conducts, or will conduct, an enterprise that provides healthcare (e.g. community pharmacy, accredited pharmacist)</td>
<td></td>
</tr>
<tr>
<td>Healthcare Provider Identifier – Individual</td>
<td>A unique 16-digit number used to identify individual healthcare providers who deliver healthcare</td>
<td>HPI-I</td>
</tr>
<tr>
<td>Healthcare Provider Identifier – Organisation</td>
<td>A unique 16-digit number used to identify organisations which deliver healthcare in the Australian healthcare setting</td>
<td>HPI-O</td>
</tr>
<tr>
<td>Individual Healthcare Identifier</td>
<td>A unique 16-digit number used to identify individuals who receive, or may receive, healthcare in the Australian health system</td>
<td>IHI</td>
</tr>
<tr>
<td>MedsCheck</td>
<td>A structured and collaborative clinical pharmacy service that takes place in the pharmacy to optimise the impact of medicines on patient health outcomes. This service involves a review of patient medicines, a face-to-face consultation between the pharmacist and patient, the development of a medication profile and an action plan and a follow-up consultation</td>
<td></td>
</tr>
<tr>
<td>My Health Record</td>
<td>An electronic record of an individual’s health information maintained by the Australian Government</td>
<td>Digital health record, eHealth record, Personally Controlled Electronic Health Record (PCEHR)</td>
</tr>
<tr>
<td>My Health Record system</td>
<td>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 one) and healthcare providers</td>
<td></td>
</tr>
<tr>
<td>NASH PKI</td>
<td>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) and secured by tokens such as smartcards. These credentials validate identity when used to access My Health Record systems that are enabled to use NASH authentication</td>
<td></td>
</tr>
<tr>
<td>Network organisation</td>
<td>A healthcare provider organisation with an HPI-O which is part of a network hierarchy. A network organisation may be set up to work under a seed organisation. A 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</td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
<td>Equivalent or related term</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Organisation Maintenance Officer</td>
<td>A person who undertakes the day-to-day administrative tasks in relation to the HI-service and the My Health Record. An OMO needs to be someone who is familiar with the IT system used by the organisation. The OMO is responsible for understanding, implementation and compliance monitoring of the My Health Record security and access policy, and for maintenance of the policy on behalf of the organisation. A healthcare provider organisation can have multiple OMOs</td>
<td>OMO</td>
</tr>
<tr>
<td>Office of the Australian Information Commissioner</td>
<td>Key regulator for the My Health Record system that has the capacity to conduct audits, commence investigations, impose sanctions and accept enforceable undertakings</td>
<td>OAIC</td>
</tr>
<tr>
<td>Patient</td>
<td>A person who uses, or is a potential user of, health services, including their family and carers</td>
<td>Consumer, healthcare recipient, client</td>
</tr>
<tr>
<td>Pharmacist</td>
<td>A provisionally or generally registered practicing pharmacist registered with the Pharmacy Board of Australia within the Australian Health Practitioner Regulation Agency (AHPRA)</td>
<td>Intern pharmacist, registered pharmacist</td>
</tr>
<tr>
<td>Pharmacy organisation</td>
<td>Organisation or business providing pharmaceutical services to patients</td>
<td>Community pharmacy, pharmacy department, pharmacy business (e.g. accredited pharmacist)</td>
</tr>
<tr>
<td>Point of care</td>
<td>Refers to the location where care is provided (e.g. ambulance, general practice, patient's home, hospital, pharmacy)</td>
<td></td>
</tr>
<tr>
<td>Prescriber</td>
<td>A healthcare provider who is responsible for patient care, specifically medicines</td>
<td>Doctor, dentist, general practitioner (GP), nurse practitioner, optometrist, other approved prescribers, specialist</td>
</tr>
<tr>
<td>Provider portal</td>
<td>A view-only interface through which healthcare provider organisations can access the My Health Record system without having to use a clinical information system</td>
<td></td>
</tr>
<tr>
<td>Responsible Officer</td>
<td>A person who has legal responsibility for understanding and compliance with the My Health Record Security and access policy and compliance with My Health Record legislation (e.g. pharmacy owner, pharmacist manager)</td>
<td>RO</td>
</tr>
<tr>
<td>Seed organisation</td>
<td>A healthcare provider organisation with an HPI-O that is a legal entity which is the head of a network hierarchy that may or may not include subordinate network organisations</td>
<td></td>
</tr>
<tr>
<td>Sensitive information</td>
<td>A type of personal information that includes health information about the person (e.g. genetic information, biometric information)</td>
<td></td>
</tr>
<tr>
<td>System Operator</td>
<td>Australian Digital Health Agency who is responsible for establishing and operating the My Health Record system</td>
<td>SO</td>
</tr>
<tr>
<td>Vulnerable persons</td>
<td>A child under the age of 18, or an individual aged 18 years and above who is or may be unable to take care of themselves, or is unable to protect themselves against harm or exploitation by reason of age, illness, trauma or disability, or any other reason</td>
<td></td>
</tr>
</tbody>
</table>

References: Neter¹; PSA²; PBA³; Australian Digital Health Agency⁴; Department of Health⁵; Department of Social Services⁶; PSA⁷; APC⁸
About the My Health Record

My Health Record is an electronic summary of an individual’s key health information, drawn from their existing records and designed to be integrated into existing local clinical information systems.11

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, not all healthcare providers use the My Health Record system or upload every clinical patient interaction, therefore it cannot be assumed to be a complete record.

Healthcare providers are able to upload different clinical documents to a patient’s My Health Record, as determined by their role (see Figure 2).

Figure 1. Information contained in a My Health Record

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

Reference: Australian Digital Health Agency11,12
System architecture

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

The system has been designed to:

- allow patients to control the content of their record, including which healthcare provider organisations can access their record
- enable healthcare providers to access their 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 healthcare 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 and should not be relied upon as the only source of patient health information.

Healthcare identifiers

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

To ensure the security of the information contained in the My Health Record system, organisations must register and obtain digital credentials (i.e. NASH PKI certificates) before accessing the HI service. These certificates authenticate the identity of the organisation and individual accessing the service. See Appendix 1 - My Health Record registration flow chart.

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 service:

- HPI-I – Healthcare provider identifier – Individual (e.g. a pharmacist)
- HPI-O – Healthcare provider identifier – Organisation delivering health care (e.g. a pharmacy or pharmacy department, accredited pharmacist)
- IHI – Individual healthcare identifier as assigned to the patient.

Healthcare identifiers are interlinked in the context of a healthcare event.

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. This covers documents and processes such as electronic referrals, discharge summaries and medication management.

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.

Pharmacists using the system must comply with obligations outlined in the relevant legislation (see Box 1).

Box 1. My Health Record 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 this 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

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 must 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](https://www.pharmacy.org.au/policy/code-conduct-pharmacists) also makes explicit reference to the pharmacist’s responsibilities in managing their use of the My Health Record.

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 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. All patient information must also be managed in accordance with the PSA Professional Practice Standards, Standard 1: Fundamental Pharmacy Practice. A policy must be in place in the pharmacy organisation to uphold privacy (see Appendix 2 - My Health Record Security and access policy).

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

All patient health information, including information accessed from a patient’s My Health Record, must be kept confidential and secure.

For further information about privacy, see:
- My Health Record Security and access policy (Appendix 2)

Consent

The legislative framework governing the My Health Record system allows a healthcare provider of a participating organisation to view 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.

Currently, patients provide standing consent when they register for a My Health Record. This enables all healthcare provider organisations directly involved in their care to upload clinical information to their record.

Generally, there is no requirement for a healthcare provider directly involved in a patient’s care to obtain consent prior to viewing or uploading clinical information to the My Health Record system. There is also no requirement for a patient to review clinical information prior to it being uploaded.

Standing consent is subject to two important exceptions:
- A patient has asked that all records, or 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 in a record, particular information without consent (see Sensitive information).

Regardless of consent requirements, it is good practice to advise patients when information is being uploaded to their My Health Record (e.g. by displaying a sign indicating that all prescriptions will be uploaded to the patient’s My Health Record by this pharmacy).

Sensitive information

Some jurisdictions enforce local requirements for patient consent. Particularly sensitive information (e.g. information relating to screening and/or diagnoses of certain cancers or notifiable conditions, such as HIV infection) may require the express or written consent of the patient to share that information with other healthcare providers, and therefore to upload to their My Health Record.

Pharmacists should refer to State or Territory legislation for further information about specific patient consent requirements (see Table 1).

Table 1. State and Territory legislation relevant to uploading of sensitive information

<table>
<thead>
<tr>
<th>State or Territory</th>
<th>Act</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australian Capital Territory</td>
<td>Public Health Act 1997</td>
<td>Section 110 to 111</td>
</tr>
<tr>
<td>New South Wales</td>
<td>Public Health Act 2010</td>
<td>Section 56</td>
</tr>
<tr>
<td>Northern Territory</td>
<td>No specific requirements apply</td>
<td></td>
</tr>
<tr>
<td>Queensland</td>
<td>Public Health Act 2005</td>
<td>Section 55</td>
</tr>
<tr>
<td>South Australia</td>
<td>No specific requirements apply</td>
<td></td>
</tr>
<tr>
<td>Tasmania</td>
<td>No specific requirements apply</td>
<td></td>
</tr>
<tr>
<td>Victoria</td>
<td>No specific requirements apply</td>
<td></td>
</tr>
<tr>
<td>Western Australia</td>
<td>No specific requirements apply</td>
<td></td>
</tr>
</tbody>
</table>

Emergency situations

In certain emergency situations (e.g. 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 if:

- 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.

* Following the opt-out period, consent to upload documents will be authorised through My Health Record legislation.
In such situations, if a patient has applied an access code to their My Health Record, healthcare providers may use emergency access to override any access controls that have been set by the patient.

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 for:

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

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

Emergency access is recorded in the access history of the My Health Record, which can be viewed by the patient. The patient can choose to be notified if and when anyone gains emergency access to their My Health Record. 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 clinical information system).

**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.

As 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.

**Authorised representatives**

Children, minors and other vulnerable people, who are unable to manage their own My Health Record, will have their record controlled by an authorised representative.

Authorised representatives can access, view and update the information in the individual’s My Health Record, as well as add or remove other people as 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.

A child under the age of 14 can apply to the System Operator to take control of their My Health Record if they can provide evidence they have capacity to make decisions about their health care and manage their record.

Children aged over 14 years can control and manage their My Health Record if they choose. Alternatively, their parent or guardian can continue as an authorised representative until the child’s 18th birthday. However, authorised representatives will not be able to view the Medical Benefits Schedule (MBS), or Pharmaceutical Benefits Scheme (PBS) information or Immunisation Register details of children aged over 14 years.

**Governance**

**Policies and procedures**

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 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.

Under the rule, pharmacy organisations must develop and maintain a robust security and access policy that details certain access and security procedures for the organisation, how authorised persons access the system, the training delivered to staff before accessing the My Health Record system, and the physical and information security measures used by the organisation. Organisations must review, update, maintain, enforce and promote to staff the policies that ensure the My Health Record system is used safely and responsibly. See Appendix 2 - My Health Record Security and access policy.

It is the responsibility of the pharmacy organisation 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 (e.g. screen saver mode is automatically activated when a page is inactive for more than one minute, clinical information systems are password protected, passwords are changed regularly).

There are penalties for the misuse (e.g. inappropriate collection, or disclosure of patient data) of any information contained in a patient’s My Health Record.
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 approved process for managing clinical incidents, outlined 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. However other clinical incidents will require the pharmacy organisation to contact a relevant third party, such as the System Operator, police, or the Office of Australian Information Commission (see Table 2). Pharmacists should consider the need to notify their professional indemnity insurer following a clinical incident.

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 2 - My Health Record Security and access policy.

Table 2. Managing clinical incidents

<table>
<thead>
<tr>
<th>Issue</th>
<th>Action</th>
</tr>
</thead>
</table>
| Error in a document (e.g. dispense record) uploaded to a patient’s My Health Record | If you made the error:  
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  
If you are unable to delete the erroneous document, contact the System Operator (1800 723 471)  
*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*
If another healthcare provider made the error:  
1. Contact and inform the patient that you have identified an error in their My Health Record  
2. Encourage the patient to exercise their right to have it corrected by the healthcare provider who uploaded the information, or offer to follow up with the healthcare provider yourself  
3. Suggest the patient hide the incorrect document, to avoid confusion while the error is corrected. If they require assistance to do this, refer them to the My Health Record helpline (1800 723 471)  
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 | Advise the patient that they can permanently hide the document from view in their My Health Record, and refer them to the My Health Record helpline (1800 723 471) if necessary  
If the issue is not resolved, contact the My Health Record helpline on 1800 723 471 |
| Upload of a document (e.g. dispense record) to the wrong patient’s My Health Record | 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 on 1800 723 471 and they can do it on your behalf  
2. Upload a new, corrected version  
3. Record this action in your own notes |
| Suspected security breach | 1. Suspend/de-activate the user account  
2. Change the password information for the account  
3. Report the breach to the police, and if relevant (see Appendix 2 Explanatory notes):  
  a) System Operator (1800 723 471)  
  b) Office of Australian Information Commission (1300 363 992) |
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 there has been no dispensing in the previous twelve 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. My Health Record system 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.

Staff training should provide information about how to use the conformant software, and/or the My Health Record provider portal, to access a patient’s My Health Record accurately and responsibly, and include privacy training (see Box 2). All staff training should be documented.


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 their 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 2).

Box 2. My Health Record system training

System training should include:

- use of conformant software and/or the 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)
- processes to follow if there is a clinical incident 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 GPs, 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 3 - Standards of documentation)
- 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

To provide measurable quality improvement systems that will assure quality delivery of the interaction, the pharmacy organisation must be able to:

- identify and log any clinical incidents (including near misses)
- identify and log potential ways breaches of patient safety and security may occur
- review work practices to prevent recurrence of clinical incidents
- implement any 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, see Australian Commission on Safety and Quality in Health Care National Safety and Quality Health Service Standards 2017.
My Health Record and the pharmacist

The My Health Record system provides pharmacists with a platform to enhance provision of patient-centred care, both through access to key patient health information, and by the contribution of clinical records of care they have provided (e.g. dispense records).

However, 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.

Access to the My Health Record

Pharmacists can access a patient’s My Health Record through:

- conformant software enabling pharmacists to view records via their clinical information system, and upload relevant patient clinical information
- the provider portal, which enables pharmacists without conformant software to search and view patient health records through their web browser (Note: documents cannot be uploaded to a patient’s My Health Record via the provider portal).

Box 3. Patient records, healthcare identifiers and My Health Record access

Patient records in the clinical information system need to be complete and accurate to access that patient’s My Health Record.

Correct patient information will assist the pharmacist to search and match against information held by the HI service, including:

- name
- surname
- date of birth
- gender
- Medicare number (including individual reference number) or Department of Veterans' Affairs (DVA) number

In some circumstances, changes to work practices and workflows may be required to ensure that information such as date of birth and gender are captured in the patient’s record in the clinical information system.

Pharmacists are responsible for the quality of the data contained in their clinical information system, and should consider the need for data cleaning.
To view and 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 (Note: 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 3)).

In addition, if pharmacists are using the provider portal to view a patient’s My Health Record, they will also need NASH PKI Certificate (e.g. a USB key or smart card) that identifies them as an authorised healthcare provider.

For further information about registering with the HI service, and applying for healthcare identifiers, pharmacists should refer to Australian Digital Health Agency at: www.digitalhealth.gov.au/using-the-my-health-record-system/for-pharmacists

Access by non-pharmacist staff

Non-pharmacist staff do not hold a HPI-I, and therefore can only use the My Health Record system if a pharmacist delegates them access.

Pharmacists should determine the need for non-pharmacists to access the My Health Record system based on their position description and role. Access to the My Health Record system by non-pharmacists must be clearly defined in the organisation’s Security and access policy (see Appendix 2).

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 delegating pharmacist’s HPI-I.

Viewing records

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

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 (i.e. enhance clinical decision-making when a clinical issue or problem has been identified). See Box 4 for example reasons for accessing a patient’s My Health Record.

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

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
- **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
- **clinical significance** — professional judgement must be used to determine if a document is clinically relevant to the care the pharmacist is providing
- **source** — the source of any document should be reviewed for appropriateness, as all healthcare providers with an HPI-I have the potential to upload information to a patient’s My Health Record.

It is important to note that the 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/carer or prescriber) in addition to, or instead of, a patient’s My Health Record, in order to provide safe and appropriate patient care.

Pharmacists should ensure reasonable attempts are made to access information required to inform appropriate clinical decisions.

---

**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.

---

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

^ For example, some information (e.g. S100 dispensing information) may not be patient-linked, and therefore may be absent from the patient’s My Health Record.
Box 4. Example reasons for accessing 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, non-prescription medicines
- Access clinical information, such as discharge summaries, medication summaries, 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

Documents in the My Health Record

The following clinical documents may be available in a patient’s My Health Record:

- **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 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. indicating a clinical intervention, improvement in a condition, treatment 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.
- **Prescription records**—a document containing information about the medications (PBS, Repatriation Pharmaceutical Benefits Scheme [RPBS] and private) prescribed to a patient, including brand name and active ingredient/s, strength, dosage instructions, maximum number of repeats, date of prescribing, prescription expiry date, the healthcare provider that prescribed the medication and the healthcare provider organisation that the patient visited.
- **Dispense records**—a document containing information about the medications (PBS, RPBS and private) dispensed to a patient, including brand name and active ingredient/s, 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.

Using a patient’s Discharge Summary

*Mrs Nyugen 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 Nyugen 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 Nyugen’s My Health Record. He views her most recent discharge summary and identifies the medicines she was discharged on. With this additional information, Andrew is able reconcile her medicines and update her medication profile.
Medicines Information view
The Medicines Information view can quickly sort and display medicines information held in a patient’s My Health Record documents in date or alphabetical order. The medicines information is gathered from the:

- patient’s most recent (and up to two years) prescription and dispense records and other PBS and PRBS claim information
- patient’s most recent Shared Health Summary and Discharge Summary
- 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 that may include any allergies or 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.

The view displays:
- the name and date a medication has been prescribed and dispensed (both the brand name as well as the active ingredient/s)
- the strength and form of the medication
- directions for use.

Using the Prescription and Dispense view
Ms Smith, a 23-year-old female, 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, who 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 in fact 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 three 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. Pharmacists 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 clinical information system 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 their organisation’s clinical information system.

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

Dispensing information
There are several ways that dispensing information is uploaded to the My Health Record system.

- Conformant software: 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 used (e.g. a pharmacist with an HPI-I and granted access by their organisation) will be uploaded.

- PBS and RPBS claim information: dispensing information from PBS and RPBS claims will flow automatically to a patient’s My Health Record, regardless of whether the pharmacy organisation is using the My Health Record system. There can be a delay of up to 6 weeks for information to be uploaded.

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 three 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 three years earlier, however, 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.
**Right medicine, right patient, wrong record**

David, the pharmacist, has suggested to George Whyte (85) that he would benefit from having his medicines packed in a dose administration aid (DAA). Mr Whyte is being treated for high cholesterol, fluid retention, lower back pain and peptic ulcer disease. Prior to 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 via the Medicines Information View. He notices 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 the diagnosis for 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 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 the correct patient is selected in dispensing software, and consequently the dispense record is uploaded to the correct patient’s My Health Record.

In either case, dispensing information will only be uploaded if the patient has an active My Health Record, and has not withdrawn consent (see Figure 3).

For software-specific information, pharmacists should consult their software vendor.

**Event Summaries**

Pharmacists can contribute patient allergy information to the 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 the My Health Record. This functionality may not be available in all conformant software systems.

In the future pharmacists may be able to add other significant patient health information to the My Health Record as an event summary, enabling pharmacists to document meaningful clinical information associated with the provision of professional services (i.e. MedsChecks, Home Medicines Reviews, 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 5).

---

**Box 5. 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:

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

The author of a clinical document (e.g. dispense record or Event Summary) can delete it from a patient’s My Health Record if it has been uploaded in error or contains a mistake. Clinical documents cannot be edited in the My Health Record system.

In the event of an error or mistake, a pharmacist can replace the clinical document by editing it in the pharmacy dispensing software or other clinical information software. The edited version is then uploaded and supersedes the original.27

If a pharmacist identifies an error in a document upload 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).

Standards of documentation

Pharmacists have a responsibility to ensure that all clinical documents uploaded to a patient’s My Health Record are of clinical benefit to other healthcare providers.

In future, pharmacists could upload an Event Summary to a patient’s My Health Record, where it can be accessed by a broad range of 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, and 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.28

Clinical documents uploaded to a patient’s My Health Record should contain26,27:

- date of consultation
- author’s printed name, designation, place of practice and signature
- 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
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 Mr Brown’s newly prescribed medicine via information in:

- Medicines Information View that 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.

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 displays:

- name of the healthcare provider organisation that accessed the patient’s My Health Record
- time the record was accessed
- 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 in error, 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 and why their health information and activities are recorded in their My Health Record and accessed by pharmacists and pharmacy staff.

When communicating with patients about My Health Record, pharmacists should consider the patient’s health and ehealth literacy, cognition, culture and beliefs and the need to involve other primary healthcare team members, family and carers, and/or translators.17

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 can15:

- choose whether they have a record
- cancel their record at anytime
- 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 restrict access to, or hide from view, 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).4 Restrictions can be applied to all organisations, or specific organisations 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.18 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 the access code.

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

Patient support

Patients need to 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 could be shared via their My Health Record and the implications of not sharing key pieces of their health information. 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. At: www.digitalhealth.gov.au/using-the-my-health-record-system/consumer-guides

---

15 Currently, the My Health Record is an opt-in system. Under the My Health Record Rule, My Health Record will move to an opt-out system in 2018 with a designated opt-out period when patients can indicate their choice not to have a My Health Record.

18 While the My Health Record system enables this functionality, results from the trial of the opt-out system indicate most patients do not invoke access controls.19
Supporting informed decision making

Joe (54 years), a regular patient at Gary’s pharmacy, presents with a prescription for vardenafil. Joe specifically requests 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 firstly 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. However, after talking to Gary, Joe decides to allow the dispense record to be included in his My Health Record without applying an access code.

Both health literacy and eHealth literacy are dynamic and are influenced by context (e.g. illness, hospitalisation). Pharmacists should consider their patient’s health literacy and eHealth literacy in order to provide tailored support and promote engagement with the My Health Record system.32


Box 6. 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 information has been delivered and received effectively
- encouraging people to speak up if they have difficulty understanding the information provided
- using ways of communicating risk information about treatment options that have been demonstrated to be effective.

Adapted from ASCQHC32

Health literacy and eHealth literacy

Health literacy is important to the safety, quality and effectiveness of healthcare. If patients do not understand the information and services they are provided, then they may be at higher risk of experiencing poor health outcomes. eHealth literacy is affected by health literacy. Patient engagement with the My Health Record system relies on their eHealth literacy, as well their level of social support and the responsiveness of healthcare providers and the health system.32

About 60% of patients don’t have adequate health literacy to make well informed health decisions and act on them. By responding to the patient’s health literacy and providing support, effective partnerships can be forged between the patient and the healthcare provider, building the patient’s capacity to make informed healthcare decisions (see Box 6).32
My Health Record Registration Guide
for Community Pharmacies using Conformant Clinical Information Systems
Developed for Primary Health Networks and pharmacy owners

Appendix 1 - My Health Record system registration flow chart

Is the pharmacy registered with the My Health Record System?

- no
  - Check if the pharmacy has a current and available:
    - Healthcare Provider Identifier Organisation (HPI-O)
    - Organisational NASH certificate
    - Personal Identification Code (PIC)

  - Missing HPI-O
    - Call 1300 361 457
      (Responsible Officer (RO) or Organisational Maintenance Officer (OMO) Only)
    - Receive HPI-O
  - Missing organisational NASH certificate
    - Call 1800 700 199
      (Responsible Officer (RO) or Organisational Maintenance Officer (OMO) Only)
    - Apply to re-issue certificate
    - Receive organisational NASH certificate
  - Missing PIC
    - Apply for organisational NASH certificate
    - Call 1800 700 199
      (Responsible Officer (RO) or Organisational Maintenance Officer (OMO) Only)
    - Receive PIC

- yes
  - Has there been a change in business details since registration?
    - yes
      - Change in business details*
        - Retire existing application
        - Complete and submit streamlined registration form
        - Receive:
          - Healthcare Provider Identifier Organisation (HPI-O)
          - Organisational NASH certificate
          - Personal Identification Code (PIC)
    - no
      - Is the pharmacy using FRED Dispense or Aquarius?
        - yes
          - All pharmacists are required to publish their details in secure Healthcare Provider Directory (HPD).
          - Contact dispensing software vendor for configuration
          - Pharmacy is registered to the My Health Record system
        - no
          - Complete and submit streamlined registration form
          - Receive:
            - Healthcare Provider Identifier Organisation (HPI-O)
            - Organisational NASH certificate
            - Personal Identification Code (PIC)

- no
  - Is the pharmacy using FRED Dispense or Aquarius?
    - yes
      - Contact dispensing software vendor for configuration
      - Pharmacy is registered to the My Health Record system
    - no
      - Complete and submit streamlined registration form
      - Receive:
        - Healthcare Provider Identifier Organisation (HPI-O)
        - Organisational NASH certificate
        - Personal Identification Code (PIC)

*Change in business details refers to a change in the ABN and/or PBS approval number. Click here for common scenarios outlining changes in business details.
## Appendix 2 - My Health Record Security and access policy

### My Health Record Security and Access Policy

<table>
<thead>
<tr>
<th>Governance</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Officer (RO)</td>
<td></td>
</tr>
<tr>
<td>Organisation Maintenance Officer/s (OMO)</td>
<td>1.</td>
</tr>
<tr>
<td></td>
<td>2.</td>
</tr>
<tr>
<td></td>
<td>3.</td>
</tr>
<tr>
<td></td>
<td>4.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorised staff will access the My Health Record system via:</td>
<td></td>
</tr>
<tr>
<td>An up-to-date list of individual healthcare providers authorised to access the Provider Portal to the System Operator (SO) by:</td>
<td></td>
</tr>
<tr>
<td>Authorised staff will be provided with a unique user account to access the My Health Record System via conformant software by:</td>
<td></td>
</tr>
<tr>
<td>The level of access granted to individual staff will be determined and documented by:</td>
<td></td>
</tr>
<tr>
<td>Access flags will be assigned by:</td>
<td></td>
</tr>
<tr>
<td>Access records will be maintained by:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User account information and access will be managed by:</td>
<td></td>
</tr>
<tr>
<td>Account passwords will be changed by users every:</td>
<td></td>
</tr>
<tr>
<td>Staff will report any suspected security breach to:</td>
<td></td>
</tr>
<tr>
<td>Confirmed security breaches will be reported to the relevant authority by:</td>
<td></td>
</tr>
<tr>
<td>A log of security breaches, including date and time of the breach, user account involved and patient information accessed (if known), and mitigation strategies employed, will be maintained by:</td>
<td></td>
</tr>
<tr>
<td>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:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Training</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>My Health Record system training will be organised for all authorised staff before they first access the system by:</td>
<td></td>
</tr>
<tr>
<td>A register of staff training, including the names of those who have completed training and the date training was completed will be maintain by:</td>
<td></td>
</tr>
<tr>
<td>Training will be reviewed to ensure currency and updated as required (i.e. if new functionality is introduced into the system) every:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Clinical incidents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Clinical incidents will be reported to the relevant party by:</td>
<td></td>
</tr>
<tr>
<td>A log of reported clinical incidents will be maintained by:</td>
<td></td>
</tr>
<tr>
<td>Clinical incident management is the responsibility of:</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Patient complaints</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient complaints regarding the My Health Record will be redirected to the My Health Record Helpline (1800 723 471) or will be referred to:</td>
<td></td>
</tr>
</tbody>
</table>
Explanatory notes

Governance

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

Organisation Maintenance Operator (OMO): 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 [insert organisation name]. OMO is responsible for understanding, implementing and compliance monitoring of the My Health Record 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 My Health Record system where access is required for the provision of patient care. The OMO will maintain a record of authorised Healthcare Provider Identifier – Individual (HI-I) numbers, and the level of access granted, in the clinical software and in the organisation’s internal records.

Provider portal: means the portal provided by the System Operator that allows for identified healthcare providers from participating healthcare provider organisations to access the My Health Record system without having to use a conformant clinical information system.

Where individual healthcare providers are authorised to access the My Health Record system, using the 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 provider portal on behalf of the organisation, the OMO will ensure 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 regarding issues with the My Health Record 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. This unique identification code will be recorded by the clinical software against any My Health Record system access. Staff will use their individual user account to access the My Health Record 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 My Health Record. 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, including a dispensary or pharmacy assistants whom may be granted a view access to My Health Record system Provider Portal, in order to access the My Health Record 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 health care 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 that seed organisation, and the network organisations for whom access flags are appropriate.

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

• Health care recipients are able to determine and control access to their My Health Record in a way that meets reasonable public expectations. Network organisations that would not be expected by health care 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 at such times as the structure changes, or in the case that a System Operator or health care 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 which user 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 which 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

Security breach: means instances of unauthorised collection, use or disclosure of health information included in a health care recipient’s My Health Record, for example when a staff member with access to the My Health Record system discovers that someone else may have gained access to their user account.

Relevant authority: where 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 is compromised, the Office of Australian Information Commission will be notified. If the breach involved the My Health Record 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 but not limited to:

• 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 Australian Information Commission 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

My Health Record system training: Staff training will provide information about how to use the conformant software, and/or the My Health Record system Provider Portal, in order to access the My Health Record system accurately, responsibly, and will include privacy training. Training will utilise materials approved by the 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 My Health Record, there is a version upgrade and release to pharmacy dispensing software. Training material produced by the Agency and/or peak organisations material will be updated to reflect new functionalities as they become available and published for public use. Additional training to staff with authorised access may need to be provided 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 and/or security issues. The incident may relate to the My Health Record system directly, or the behaviour of clinical software when interacting with the My Health Record 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 as necessary.
Clinical incidents management

<table>
<thead>
<tr>
<th>Issue</th>
<th>Action</th>
</tr>
</thead>
</table>
| Error in a document (i.e. dispense record) uploaded to a patient’s My Health Record | If you made the error:  
1. Delete the incorrect document (i.e. dispense record) from your dispensing system immediately and re-dispense.  
2. Upload the new, corrected version  
3. Record all actions in your notes  
If you are unable to delete the erroneous document, contact the System Operator (1800 723 471).  
**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.  
If another healthcare provider made an error:  
1. Contact and inform the individual that you have identified an error in their My Health Record.  
2. Encourage the individual to exercise their right to have it corrected by the healthcare provider who uploaded the information, or offer to follow up with the healthcare provider yourself.  
3. Suggest the consumer delete the incorrect document while the error is corrected. If they require assistance to do this, refer them to the My Health Record Helpline (1800 723 471).  
Record your actions in your own notes. |
| Upload of document (i.e. dispense record) if consent has been withdrawn | Advise the patient that they can remove the document from their My Health Record, and refer them to the My Health Record Helpline (1800 723 471) if necessary.  
If the issue is not resolved contact the My Health Record Helpline on 1800 723 471. |
| Upload of document (i.e. dispense record) to wrong patient’s My Health Record | If you have made an error in a document you have uploaded:  
1. Delete the incorrect document (i.e. dispense record) immediately from the dispensing software and insert “incorrect identity” as the reason. If you are unable to delete, please contact the My Health Record Helpline on 1800 723 471 and they can do it on your behalf;  
2. Upload a new, corrected version; and  
3. Record this action in your own notes. |
| Suspected security breach                                              | • Suspend/deactivate the user account  
• Change the password information for the account  
• Report the breach to the police, and if relevant (see relevant authority)  
  • the System Operator (1800 723 471)  
  • the Office of Australian Information Commission (1300 363 992) |

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 health care recipient and the complaint will be referred to the management of that service and/or the Office of the Information Commissioner.

Where a health care recipient requests a document is 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 health care recipient will be directed to exercise their personal controls over the document.

Policy Manager:  
Contact: Tel:  
Approval Authority:  
Latest Review Date:  
My Health Record Guidelines for Pharmacists
Appendix 3 - Standards of documentation

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

**Subjective:** This section describes 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, BP).

**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 completed and updated as new issues arise.

**Plan:** Document a clear plan, further investigations, referrals, procedures, new medications to be charted, estimated follow up date.

See SOAP template below.

SBAR communication technique

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

**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 SBAR toolkit, Institute for Healthcare Improvement at: www.ihi.org/resources/Pages/Tools/sbartoolkit.aspx
### SOAP template

<table>
<thead>
<tr>
<th><strong>Subjective/ Objective</strong></th>
<th><strong>Assessment</strong></th>
<th><strong>Plan</strong></th>
<th><strong>Goals and monitoring parameters</strong></th>
<th><strong>Patient education</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Problem:</strong> Subjective and objective evidence</td>
<td><strong>Current medicines</strong></td>
<td><strong>Aetiology</strong></td>
<td><strong>Evaluate need for therapy</strong></td>
<td><strong>Recommended drug treatment</strong></td>
</tr>
<tr>
<td>Subjective evidence</td>
<td>- What medicine is the patient taking for the specific problem?</td>
<td>- What is the cause of the problem?</td>
<td>Need for therapy</td>
<td>- Continue treatment</td>
</tr>
<tr>
<td>Subjective evidence</td>
<td>- 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</td>
<td>- Does the patient have any risk factors?</td>
<td>Need for therapy</td>
<td>- Discontinue medication—reasons for discontinuation</td>
</tr>
<tr>
<td>Objective evidence</td>
<td>- Listen to what the patient is saying about how he/she feels.</td>
<td>- Is this a medicine-induced disease?</td>
<td>Need for therapy</td>
<td>- Recommend medicine, dose, dosage form, route, schedule, and duration</td>
</tr>
<tr>
<td>Objective evidence</td>
<td>- Observe the patient.</td>
<td>- Evaluate current or new therapy</td>
<td>Need for therapy</td>
<td>- Begin full dose or titrate</td>
</tr>
<tr>
<td>Objective evidence</td>
<td>- Note observations of others.</td>
<td>- Treatment options</td>
<td>Need for therapy</td>
<td>- Reasons why chosen (stated under Evaluate)</td>
</tr>
<tr>
<td>Objective evidence</td>
<td>- Laboratory test results</td>
<td>- Subjective evidence: Listen to what the patient is saying about how he/she feels.</td>
<td>Need for therapy</td>
<td>- Drugs to avoid</td>
</tr>
<tr>
<td>Objective evidence</td>
<td>- Physical assessment parameters</td>
<td>- Observe the patient.</td>
<td>Need for therapy</td>
<td>- Should any medicines be specifically avoided in this patient?</td>
</tr>
<tr>
<td>Objective evidence</td>
<td>- Results of procedures and other diagnostic tests</td>
<td>- Note observations of others.</td>
<td>Need for therapy</td>
<td>- Why?</td>
</tr>
<tr>
<td>Objective evidence</td>
<td>- History as documented in the medical record</td>
<td>- Subjective evidence: Listen to what the patient is saying about how he/she feels.</td>
<td>Need for therapy</td>
<td>- Follow up:</td>
</tr>
</tbody>
</table>

Adapted from: [http://pharmacy.ucsd.edu/faculty/ExperientialEducation/docs/FA_SOP_forms_2_29_12_AMPC.pdf](http://pharmacy.ucsd.edu/faculty/ExperientialEducation/docs/FA_SOP_forms_2_29_12_AMPC.pdf)
References


My Health Record Guidelines for Pharmacists