Pharmaceutical Society of Australia

Australian Government
Australian Digital Health Agency

My Health Record

My Health Record security and access policy

[Insert organisation name]	[Insert version number}	[Insert date version was enacted]

Governance	
Responsible Officer (RO)	[Insert name]
Organisation Maintenance Officer/s (OMO)	1. [Insert name]
	2. [Insert name]
	3. [Insert name]
	4. [Insert name]

Access	
Authorised staff will access the My Health Record system via:	[Insert provider portal and/or conformant software]
An up-to-date list of individual healthcare providers authorised to access the **Provider Portal** will be provided to the **System Operator** (SO) by:	[Insert RO/OMO]
Authorised staff will be provided with a **unique user account** to access the My Health Record system via conformant software by:	[Insert RO/OMO]
The **level of access** granted to individual staff will be determined and documented by:	[Insert RO/OMO]
Access flags will be assigned by:	[Insert RO/OMO or not applicable if not required]
Access records will be maintained by:	[Insert RO/OMO or clinical software]

Security	
User account information and access will be managed by:	[Insert RO/OMO]
Account passwords will be changed by users every:	[Insert frequency]
Staff will report any suspected **security breach** to:	[Insert RO/OMO]
Confirmed security breaches will be reported to the **relevant authority** by:	[Insert RO/OMO]
A log of security breaches including date and time of the breach, user account involved, patient information accessed (if known), and **mitigation strategies** employed will be maintained by:	[Insert RO/OMO]
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:	[Insert frequency]

Training	
My Health Record system training will be organised for all authorised staff before they first access the system by:	[Insert RO/OMO]
A register of staff training including the names of those who have completed training and the date training was completed will be maintain by:	[Insert RO/OMO]
Training will be reviewed to ensure currency and updated as required (i.e. if **new functionality** is introduced into the system) every:	[Insert frequency]

Clinical incidents	
Clinical incidents will be reported to the **relevant party** by:	[Insert RO/OMO]
A log of reported clinical incidents will be maintained by:	[Insert RO/OMO]
Clinical incident management is the responsibility of:	[Insert RO/OMO]

Patient complaints	
Patient complaints regarding My Health Record will be redirected to the My Health Record Helpline (1800 723 471) or will be referred to:	[Insert RO/OMO]

Explanatory notes

Governance

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

Organisation Maintenance Officer (OMO): undertakes the day-to-day administrative tasks in relation to the HI-service and the My Health Record system. An OMO needs to be 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 (HPO). It 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 (HPI-I) numbers, and the level of access granted, in the clinical software and in the organisation's internal records.

Provider Portal: the portal provided by the System Operator that allows 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 My Health Record system via 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: the Australian Digital Health Agency. To contact the Agency regarding issues with the My Health Record system, phone the My Health Record 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 assistant whom may be granted a view access to 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 healthcare organisation, the RO/OMO will define an appropriate network hierarchy for the organisation and assign access flags appropriately for the structure of the organisation. The network hierarchy will define the seed organisation, the network organisations that fall under 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:

- patients 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 patients 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 patient query reveals potential structural issues. The organisation commits to making reasonable changes in line with requests from the System Operator.

Access records: records that identify which user accessed the system via conformant software on a particular day. The OMO will determine whether the pharmacy 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: instances of unauthorised collection, use or disclosure of health information included in a patient's My Health Record, e.g. 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 My Health Record system using the clinical information system, and associated mitigation strategies if required
- potential for misuse or unauthorised disclosure of information from a patient's My Health Record by persons authorised to access the My Health Record system, and associated mitigation strategies if required
- potential for accidental disclosure of information contained in a patient's My Health Record 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, Pharmaceutical Society of Australia, Pharmacy Guild of Australia or Society of Hospital Pharmacists of Australia (i.e. My Health Record training modules or My Health Record continuing professional development 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 will be updated to reflect new functionalities as they become available and published for public use. Additional training for staff with authorised access may need to be provided using the updated training material.

Clinical incidents

Clinical incident: an event or circumstance that resulted, or could have resulted, in unintended and/or unnecessary harm to a patient 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 My Health Record Helpline (1800 723 471). The System Operator will triage the clinical incident and refer as necessary.

Clinical incident management

Issue	Action
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 redispense. 2. Upload the new, correct 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 patient 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 patient 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). 4. Record your actions in your own notes.
Upload of document (i.e. dispense record) to a patient's My Health 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 the 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, 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/deactivate the user account. 2. Change the password information for the account. 3. Report the breach to the police, and if relevant (see 'relevant authority'): • System Operator (1800 723 471) • Office of Australian Information Commission (1300 363 992)

Patient complaints

Patient complaints: patients 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 patient and the complaint will be referred to the management of that service and/or the Office of the Information Commissioner.
- Where a patient 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 patient will be directed to exercise their personal controls over the document.

Policy Manager: [Insert Organisation Maintenance Officer's name]

Contact Tel: [Insert phone number] Email: [Insert email address]

Approval Authority: [Insert Responsible Officer's name] Latest Review Date: [DD/MM/YY]