



Cybersecurity in General Practice & My Health Record Compliance

Thursday, May 16th 2024

Acknowledgement of Country

I would like to acknowledge the traditional owners of the land on which we all meet today and to pay my respects to Aboriginal elders past, present and emerging.

I would also like to extend my respect to all Aboriginal people present today.



Housekeeping

- Attendees muted for duration of webinar
- 1 hour duration
- Webinar being recorded and will be available on our website
- Q & A

Guest Speakers & Panellists



Miroslav Doncevic

Cybersecurity Architect – Mint IT



Tony Nicholson

Director – Mint IT



My Health Record Compliance

Presented by Nisha Sathyan

Digital Health Program Officer – NBMPHN

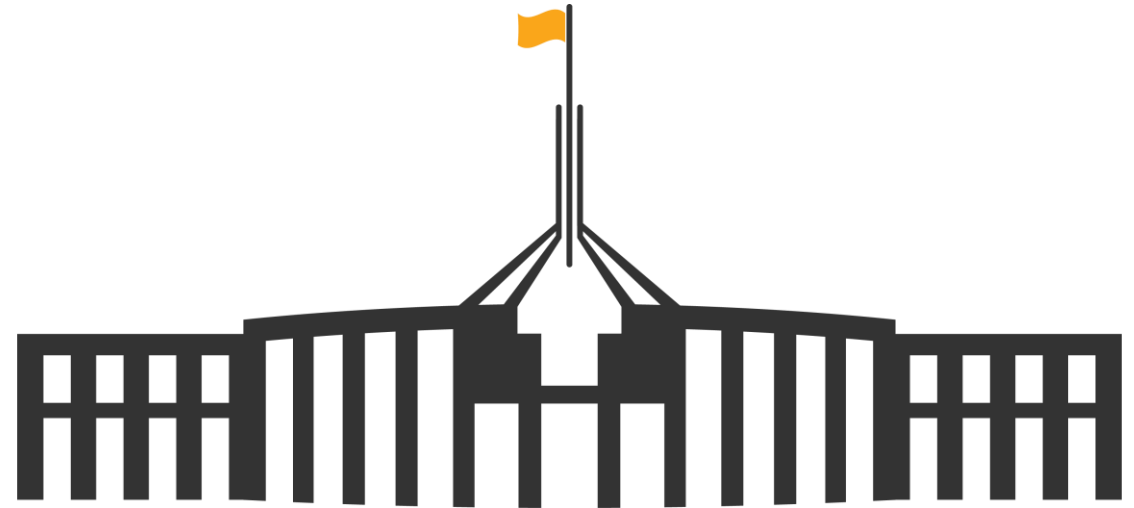
Legislation

The My Health Record system is supported by a legislative framework that sets controls around who can access the system and the information contained within.

Relevant acts and instruments include:

[My Health Records Act 2012](#)

[My Health Records Rule 2016](#)



The Australian Digital Health Agency website has information about the My Health Records Act and more. [My Health Record legislation and governance](#).



Rules 42, 43, 44



Rule 42

Includes the matters in which need to be addressed in your My Health Record security and access policy.



Rule 43

- A copy of your organisation's policy may be requested by the system operator.
- Must provide a copy of the My Health Record security and access policy within 7 days.



Rule 44

- Covers user account management.
- Ensure that IT systems employ reasonable use account management practices

These are in place to safeguard the use of My Health Record and to give both patients and clinicians confidence that the system is secure.



Ongoing My Health Record participation obligations

Regular review of My Health Record Security & Access Policy

User account management in your clinical software

Respond to requests made by The Agency/System Operator

Comply with notifiable data breach requirements

Provide My Health Record training to staff

Ongoing My Health Record participation obligations

Regular review of My Health Record Security & Access Policy

User account management in your clinical software

Respond to requests made by The Agency/System Operator

Comply with notifiable data breach requirements

Provide My Health Record training to staff

Regular review of My Health Record Security & Access Policy



Australian Government
Office of the Australian Information Commissioner

My Health Record system security and access policy template

Background

This My Health Record system security and access policy template provides guidance for healthcare provider organisations on meeting the requirements set out in Rule 42 of the *My Health Records Rule 2016*.

Under Rule 42, healthcare provider organisations must establish a security and access policy prior to registering with the My Health Record system. The policy must be communicated to all employees and any healthcare providers to whom the organisation supplies services under contract. The policy must be enforced in relation to all employees and healthcare providers to whom the organisation supplies services under contract. Healthcare provider organisations must also ensure that the policy is kept up to date by reviewing it, at least annually, as well as when any material new or changed risks are identified.

The policy must cover the following matters:

- the manner of authorising people to access the My Health Record system, and deactivating or suspending [access](#)
- training that will be provided to employees before they access the My Health Record [system](#)
- the process for identifying a person who requests access to a healthcare recipient's My Health Record and communicating the person's identity to the System Operator³
- physical and information security measures that will be established and adhered to by the healthcare provider organisation and people accessing the My Health Record [system](#)
- mechanisms for the prompt identification and mitigation of My Health Record system-related security risks

- Policy template can be downloaded from [Office of the Australian Information Commissioner \(OAIC\)'s website](#)
- Policy covers areas such as how your practice:
 - ▶ Accesses My Health Record
 - ▶ authorises and deactivates users accessing My Health Record.
 - ▶ Intends to train staff to use My Health Record (Practices are encouraged to keep a Training Register)

Training Register

ABC GENERAL PRACTICE								
MY HEALTH RECORD STAFF TRAINING REGISTER					SECURITY PRACTICE AND POLICIES CHECKLIST			
Staff Name	Role	User Training Checklist & Declaration ?	Date Trained & Date Due	RO/OMO Initials	Date Trained & Date Due	RO/OMO Initials	Date Trained & Date Due	RO/OMO Initials
Dr James Bond	General Practitioner	Completed	01/01/20 Due: 01/07/20	LL	29/06/20 Due: 01/12/20	LL		
Louis Lane	Practice Manager	Completed	09/01/2020 Due: 09/07/20	LL	09/07/2020 Due: 09/01/21	LL		
Clark Kent	Receptionist	Completed	21/03/20 Due: 21/09/20	LL	N/A – Left Practice			
MY HEALTH RECORD DEACTIVATED USERS								
Former Staff Name	Last day of Employment	User Account Deactivated or Deleted?	Date of Deactivation	Name & Role	Signed			
Clark Kent	12/08/2020	Yes	12/08/2020	Louis Lane /OMO	LL			



Regular review of My Health Record Security & Access Policy



Australian Government
Office of the Australian Information Commissioner

My Health Record system security and access policy template

Background

This My Health Record system security and access policy template provides guidance for healthcare provider organisations on meeting the requirements set out in Rule 42 of the [My Health Records Rule 2016](#).

Under Rule 42, healthcare provider organisations must establish a security and access policy prior to registering with the My Health Record system. The policy must be communicated to all employees and any healthcare providers to whom the organisation supplies services under contract. The policy must be enforced in relation to all employees and healthcare providers to whom the organisation supplies services under contract. Healthcare provider organisations must also ensure that the policy is kept up to date by reviewing it, at least annually, as well as when any material new or changed risks are identified.

The policy must cover the following matters:

- the manner of authorising people to access the My Health Record system, and deactivating or suspending [access](#)
- training that will be provided to employees before they access the My Health Record [system](#)
- the process for identifying a person who requests access to a healthcare recipient's My Health Record and communicating the person's identity to the System Operator³
- physical and information security measures that will be established and adhered to by the healthcare provider organisation and people accessing the My Health Record [system](#)
- mechanisms for the prompt identification and mitigation of My Health Record system-related security risks

- Legislation states you should Review your policy:
 - at least once per year
- Or when situations your organisation is required to review and update the policy:
 - ▶ A change within the system, organisation or regulation
 - ▶ When a data breach has occurred and risks have been identified.

Ongoing My Health Record participation obligations

Regular review of My Health Record Security & Access Policy

User account management in your clinical software

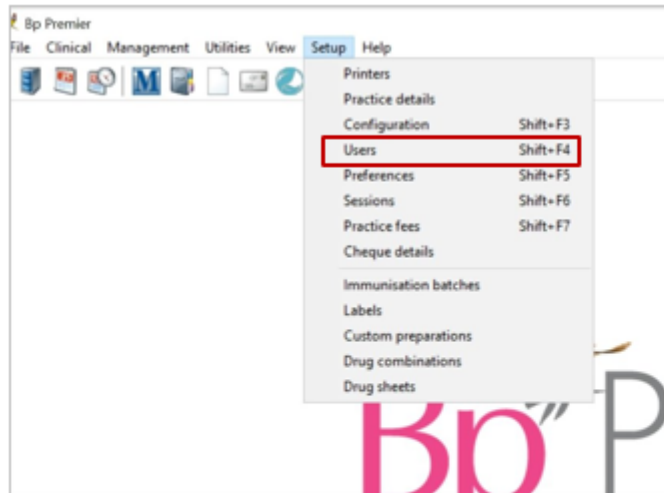
Respond to requests made by The Agency/System Operator

Comply with notifiable data breach requirements

Provide My Health Record training to staff

User account management in your clinical software

e.g. Best Practice



A screenshot of the 'Edit user details' form for a user named Dr. Terence Walker. The form contains various fields for personal and professional information, including title, name, contact details, and professional registration. A 'Set Permissions' button is highlighted with a red rectangle at the bottom left.

Title:	Dr	Usual location:	Main surgery
First name:	Terence	Provider No.:	24266218
Surname:	Walker	Prescriber No.:	2173711
Category:	Principal doctor	Registration No.:	
Home phone:	(07) 3333-3333	Health Identifier:	8003618233334167
Mobile phone:	0444-444-444	CPD No.:	
Pager:		<input checked="" type="radio"/> Full time	<input type="radio"/> Part time <input type="radio"/> Locum
E-mail:	doctor@gp.com	<input type="checkbox"/> Vocationally registered	<input type="checkbox"/> DVA LMD
Qualifications:	GP	<input type="checkbox"/> Has appointments	<input type="checkbox"/> Has accounts
		<input type="checkbox"/> Requires a referral for Medicare billing	Business name: <input type="text"/>
<input type="checkbox"/> Inactive		Default account type:	Direct Bill
<input type="checkbox"/> Force password change on next login		Default item No.:	<input type="text"/>
<input type="checkbox"/> Make notes confidential		<input type="checkbox"/> Make notes confidential	

A screenshot of the 'Permissions' dialog box for Dr. Terence Walker. It shows a list of sections and their corresponding permissions. The 'My Health Record Access' row is highlighted with a red rectangle and has a blue checkmark in the permission column.

Section	Permission
Family/Social history	Add/Edit/Delete
Setup Drug sheets	Allow access
Practice Email	Allow access
Daily message	Allow access
Contacts	Add/Edit/Delete
Messages	Allowed
Export demographic data	Allow access
Export clinical data	Allow access
Import clinical data	Deny access
Subpoena Tool	Deny access
My Health Record Access	Allowed
My Health Record Registration	Allowed
Search clinical data	Allow access
Change patient confidential status	Allowed
Allocate investigation reports	Allow access
Reminder lists	Allow access
Word processor templates	Add/Edit/Delete
Word Processor	Allow clinical access
Configuration	Allow access
Passwords	Allow access
Perform a backup	Allow access

- Ensure that any authorised staff have been given access in your software through the user preferences section.

User account management in your clinical software

e.g. MedicalDirector – user preferences for a non-GP user

The screenshot shows the 'Add User' dialog box with the following details:

- User's Name:** [Empty text box]
- Location:** MedicalDirector Samples Database
- Category:** [Empty dropdown]
- Supervising Doctor:** [Empty dropdown]
- Access Level:**
 - Full - access to patient files, addition and editing of all information except medications. (highlighted)
 - Limited - access to patient files. Letters containing patient information can be created. No other additions/alterations can be made.
 - Basic - access to demographic files. No access to clinical information is allowed.
- Australian Immunisation Register (AIR):**
 - Ancillary Provider Number: [Empty text box]
- Healthcare Identifier:**
 - HPH No: [Empty text box]
- MyHealthRecord Details:**
 - Participate in MyHealthRecord (highlighted)
 - When the 'Participate in MyHealthRecord' option is checked:
 - You can download or upload clinical documents to each patient's MyHealthRecord. This is subject to each patient's MyHealthRecord security status.
 - Title: [Empty text box]
 - First Name: [Empty text box]
 - Middle Name: [Empty text box]
 - Last Name: [Empty text box]
- Additional Options:**
 - Data Export Privileges?
 - Options Editing?
 - PKI Encryption
 - Auto-capitalise name
 - MyHealthRecord Assisted Registration
- Buttons:** OK, Cancel

- Ensure that any authorised staff have been given access in your software through the user preferences section.

User account management in your clinical software

- Be aware of how to suspend access to My Health Record
- Have a unique user account for each individual
- Regularly reviewing password
- Having other access mechanisms e.g. locking screen



Ongoing My Health Record participation obligations

Regular review of My Health Record Security & Access Policy

User account management in your clinical software

Respond to requests made by The Agency/System Operator

Comply with notifiable data breach requirements

Provide My Health Record training to staff

Respond to requests made by The System Operator/The Agency

Your practice will need to be able to:

Assist with any inquiry, audit, review, assessment, investigation, or complaint regarding My Health Record



e.g. Letters are sent out to organisations that have used Emergency Access/Break Glass function and the organisation is to investigate to see if the it was authorised use or not.



e.g. Be requested to provide a copy of your organisation's policy within 7 days if requested.

Ongoing My Health Record participation obligations

Regular review of My Health Record Security & Access Policy

User account management in your clinical software

Respond to requests made by The Agency/System Operator

Comply with notifiable data breach requirements

Provide My Health Record training to staff

Comply with notifiable data breach requirements

- What is a notifiable My Health Record data breach?
 - ▶ There has been unauthorised collection, use or disclosure of health information included in a patient's My Health Record
 - ▶ An event or circumstance has occurred that compromised the security or integrity of the My Health Record system.
- Report data breaches as soon as practicable to the OAIC and The Agency.
- More guidance can be found on The Agency's website -
<https://www.digitalhealth.gov.au/healthcare-providers/initiatives-and-programs/my-health-record/data-breaches>



Ongoing My Health Record participation obligations

Regular review of My Health Record Security & Access Policy

User account management in your clinical software

Respond to requests made by The Agency/System Operator

Comply with notifiable data breach requirements

Provide My Health Record training to staff

Provide My Health Record training to staff



The screenshot shows the header of a webpage with the Australian Government logo and the Australian Digital Health Agency name. It also features the My Health Record logo and a blue banner that reads 'Recommended My Health Record Training'. The main content area is titled 'Recommended My Health Record Training' and contains the following text:

Healthcare provider organisations must provide staff with My Health Record training *before* they are authorised to use the system. The training is required to cover:

- How to use the system accurately and responsibly
- Legal obligations of the healthcare provider organisation and people who access the system on behalf of the organisation
- Consequences of breaching those obligations

Details of training provided to staff should be set out in the organisation's [My Health Record security and access policy](#). Healthcare organisations may be required to provide evidence of how they comply with these obligations, and it is recommended that a training register is maintained. It is recommended that training is provided to staff on a regular and ongoing basis.

Available Training
Staff can access a range of free online eLearning modules about My Health Record [here](#). At a minimum, staff should complete the My Health Record security, privacy and access [eLearning module](#).

Staff may be directed to attend a training session or webinar hosted by the Australian Digital Health Agency. A list of available events can be found [here](#).

A range of [podcasts](#) are available to support staff training.

Other training options
Organisations are also able to conduct internal training covering the below topics (1-7).

- 1. [What is in a record](#)
- 2. [Understand when you can view and upload information](#)
- 3. [Appropriate and lawful use of the Emergency Access \('break glass'\) function](#)
- 4. [Participation obligations](#)
- 5. [Penalties for misuse](#)
- 6. [Data breaches and how to manage them](#)


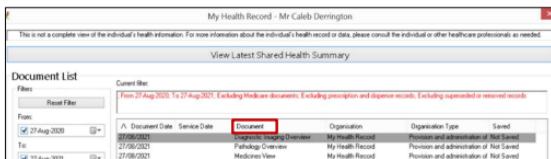
- Training needs to be provided:
 - ▶ Before staff are authorised to access the system for the first time
 - ▶ As a yearly refresher for those who have already completed the training
- Train users of the system regarding:
 - ▶ Accurate and responsible use
 - ▶ Legal obligations of accessing the system

Provide My Health Record training to staff

Best Practice Fact Sheet

Viewing Clinical Documents in My Health Record

Note: These steps assume that your software is connected to the My Health Record system, the patient has a My Health Record and their individual healthcare identifier (IHI) has been validated in your system

<p>STEP 1:</p> <p>To gain access to the patient's My Health Record, either:</p> <ul style="list-style-type: none">• Select My Health Record tab, then View Document List from the drop-down menu; or• Click on the My Health Record button.	
<p>STEP 2:</p> <p>The document list window will appear, displaying documents in the patient's My Health Record (subject to any search filters which are set).</p>	

Example of a Best Practice Software Summary Sheet

Training & Education Resources:

- [eLearning Modules](#)
- [On-Demand Webinars](#)
- [Software Summary Sheets](#)
- [Training Simulator](#)
- Your Engagement Officer and Digital Health Officer can provide training for new and existing users

Thank you

Nisha Sathyan

Digital Health Program Officer

T: 02 4708 8136

E: nisha.sathyan@nbmphn.com.au

