Train IT Medical
Competence with Confidence

Managing compliance for digital health

- Including My Health Record and ePIP-

:
Sue Cummins & Katrina Otto, Train IT Medical Pty Ltd
enquiries@trainitmedical.com.au www.trainitmedical.com.au

Learning Objectives

1. Describe how to use the My Health Record system accurately and responsibly in accordance with the My Health Records Act
2. Understand the legal obligations for organisations and individuals using the system, and the consequences of breaching these obligations
3. Develop policies and procedures for using My Health Record and ePIP that comply with legislative requirements
4. Understand the My Health Record changes introduced in 2026 and what they mean for your practice

Learning Objective 1

Describe how to use the My Health Record system accurately and responsibly in accordance with the My Health Records Act

My Health Record legislative framework

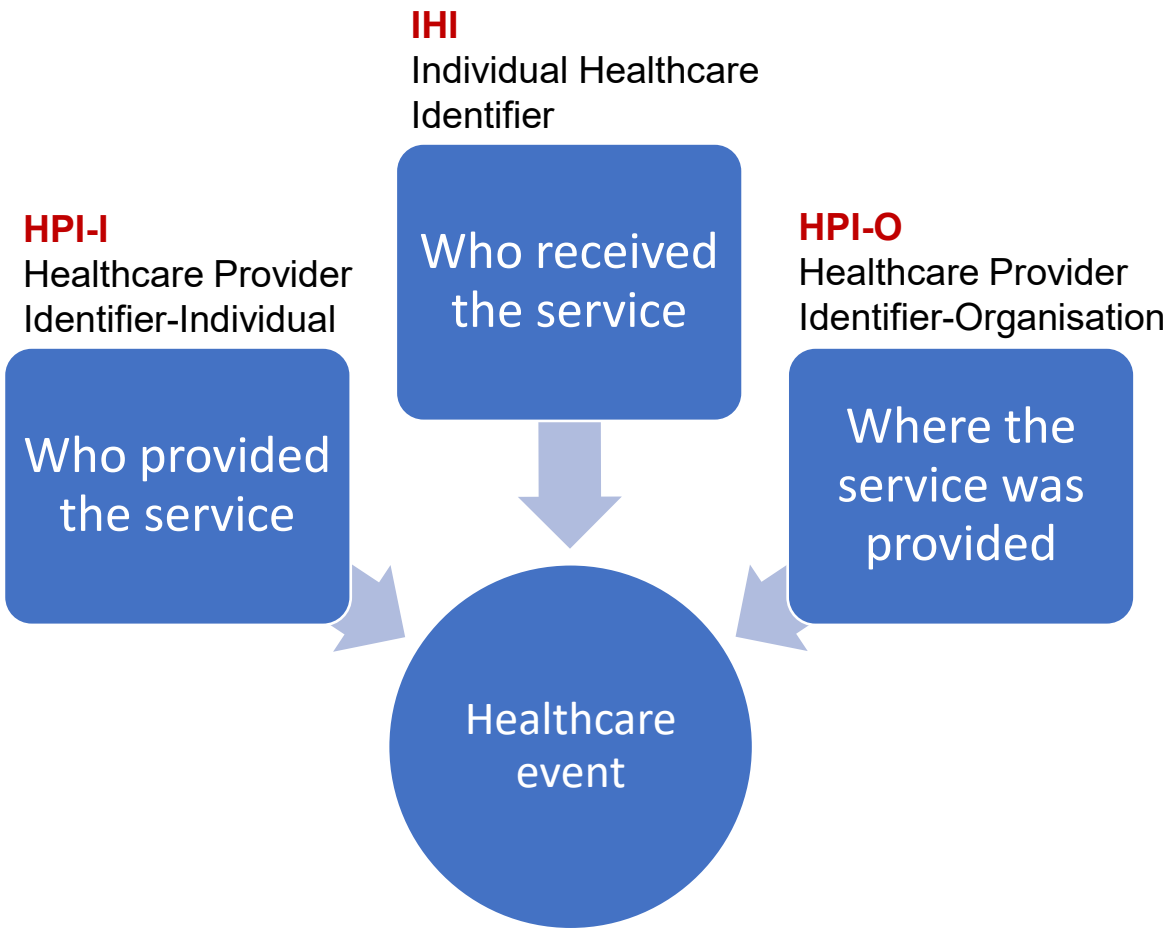
The My Health Record system operates under the *My Health Records Act 2012* and *The Privacy Act 1988*.

The Acts establish:

- The role and functions of the system
- A registration framework
- A privacy framework

OAIC: Australian privacy principles

Healthcare Identifiers Service



My Health Record

Roles and responsibilities

OMO Organisational Maintenance Officer
RO Responsible Officer

Authorising Users, Access and Security

- Ensure users are **AHPRA registered** / have an HPI-I
- **Record HPI-O and HPI-I in practice software**
- Communicating user identity to the System Operator
- Physical security
- Mitigation Strategies: risk assessments, audit reports

My Health Record

Roles and Responsibilities Matrix

Role	Employee from general practice	IHI search and download	My Health Record Assisted Registration	View My Health Record and download clinical documents	Author clinical documents for a My Health Record	Upload clinical document to My Health Record	Manage organisation interactions with HI Service and My Health Record
Responsible Officer (RO)	Business Owner						✓
Organisation Maintenance Officer (OMO)	Practice Manager						✓
Authorised Employee (HI Service only)	Receptionist	✓					
Authorised Employee (My Health Record system)	Social Worker / Aboriginal and Torres Strait Islander health worker	✓	✓	✓		✓	
Provider (HPI-I)	GP / Registered Nurse	✓	✓	✓	✓	✓	

*If using the **National Provider Portal,** add and maintain users in HPOS*

Maintain quality data

Uploading accurate information

- Healthcare providers are under an obligation to take reasonable steps to upload accurate and up-to-date information (this is an obligation that exists already when sharing patient information with other providers)

Use clinical coding

- Select from existing drop-down lists when adding to Past History
- Only chronic and significant medical conditions in Past History
- Avoid duplication of conditions
- Clean up Health Summary Information (Allergies, Current medications, Immunisations, Past History)

Data quality checklist

[ADHA Data Quality Checklist]

Learning Objective 2

Understand the legal obligations for organisations and individuals using the system, and the consequences of breaching these obligations

Standing consent

Providers who have a legitimate reason to access the My Health Record (e.g. to provide care to a patient) are authorised to do so subject to patient controls.

Authority to access and upload

A provider is authorised by law to access and upload clinical documents without gaining consent of the patient each time in order to provide healthcare to the patient.

AMA Guide

Individuals control who has access to their record

They can choose to restrict access to specific documents in their My Health Record by establishing a code (LDAC).

Any Organisation given the LDAC can access those documents

They can restrict access to their record by establishing a code (RAC) that will mean only organisations given the code can access any part of their My Health Record

They can subscribe to SMS or email alerts that report in real time when a new health provider organisations accesses their My Health Record

All instances of access to My Health Record are monitored and logged

Consumer view & access controls

The National Consumer portal gives the consumer a view of clinical documents in My Health Record and allows them to control access

How to set access controls

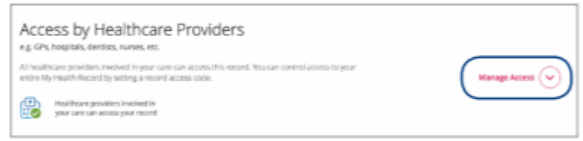
Use myGov to look at your My Health Record. If you don't have a myGov account, go online to my.gov.au to set one up. Once you have logged in to myGov, select 'Services', then select the 'Link' button to set up your My Health Record. You will need to identify yourself by answering a series of questions about your last visit to a healthcare provider.

How to set a Record Access Code (RAC)

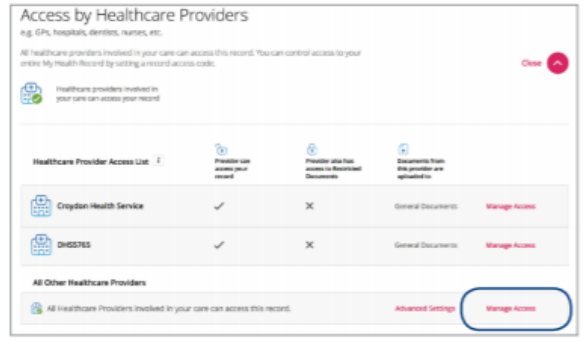
Log in to your My Health Record via myGov

1. Select 'Privacy & Access'

2. In the 'Document Access Settings' section select 'Manage Access'



3. A drop-down list appears. Select 'Manage Access' from the list



Ongoing participation obligations

- Must **not discriminate** against an individual
- Uploaded information is **accurate, up-to-date, not misleading and not defamatory**;
- Not upload information where an individual has **withdrawn consent**
- Only upload a clinical document prepared by a **registered healthcare provider (HPI-I)**
- Advise System Operator if you **cease to be eligible** to be registered
- **Give assistance** in relation to any inquiry, audit, investigation or complaint

Security practices and policies checklist

- ❑ My Health Record System Security Policy
- ❑ Managing User Accounts
- ❑ Identification of Staff
- ❑ Staff Training
- ❑ Handling of Privacy Breaches and Complaints
- ❑ Risk Assessments

Checklist

The checklist is based on the requirements of the *My Health Records Rule 2016*.

Training Staff

- **Prior to** accessing My Health Record & for ongoing updates
- Accurate and responsible use
- **Legal obligations and consequences of breaching**
- Staff **not eligible to access My Health Record** understand their obligations in relation to privacy and security of patient information
- **Maintain register of staff trained** to access and use the system

Australian Government
Australian Digital Health Agency

My Health Record

Recommended Training Checklist

Recommended Training Checklist and Declaration

Before using the My Health Record system, you are obliged to undertake training in relation to using the My Health Record system and the consequences of breaching those obligations. It is recommended that My Health Record training includes the below topics (1-8).

Recommended Training Checklist

- ☐ 1. View a My Health Record
- ☐ 2. Upload clinical information
- ☐ 3. Understand when you can view and upload information
- ☐ 4. Appropriate and lawful use of the Emergency Access ('break glass') function
- ☐ 5. Participation obligations
- ☐ 6. Penalties for misuse
- ☐ 7. Data breaches, and how to manage them
- ☐ 8. Clinical incidents, and how to report them

Available from your Responsible Officer

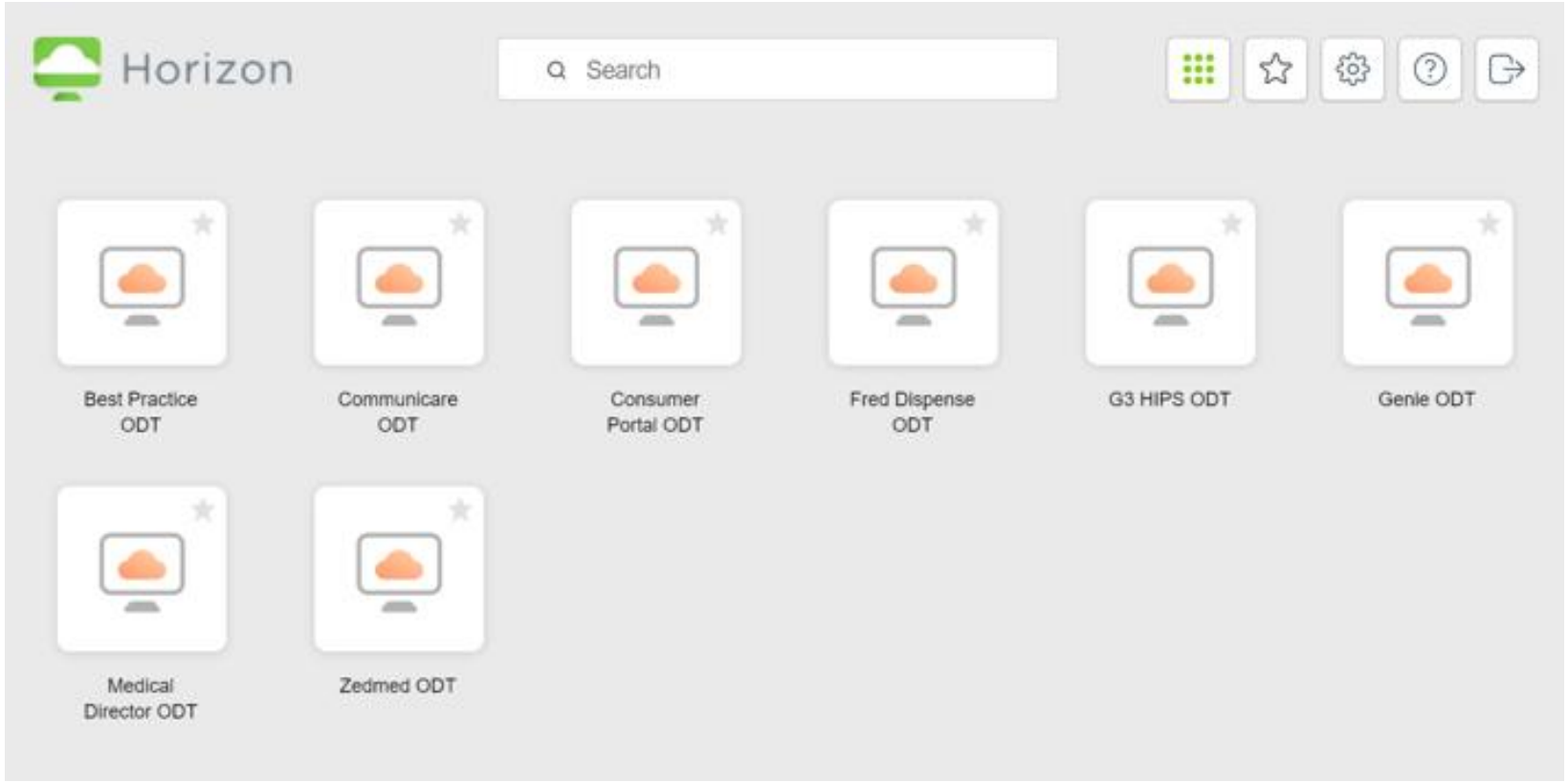
Declaration

- ☐ I have understood the information within the above web pages (1-8)
- ☐ I have understood my organisation's My Health Record Security & Access Policy

First Name: _____ Designation: _____ Signature: _____
Surname: _____ Date: _____

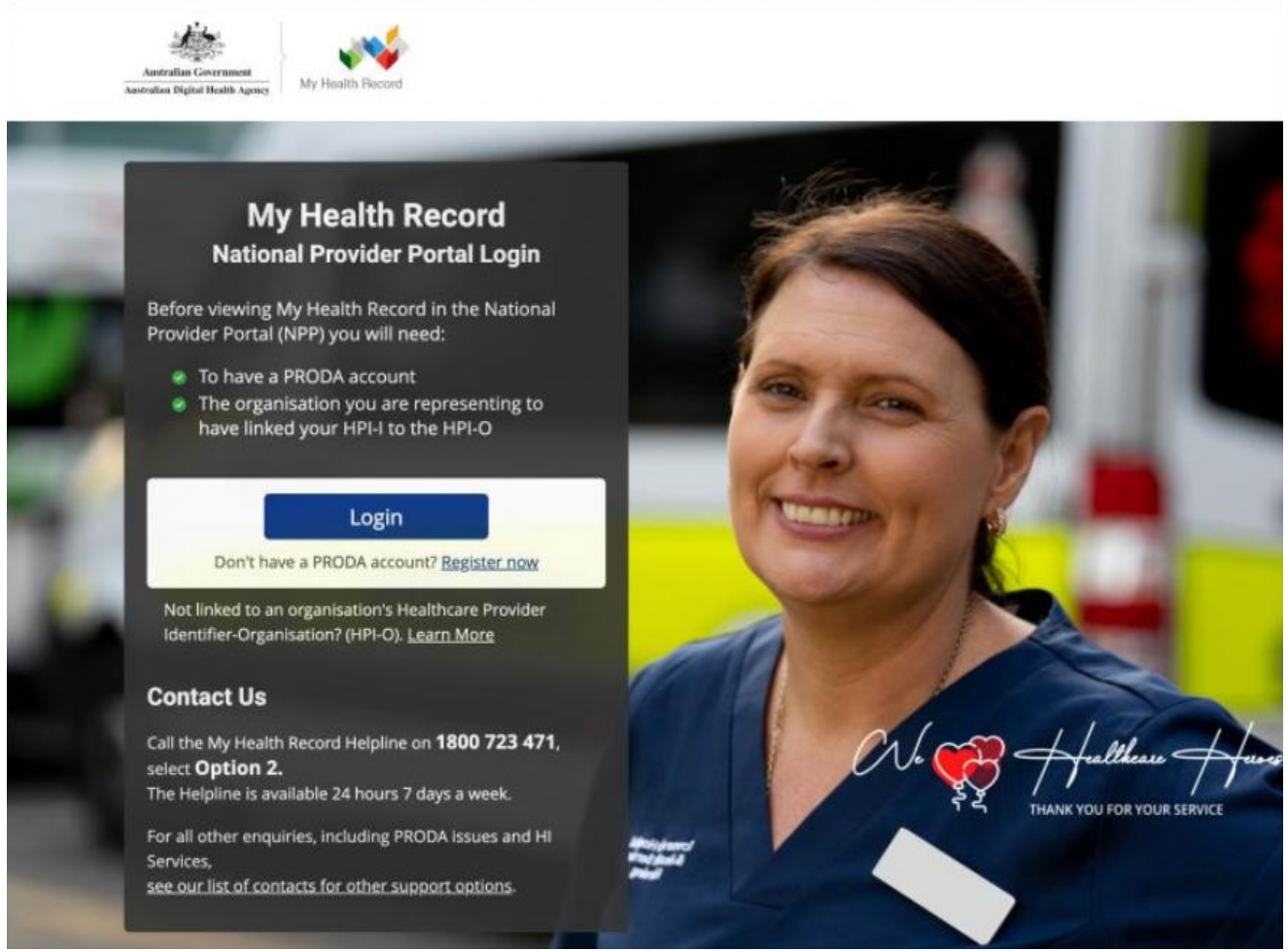
ADHA: Recommended training checklist

On Demand Training



On Demand training

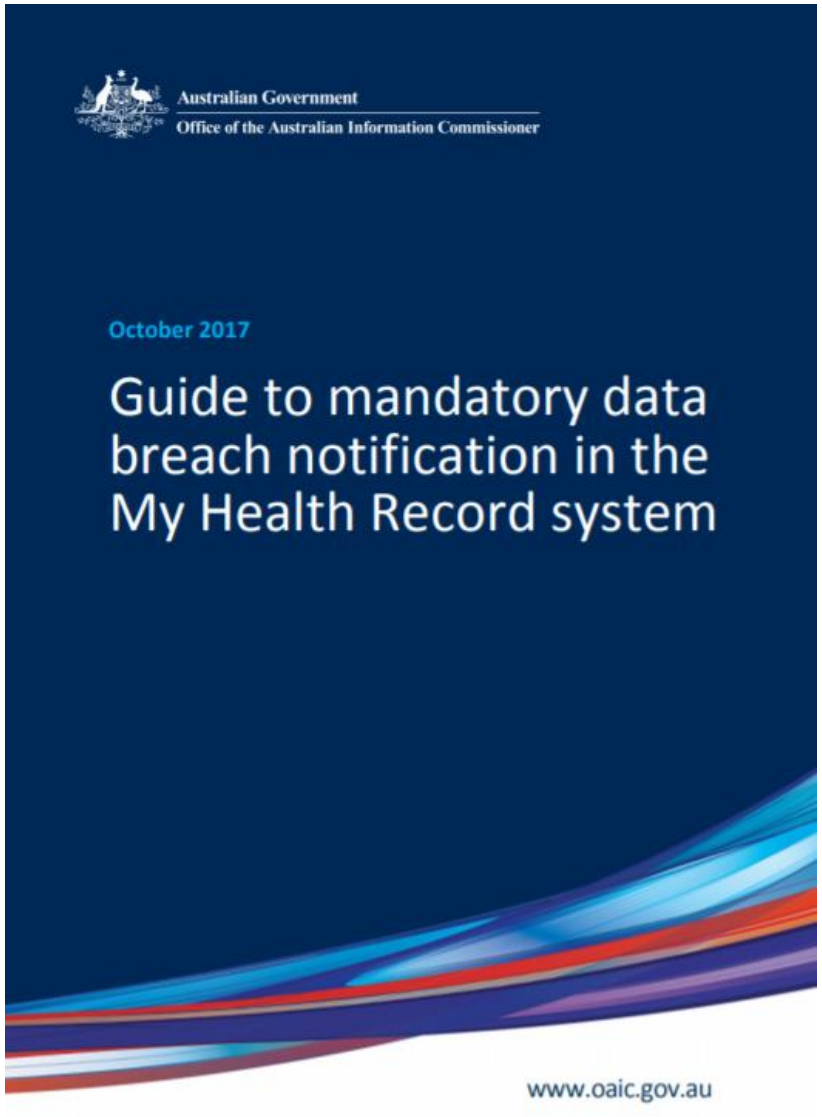
National provider portal



In the case of a data breach

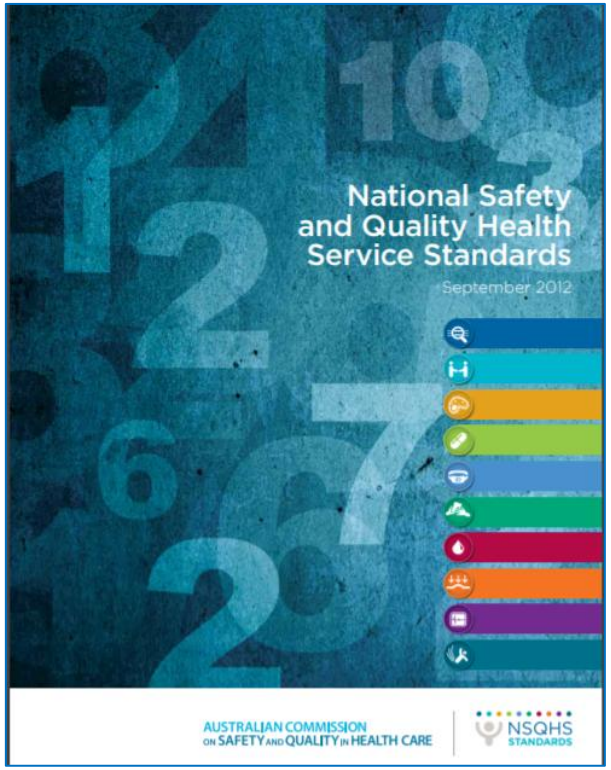
Examples:

- Infection by malicious software
- Unauthorised user access to a patient record
- Hacking attack has compromised IT system
- Intercepting pager messages between healthcare providers



Source

Reporting Clinical Incidents



A **clinical incident** is defined as "an event or circumstance that resulted, or could have resulted, in unintended and/or unnecessary harm to a person and/or a complaint, loss or damage".

24/7 My Health Record helpline 1800 723 471

Source: ACSQHSC

Strengthened privacy regulations

In November 2018, My Health Record privacy laws were strengthened:

1. Access by insurers and employers
2. Access by law enforcement and government agencies
3. Permanent deletion of a cancelled My Health Record
4. Greater privacy for teenagers aged 14 and over
5. Increased penalties for misuse of information
6. Strengthening protections for victims of domestic and family violence
7. Operation of the My Health Record system
8. Use of My Health Record data for research purposes
9. No commercial use of My Health Record data

Privacy protections

Penalties for misuse

Access to My Health Record is limited to provisions in the law

- A record can only be accessed by healthcare providers providing healthcare to a patient
- There are strict penalties for misuse, including civil and criminal penalties such as imprisonment (up to 5 years) and fines of up to $315,000
- Access history is recorded, including who accessed the record and what actions were taken
- Court order is required to release health information to law enforcement or government agencies
- Patients can be notified when their My Health Record is accessed

Learning Objective 3

Develop policies and procedures for using My Health Record that comply with legislative requirements

Putting policies in place

Policies for organisations using My Health Record:

- NASH certificate policy
- My Health Record security and access policy

Policies for General Practice eligibility for PIP eHealth Incentive:

- Data records and clinical coding policy
- Secure Message Delivery policy
- ePrescribing policy

Organisations should develop, maintain, enforce and communicate written policies to all staff to ensure use of My Health Record is secure, responsible and accountable.

My Health Record security and access policy

"The My Health Record system Rule states that in order to participate in the My Health Record system, your organisation needs a written policy in place to address access and security issues relating to the use of the system."

Policy must include:

- Managing user accounts to access My Health Record
- How staff requesting access to My Health Record will be identified
- How staff training on use of My Health Record will be provided
- Physical and information security measures
- Mitigation strategies to ensure risks can be identified
- Assisted Registration protocols
- Document controls (versions, reviews, amendments etc)

Policy must be revised at least annually and be provided to the system operator on request

Australian Government
Australian Digital Health Agency

My Health Record

Overview of policies to participate

Overview of policies required to participate in digital health

This document provides an overview of the policies that are required for healthcare organisations to participate in digital health.

Directory Name	Objective of the policy	Sample Policy
My Health Record system Policy	To govern the use of the My Health Record system, the My Health Record system Rule state that in order to participate in the My Health Record system, your organisation needs a written policy in place to address the following: a) the manner of authorising persons accessing the My Health Record system via or on behalf of the healthcare provider organisation, including the manner of suspending and deactivating the user account of any authorised person: (i) who leaves the healthcare provider organisation; (ii) whose security has been compromised; or (iii) whose duties no longer require them to access the My Health Record system; b) the training that will be provided before a person is authorised to access the My Health Record system, including in relation to how to use the My Health Record system accurately and responsibly, the legal obligations on healthcare provider organisations and individuals using the My Health Record system and the consequences of breaching those obligations; c) the process for identifying a person who requests access to a consumer's My Health Record and communicating the person's identity to the System Operator where required; d) the physical and information security measures that are to be established and adhered to by the healthcare provider organisation and people accessing the My Health Record system via or on behalf of the healthcare provider organisation, including; i. restricting access to those persons who require access as part of their duties; ii. uniquely identifying individuals using the healthcare provider organisation's information technology systems, and having that unique identity protected by a password or equivalent protection mechanism; iii. having password and/or other access mechanisms that are sufficiently secure and robust given the security and privacy risks associated with unauthorised access to the My Health Record system; iv. ensuring that the user accounts of persons no longer authorised to access the My Health Record system via or on behalf of the healthcare provider organisation prevent access to the My Health Record system; and v. suspending a user account that enables access to the My Health Record system as soon as practicable after becoming aware that the account or its password or access mechanism has been compromised; and e) mitigation strategies to ensure My Health Record-related security risks can be promptly identified, acted upon and reported to the healthcare provider organisation's management. f) where the healthcare organisation provides assisted registration: (i) the manner of authorising employees of the organisation to provide assisted registration; (ii) the training that will be provided before a person is authorised to provide assisted registration; (iii) the manner of recording a consumer's consent and how that record will be handled for retention purposes; and (iv) the process and criteria for identifying a consumer for the purposes of assisted registration.	**Download a sample policy**

Source: myhealthrecord.gov.au

NASH certificate policy

What is NASH?

What does the NASH policy need to include?

- Who can use the certificate
- Identifies individuals / accountability for use
- Administration and maintenance tasks

The NASH PKI is a set of hardware, software, policies and procedures that let the recipient of an electronic communication know that:

- the sender of the communication was recorded as being registered with the HI Service at the time they were issued with a certificate, and information related to the sender's registration can be reliably represented to the recipient for verification (authentication)
- the communication content has not been changed in transit between the sender and the recipient (integrity), and
- only the intended recipient is able to open the communication (confidentiality) of the relying party (assurance).

eHealth PIP policies

Electronic Transfer of Prescriptions policy

To ensure the majority of prescriptions generated by our practice are sent electronically to a prescription exchange service (PES).

Background
Electronic medication management (eMM) enables all stages of the prescribing, dispensing and supply of medicines to be completed electronically. Electronic medication management has the potential to reduce errors and adverse medication outcomes. eTP is an essential part of electronic medication management.

Our practice supports a prescribing process where the prescription is generated electronically, encrypted and authenticated via an organisational digital electronic signature and transmitted securely for dispensing by a pharmacy.

Practice procedure
Our practice:

- ensures that all prescribers use, where appropriate, eTP as a component of their prescribing process and has selected conformant clinical software for the eTP
- provides practice-based education and skills training to all staff to ensure competency in the use of the eTP.

Software requirements
The eTP software used in our practice is: eRx

Staff responsibility
It is the responsibility of all healthcare prescribers to use, where appropriate, eTP as part of their prescribing process.

It is the responsibility of all administrative staff to support the use of eTP by undertaking any administration tasks involved in the maintenance or use of the eTP software. When any problems arise with the eTP software within our practice, the appropriate software vendor and/or the company that provide IT support for the practice, will be contacted to assist in resolving the problem in a timely manner.

Related resources

RACGP *Standards for general practices (5th edition)*
https://www.racgp.org.au/running-a-practice/practice-standards/standards-5th-edition/standards-for-general-practices-5th-ed

RACGP *Information security in general practice*
https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice

Data Records and Clinical Coding policy

Practices must ensure that where clinically relevant, they are working towards recording the majority of diagnoses for active patients electronically, using a medical vocabulary that can be mapped against a nationally recognised disease classification or terminology system. Practices must provide a written policy to this effect to all GPs within the practice.

Our practice ensures that important elements of our patients' health information is recorded in their health record consistently, regardless of the provider they see. The clinical terminologies used are based on agreement by our practice and/or the practice team.

Background and rationale
Using consistent clinical coding terminologies will support better utilisation of searchable chronic disease registers and avoid confusion that can result from 'free text' descriptions in the health record. Best practice is the use of medical vocabulary that can be mapped against a nationally recognised disease classification or terminology system.

Practice procedure
Our practice:

- discourages the use of free-text coding for the recording of all important diagnoses and current and past clinical history in patients' health records
- is working towards consistent recording by encouraging the use of agreed clinical coding terminologies by using, for example, a 'pick list' or 'drop down box' function in the clinical desktop system
- uses clinical coding terminologies, at a minimum, for all 'active patients' of the practice[1]
- provides practice-based education and skills-based training to all healthcare providers and staff to ensure compliance with the policy and competency in the use of the technology.

Software requirements
The clinical desktop system used in our practice is:

Medical Director

The medical vocabulary used in the clinical desktop system is:

DOCLE

[1] The definition of an 'active' patient is a patient who has attended the practice three (3) or more times in the past two (2) years.

Secure Messaging Delivery policy

To ensure that our practice utilises standards-compliant secure messaging systems that have the capability to both securely send and transmit clinical messages to and from other healthcare providers.

Background
Secure electronic messaging significantly lessens the chance of clinical information being accessed and read by a non-healthcare recipient. While electronic transmission carries an inherent risk of inadvertent wider broadcast of information, it also offers the opportunity to protect information more efficiently through higher security standards.

Practice procedure

Our practice:

- sends and receives correspondence and reports to and from our clinical desktop system to other healthcare providers through the use of conformant secure messaging software.
- supports all healthcare providers in our practice to actively use secure messaging software to send and receive patient documentation, where feasible
- adheres to the use of compliant software to ensure that message contents are encrypted for the entire transmission process using appropriate digital certificates
- has verified that the installed software for SMD has been configured in accordance with ok
- Commissioning Requirements
- does not support or condone the use of insecure electronic methods of transmission for communications containing identifiable clinical information
- encourages a sustained increase in the use of standards-compliant secure messaging systems
- can demonstrate that the product is interoperable with other standards-compliant products
- uses a National Authentication Service for Health (NASH) Public Key Infrastructure (PKI) organisation certificate
- provides practice-based education and skills-based training to all healthcare providers and staff to ensure compliance with the policy and competency in the use of the technology.

Software requirements
The secure messaging software used in the practice is: Healthlink and Argus

Staff responsibility
It is the responsibility of all healthcare providers in our practice to send electronic health information using secure messaging systems as outlined in this policy.

RACGP eHealth PIP policy templates

Learning Objective 4

Understand the My Health Record changes introduced in 2026 and what they mean for your practice

2026 changes to My Health Record

There have been several significant My Health Record changes in 2025- 2026. They fall into 2 distinct categories:

Better and faster access to results

- Oct 2025 – faster access for most pathology
- Early 2026 – faster access for diagnostic imaging
- 1 July 2026 - **Share by default**

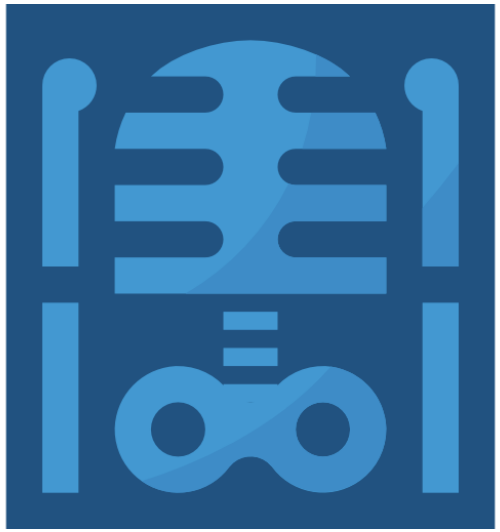
Stricter security access and record keeping obligations took effect April 1, 2026 replacing the 2016 rules.

The My Health Record Rules 2026 shift practices from passive compliance to active governance

Pathology and diagnostic imaging shared by default

Pathology and diagnostic imaging providers must now upload **written reports** to a patient's My Health Record by default, unless an exception or approved extension applies. This includes:

- Blood and urine pathology
- X-ray reports
- CT, PET scans and MRI reports
- Ultrasound reports
- Mammography reports

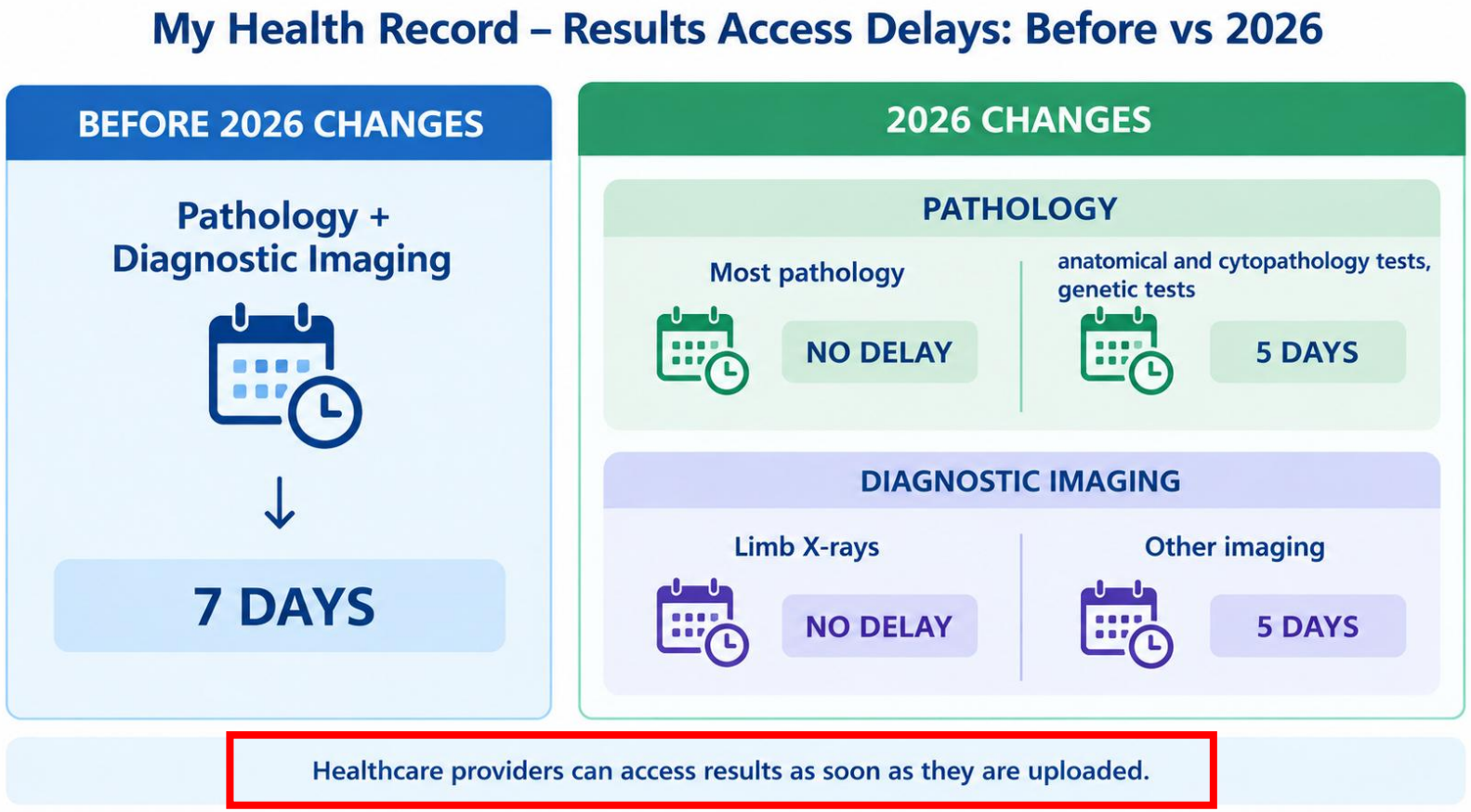


The actual diagnostic images are not uploaded under this requirement it is the report
There are exceptions to this rule e.g. patient request

Note there are exceptions to this rule such as on patient request not to upload a report

Pathology and diagnostic imaging – faster access

The delay in uploading reports to My Health Record for patients to see has been reduced from 7 to 5 days for some reports and **no delay** for many others:



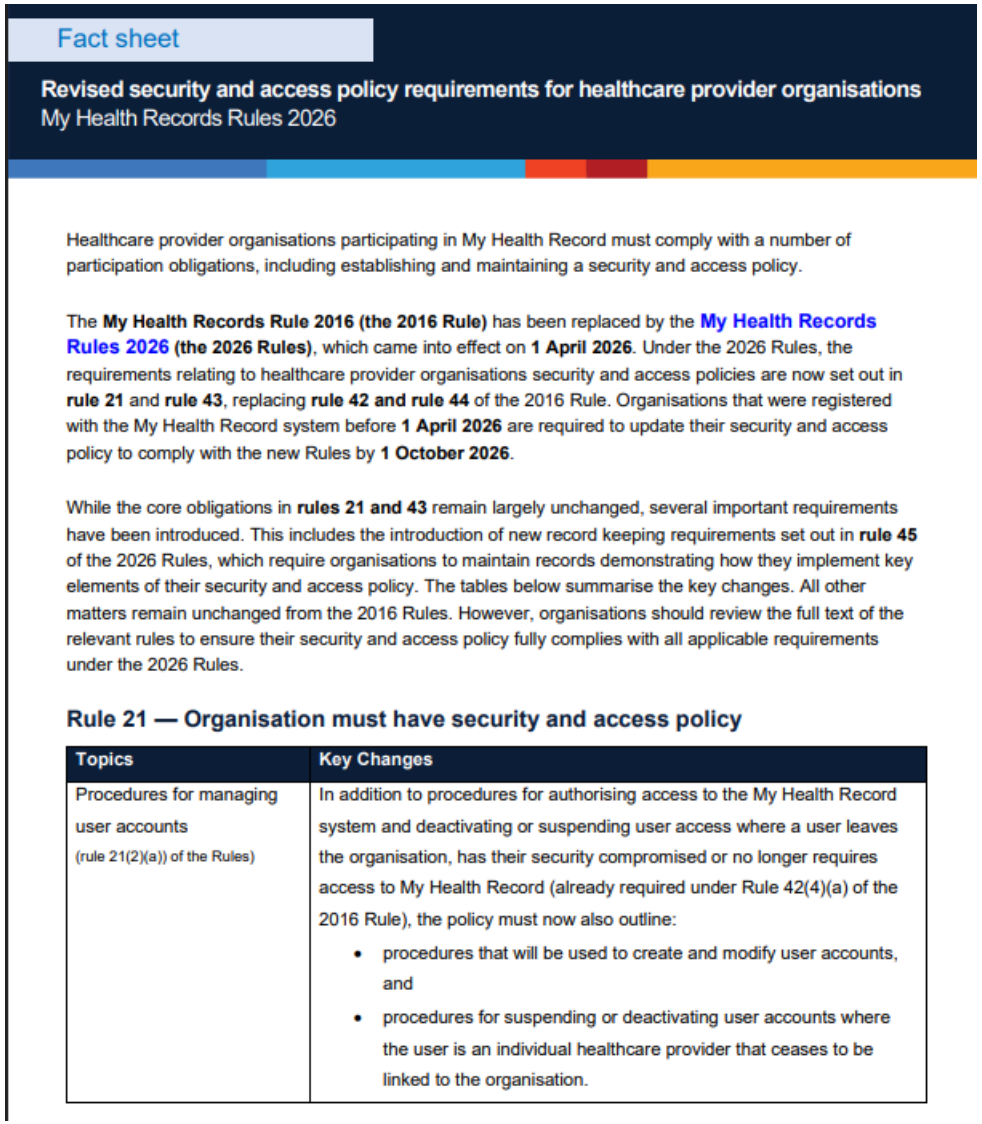
My Health Record rules 2026

These new rules replace the My Health Record relevant rules introduced in 2016.

For healthcare provider organisations, the changes strengthen and clarify obligations around:

- security
- access controls
- staff training and authorisation
- user-account management
- record keeping
- security and access policies.

There is a transition period for organisations that were already participating in My Health Record. **From 1 October 2026, all participants are expected to comply with the 2026 Rules.**



Fact sheet

Revised security and access policy requirements for healthcare provider organisations
My Health Records Rules 2026

Healthcare provider organisations participating in My Health Record must comply with a number of participation obligations, including establishing and maintaining a security and access policy.

The **My Health Records Rule 2016 (the 2016 Rule)** has been replaced by the **My Health Records Rules 2026 (the 2026 Rules)**, which came into effect on **1 April 2026**. Under the 2026 Rules, the requirements relating to healthcare provider organisations security and access policies are now set out in **rule 21** and **rule 43**, replacing **rule 42 and rule 44** of the 2016 Rule. Organisations that were registered with the My Health Record system before **1 April 2026** are required to update their security and access policy to comply with the new Rules by **1 October 2026**.

While the core obligations in **rules 21 and 43** remain largely unchanged, several important requirements have been introduced. This includes the introduction of new record keeping requirements set out in **rule 45** of the 2026 Rules, which require organisations to maintain records demonstrating how they implement key elements of their security and access policy. The tables below summarise the key changes. All other matters remain unchanged from the 2016 Rules. However, organisations should review the full text of the relevant rules to ensure their security and access policy fully complies with all applicable requirements under the 2026 Rules.

Rule 21 — Organisation must have security and access policy

Topics	Key Changes
Procedures for managing user accounts (rule 21(2)(a)) of the Rules)	In addition to procedures for authorising access to the My Health Record system and deactivating or suspending user access where a user leaves the organisation, has their security compromised or no longer requires access to My Health Record (already required under Rule 42(4)(a) of the 2016 Rule), the policy must now also outline: • procedures that will be used to create and modify user accounts, and • procedures for suspending or deactivating user accounts where the user is an individual healthcare provider that ceases to be linked to the organisation.

2026 My Health Record changes factsheet

Security and Access Policy – key changes

Policy Review & Revision: The policy must be updated by 1 October 2026 to align with Rules 21 and 43 which deal with managing user access to My Health Record.

Universal Application: The policy must address the specified topics regardless of organisation size due to the removal of former exemptions for smaller or remote organisations.

Dedicated Data Breach Protocols: the policy needs to explain how the organisation identifies, manages and responds to My Health Record data breaches.

The policy must be reviewed at least annually or when any significant change takes place.

Security and Access Policy

User Account & Access Management

Strict Individual Account Controls: Elimination of shared or generic staff logins; every access event must map directly to an individual user identity.

Lifecycle Governance: Formalized processes for user account creation, role updates, prompt unlinking of uncredentialed/departed staff, and regular internal access reviews.

Audit Trail Reviews: Practice Managers/OMOs should regularly monitor user access and audit logs for unusual or unauthorized activity.

Security and Access Policy – protecting My Health Record information

Physical security
- Secure practice premises and work areas
- Privacy screens where appropriate
- Preventing unauthorised access to computers and records

Information & cybersecurity
- Strong passwords and secure user access
- Antivirus and malware protection
- Security updates, patches and system maintenance
- Appropriate backups and data protection

Access monitoring
- Ability to identify individual users
- Monitoring and investigating unusual or unauthorised access
- Promptly removing access when staff leave or no longer require it

Staff awareness
- Staff understand their privacy and security responsibilities
- Security incidents and suspected breaches are reported promptly

Staff Training & compliance documentation

Fact sheet

Recommended My Health Record Training

Recommended My Health Record Training

Healthcare provider organisations must provide staff with My Health Record training *before* they are authorised to use their system, following any significant changes to My Health Record legislation and annually. The training is required to cover:

- how to use the system accurately and responsibly
- legal obligations of the healthcare provider organisation and the staff using My Health Record
- consequences of breaching those legal obligations.

Details of training provided to staff must 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 must keep a record of the organisations provision of training via a maintained training record. The organisation must retain the training record for 5 years, starting on the day the training record was created.

Available Training

Staff can access a range of free online eLearning modules about My Health Record via the Australian Digital Health Agency Online Learning Portal. At a minimum, staff should complete the My Health Record security, privacy and access eLearning module.

Staff may be directed to attend a webinar hosted by the Australian Digital Health Agency. A list of available events can be found on the Agency's webinar page.

Organisations interested in hosting eLearning modules on their own learning management system can contact engagement@digitalhealth.gov.au.

ADHA Recommended My Health Record training

Pre-Access & Refresher Training: Staff must complete mandatory training on privacy, security, and legal obligations before access is granted, followed by annual refresher training. Minimum annually.

Extended Record Retention: Practices must retain verifiable proof of staff training and operational compliance logs for a mandatory minimum period.

Security and Access Policy – how it is applied

- Communicating & making the policy accessible
- Keeping the policy up-to-date
- Record keeping

Topics	Retention Period
Procedures for authorising users and managing user accounts	5 years
Training	5 years
Process for identifying the individual who accesses a person's record (on each occasion).	2 years
Process for ensuring compliance with My Health Record data breach obligations	2 years
Security Measures	2 years

Checklist

ARE YOU READY FOR OCT 1, 2026?

Topic	Action
Policy	Security & Access Policy reviewed and updated
Access	User roles and individual access checked
Training	All authorised users trained
Accounts	Joiner/mover/leaver processes working
Records	Required evidence being retained
Security	Physical, information and cyber controls documented
Incidents	Data-breach response process understood

Links to further learning

www.digitalhealth.gov.au
Using My Health Record System: Healthcare provider education and training
Digital Health healthcare provider education and training
Digital Health Factsheets and Resources
Digital Health Agency Youtube channel
ADHA – Recommended training list
My Health Record practice managers handbook | ADHA and AAPM 2021
PIP eHealth Incentive
My Health Record legislation and governance
My Health Record Data breach notification online form
Healthcare Identifiers service
ADHA Podcasts (including My Health Record episodes)
ADHA Online Learning portal

Australian Privacy Principles Quick Reference | OAIC
AMA : What you need to know – Health Care Records | AMA

Digital health policy templates

My Health Record participation obligations and policy information
ADHA – My Health Record security and access policy template
RACGP – Policy and procedure templates hub
SEMPHN – My Health Record Security and Access policy template

For further learning and free resources:

enquiries@trainitmedical.com.au

Twitter: trainitmedical

Facebook: trainitmedical

www.trainitmedical.com.au
Access more free practice resources
& blog posts
Subscribe to our blog