WELCOME

Understanding My Health Record 2026 Changes for your Practice

Pan Teng, SNHN Digital Health Manager

Monday 14 September 2026

SNHN.ORG.AU

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

Acknowledgement of Country

Sydney North Health Network would like to acknowledge the Aboriginal lands and its traditional custodians the Cammeragyl people of the Northern Sydney region. We would like to pay our respects to past, present, and emerging Elders.

As we work to serve the community's health needs, we recognise the importance of the land and waterways as an essential component of people's health and well-being. We recognise that Aboriginal and Torres Strait Islander knowledge and learning are integral to the cultural fabric of all Australians

SNHN.ORG.AU

Housekeeping

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

All attendees are muted

This will be for the duration of the webinar

Experiencing technical issues?

Your connection may be limited, try moving closer to your Wi-Fi router

Your feedback is important!

Understanding My Health Record 2026 Changes for your Practice

All cameras will be off

As this is a webinar, your camera will remain off

Have a question?

Please use the **CHAT to make comments**, and the **Q&A for questions**

Reminder:

Be mindful not to use any patient identifying information during your participation

Neighbourhood Health Hubs & Psychology Update

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

Neighbourhood Health Hubs are part of an SNHN-led strategy to improve access, coordination and patient outcomes across **Ryde, Northern Beaches and Hornsby**.

- The hubs will connect general practice, allied health, mental health, AOD and community services
- Designed to support **simpler referral pathways**, stronger local connections & coordinated care
- **Built with and for health professionals**, informed by local data and community need

Psychology service change (from 1 July 2026)

- As part of the Neighbourhood Health Hubs rollout, psychology services transition from **New Vision Psychology** to **PCCS – Access+**
- Same core service, **no gap in care**, broader access for patients while maintaining CALD clinician support

Find out more
Scan the QR code

HealthPathways

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

Free, online health information tool which supports GPs, Hospital Doctors, Nurses, Pharmacists, Allied Health and other Clinicians within Northern Sydney.

Provides:

- ✓ Condition management
- ✓ Service navigation
- ✓ Referral information, including eReferral acceptance criteria to NSLHD outpatient services
- ✓ Access to reference materials and patient education resources

Designed to be used during patient consultations

Developed collaboratively by GPs, Hospital and Allied Health Clinicians

Evidence-informed, reflecting local reality

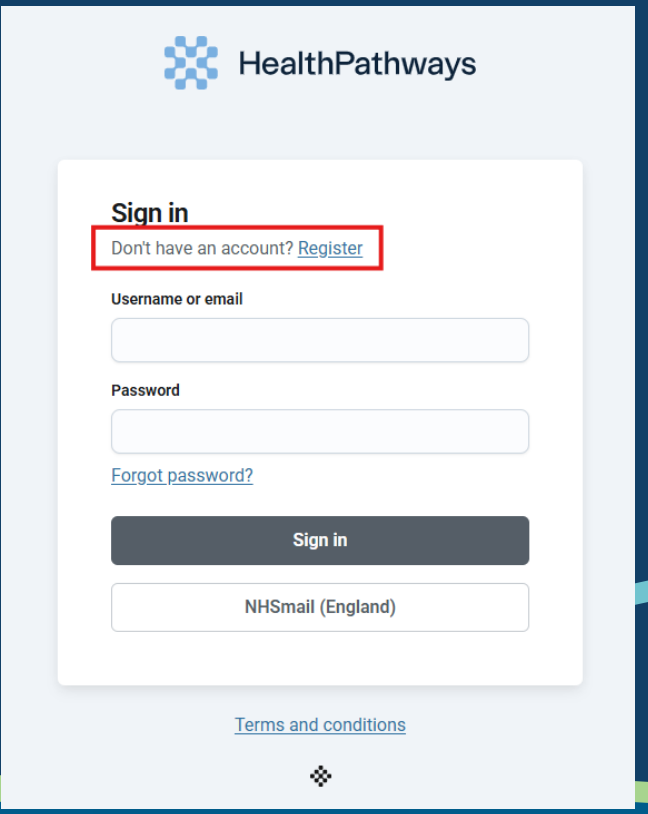
NSW GOVERNMENT Health
Northern Sydney Local Health District

Register for your Personal Account

Sydney North
HEALTHPATHWAYS

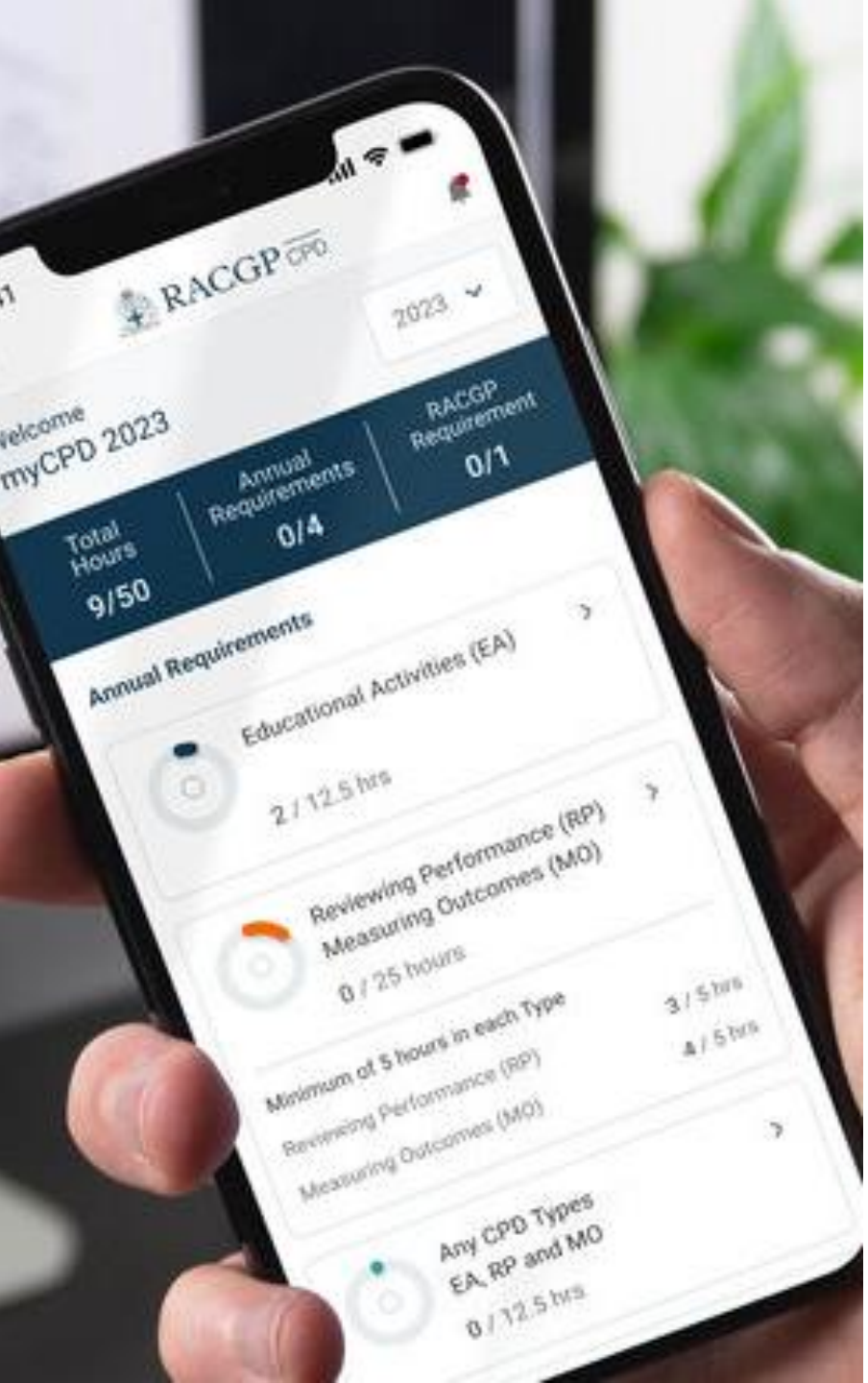
Features:

- ✓ CPD reporting
- ✓ Easy request to access other HealthPathways sites
- ✓ Enhanced security



phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network



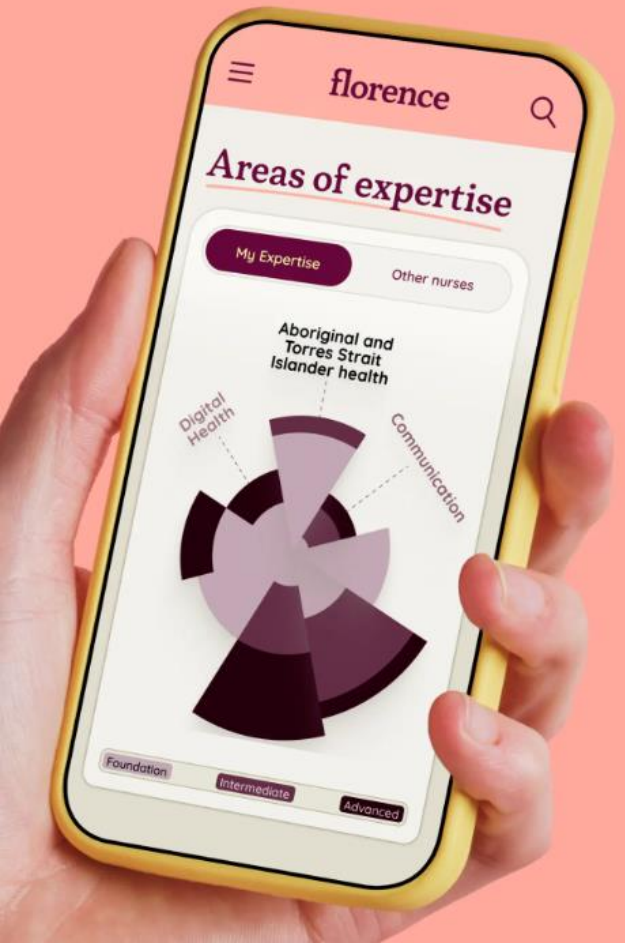
phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

RACGP Quick Log

- GPs can use the RACGP's myCPD app to log evidence of the training today.
- SNHN will provide a Statement of Attendance for your participating in this activity.
- Using the app, you can upload your evidence of participation
- The myCPD app is available on Google Play and the App Store
- The myCPD app is designed let members manage their continuing professional development from anywhere, on any device.

florence by APNA



Tailored CPD to power professional growth

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

Florence: Your Free CPD Companion

This activity is enabled with Florence – click on QR code to log your CPD

- ✓ Manage professional development easily and transparently
- ✓ Get tailored CPD recommendations from trusted sources
- ✓ Track all learning in one AHPRA-compliant place
- ✓ Set goals and monitor progress at a glance
- ✓ Consolidate past and current CPD records
- ✓ Made for Nurses & Midwives
- ✓ Personalized learning suggestions
- ✓ 100% free, no subscription required

GET IT ON Google Play

Download on the App Store

SNHN.ORG.AU

What is My Health Record?

Online summary of an individual's key health information

Personally controlled

Part of a national system

Accessible at all times

Protected by legislation

My Health Record documents

Healthcare provider documents

- Shared health summaries
- Discharge summaries
- Event summaries
- Prescription and dispense records
- Specialist letters
- Pharmacist Shared Medicines List
- Diagnostic Imaging reports
- Pathology reports
- Goals of care
- eReferrals
- Residential care transfer reason
- Residential care health summary
- Residential care medication chart

My Health Record

Medicare information

- Prescription information
- Australian Immunisation Register
- Australian Organ Donor Register
- Medicare Services -MBS and DVA items

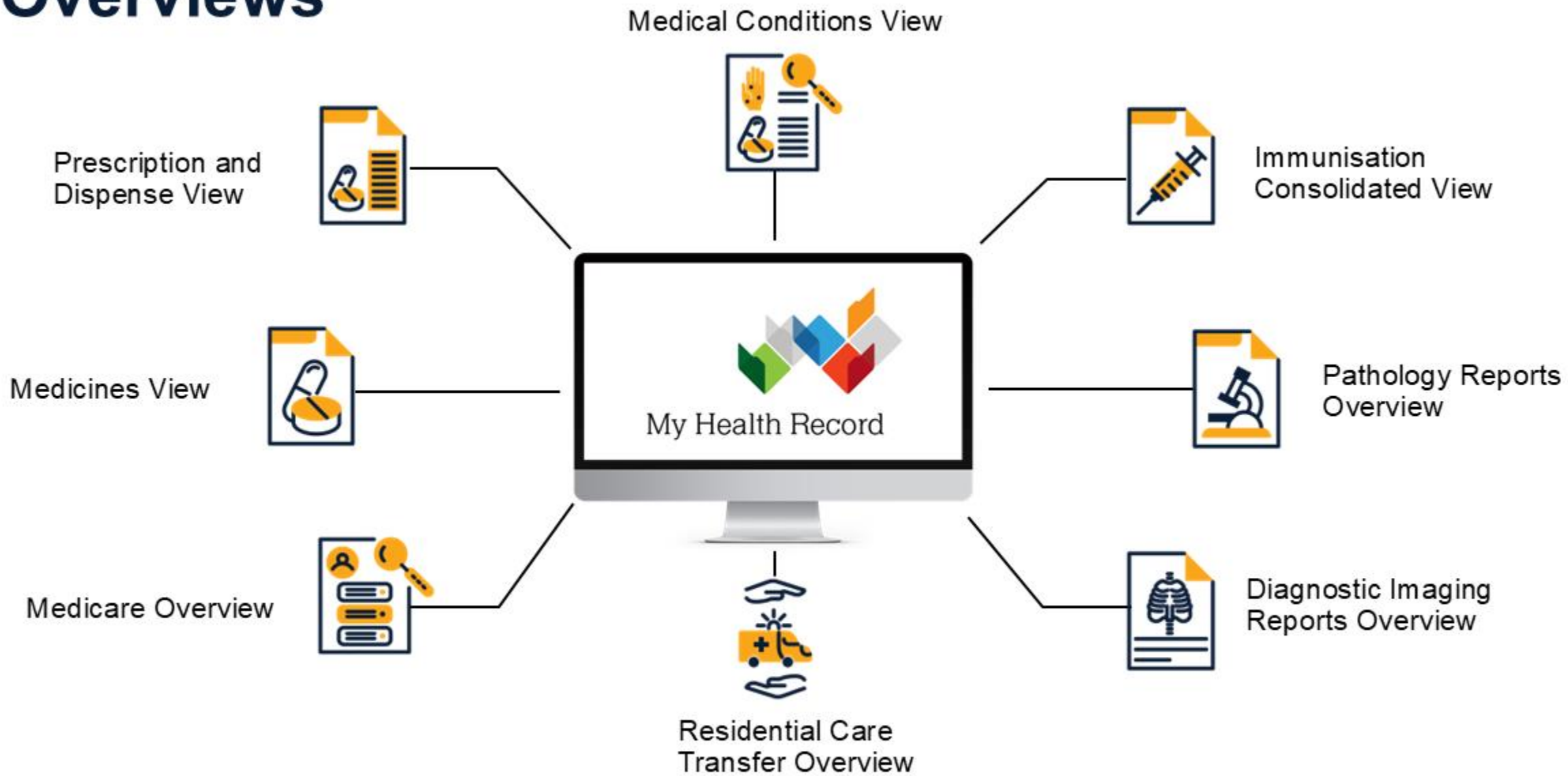
Consumer entered information

- Personal health summary
- Personal health notes
- Advance Care Planning documents
- Emergency contacts

Shared with My Health Record

- Care and support plans
- MyMedicare registrations

Overviews


Medical Conditions View
Prescription and Dispense View
Immunisation Consolidated View
Medicines View
My Health Record
Pathology Reports Overview
Medicare Overview
Diagnostic Imaging Reports Overview
Residential Care Transfer Overview

My Health Record - benefits

Enhanced continuity of care in a person's health journey

Improved access to clinical information, especially in the context of an emergency

Improved access to medication history and visibility of medications prescribed

Enhanced capacity to better coordinate care and provide support for a person and their carers

Greater understanding and visibility between healthcare providers involved in the care of a person

Enhanced self-management

My Health Record matters for care delivery by

- reducing the need to request faxed or paper records
- helping to check information a patient shares
- letting healthcare providers quickly see important health information shared by other healthcare providers.
- providing allergy and adverse reactions information.
- listing immunisations records and medicines information.
- stopping the need to repeat blood tests or scans that have already been done, and
- making it easier for health information to be shared, including information to help guide care at the end of someone's life and to show if they want to be an organ donor.

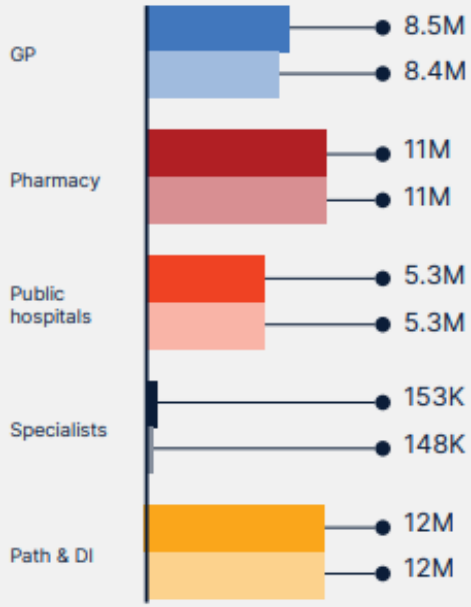
July 2026 national stats

Providers

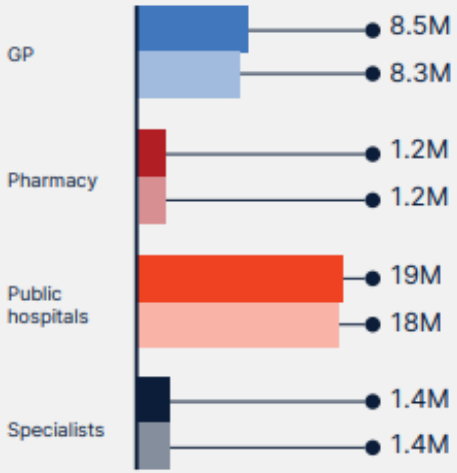
https://www.digitalhealth.gov.au/initiatives-and-programs/my-health-record/statistics

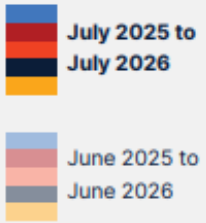
Providers

Healthcare providers **uploaded** documents that were **looked at by other** healthcare provider organisations

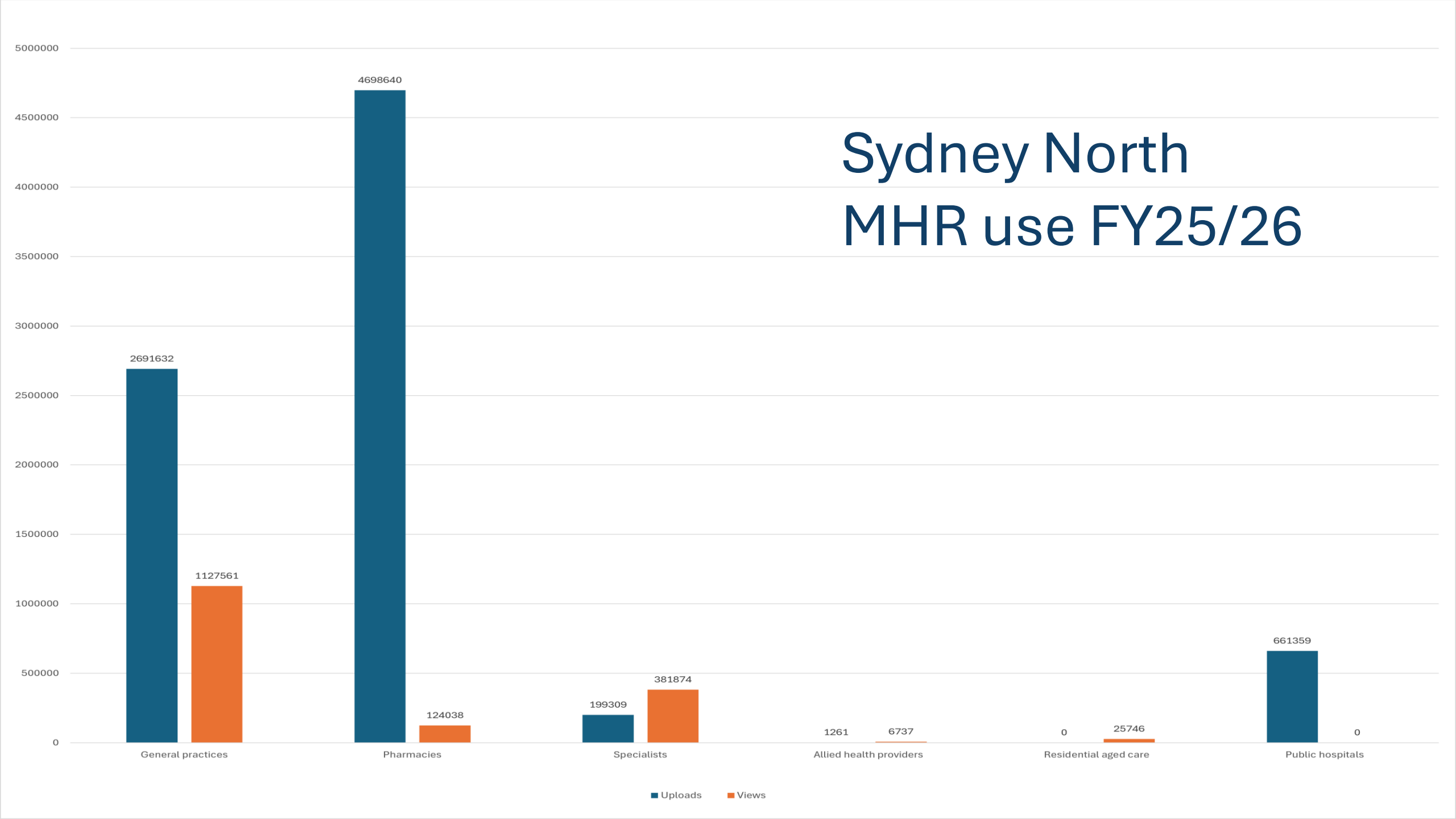


Healthcare providers **looked at** documents that were **uploaded by other** healthcare provider organisations





Sydney North
MHR use FY25/26



What is better and faster access?

Better access: introducing a legislative requirement for information to be shared with My Health Record by default, starting with pathology and diagnostic imaging reports.

Faster access: amending the 7-day delay to provide consumers with access to most of their results as soon as they have been uploaded to My Health Record. For some categories of results, there will be a 5-day delay before consumers can access them (based on the test type, not the result).

Faster Access

Aligned with CRG recommendations

October 2025

Pathology Test Type	Patient Access Delay
Anatomical and cytopathology tests, genetic tests	5 days
Other pathology results	No delay

February 2026

Diagnostic Imaging Report type	Patient Access Delay
Cross sectional Imaging reports (CT, MRI, PET, Ultrasound) and X-ray reports – head and thorax (chest, abdomen, pelvis)	5 days
X-ray extremities	No delay

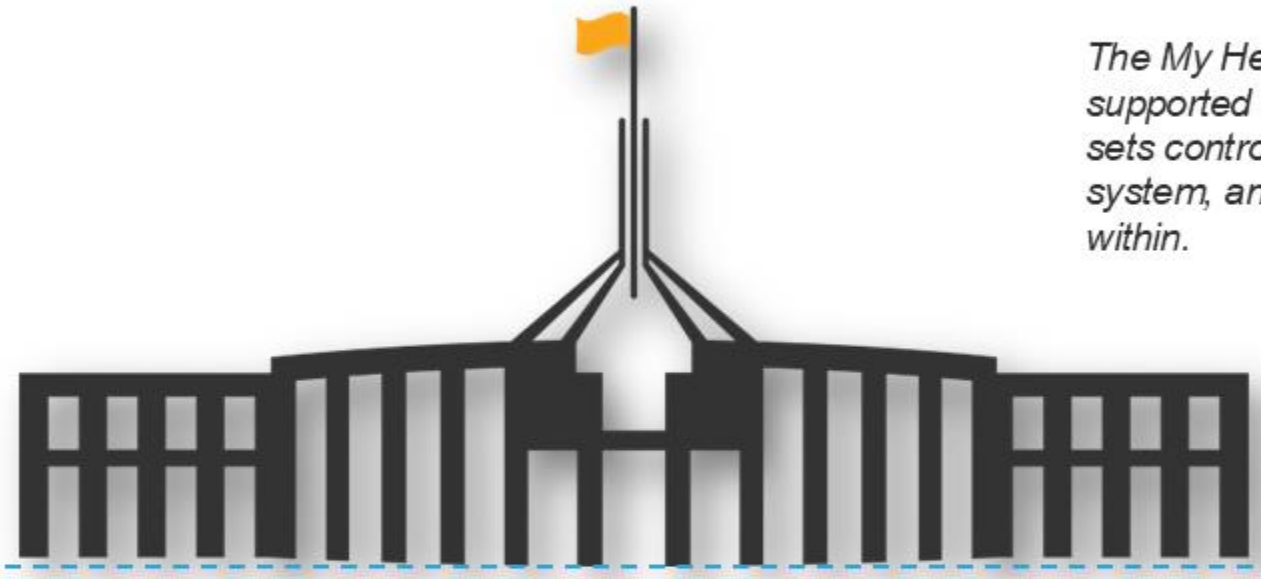
My Health Record – System Security

- Many safeguards are in place to protect the My Health Record system.
- These include strong encryption, firewalls, secure login processes and audit logging.

- The Agency monitors the system.
- Health information in the system is protected by legislation.
- Significant penalties apply for deliberate misuse.

- All data within the My Health Record system is stored securely in Australia.
- External software goes through a conformance process before it is allowed to connect.

My Health Record 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.

- Privacy Act 1988
- Healthcare Identifiers Act 2010
- My Health Records Act 2012
- My Health Record (Share by Default) Rules 2025
- My Health Records Regulations 2026
- My Health Records Rules 2026

My Health Record – what do healthcare organisations need to do?

Ensure there is a My Health Record security and access policy

Register and set up access

Train staff and ensure they are familiar with policies in place

Enable user account access for appropriate staff

Ongoing participation and obligations

My Health Record – Security & Access Policy

Registered healthcare provider organisations that use, or upload documents into, the My Health Record system are required to develop and maintain a My Health Record security and access policy that outlines the:

- Process for identifying and authorising users, and for suspending or deactivating accounts of those who no longer require access.
- Training to be provided to the workforce on the responsible use of the My Health Record system, professional and legal obligations and the consequences of non-compliance.
- Physical, technical and cybersecurity measures implemented to control access to the system.
- Identification, management and escalation of system-related security risks.
- Process for ensuring data breach reporting obligations are being met.
- Record-keeping practices that will be followed.

https://www.digitalhealth.gov.au/healthcare-providers/initiatives-and-programs/my-health-record/register-and-set-up-access/participation-obligations

My Health Records Rules 2026 changes

The My Health Records Rule 2016 has been replaced by the new My Health Records Rules 2026 effective 1 April 2026.

Existing participants (registered for My Health Record prior to 1 April 2026):

- Transition period – Previous requirements under Rule 42 of the My Health Records Rule 2016 will continue to apply to registered organisations until 1 October 2026.
- Organisations must update existing policy by 1 October 2026 in line with the 2026 Rules.

New participants (organisations registering for My Health Record from 1 April 2026):

- Develop a security and access policy in accordance with the requirements outlined in Rule 21 of the My Health Records Rules 2026.
- Requirements under the My Health Records Rules 2026 now apply to all organisations irrespective of their size.

Policy Guidance: https://www.digitalhealth.gov.au/healthcare-providers/initiatives-and-programs/my-health-record/register-and-set-up-access/participation-obligations

My Health Records Rules 2026 changes – security and access policy

The policy must continue to be reviewed at least annually and when new or changed risks are identified. In addition, it must now be reviewed upon request by the System Operator.

Revised and expanded security and access policy requirements include:

- **Procedures** authorising access to the My Health Record system and deactivating or suspending user access includes procedures for creating and modifying user accounts and suspension and deactivation of user accounts of individual healthcare providers ceasing to be linked to the organisation.
- **Training** provided to employees required not just before being authorised to access My Health Record system but also annually and following any significant changes to the My Health Record system and governing legislation.
- **Processes** used by the organisation must also address how the organisation will ensure compliance with its My Health Record data breach obligations.
- **Security measures** the organisation will implement must include not only physical and information security measures (account management) but also cybersecurity, and technical and organisational measures (e.g. data protection, including encryption and regular back-up, regular system maintenance and monitoring and review measures).
- **No longer required** for the policy to address assisted registration (however it is recommended healthcare provider organisations include it in the policy, if providing this service).

Note: Other changes under the Rules 2026 reflect expanded or clarified requirements, not entirely new matters

My Health Record Rules 2026 changes – record keeping

Authorising access to My Health Record system (5 years)

- How the healthcare provider organisation authorises access to the My Health Record system, including records of the user accounts created, changed, suspended or deactivated.

Training (5 years)

- The training that has been provided to employees of the healthcare provider organisation before they were authorised to access the My Health Record system, annually and following significant changes to the legislation or system.

Identification (2 years)

- How the healthcare provider organisation has applied the process for identifying a person requesting access to My Health Record and communicating their identity to the System Operator.

Data breach obligations (2 years)

- How the healthcare provider organisation ensures that it can identify, manage and respond to My Health Record data breaches and that these processes comply with obligations under section 75 of the *My Health Records Act 2012* (for example, evidence of documented processes and any action planned or taken).

Security measures (2 years)

- How the healthcare provider organisation has implemented physical security, information security, cybersecurity, technical and organisational measures.

Each iteration of the policy (5 years)

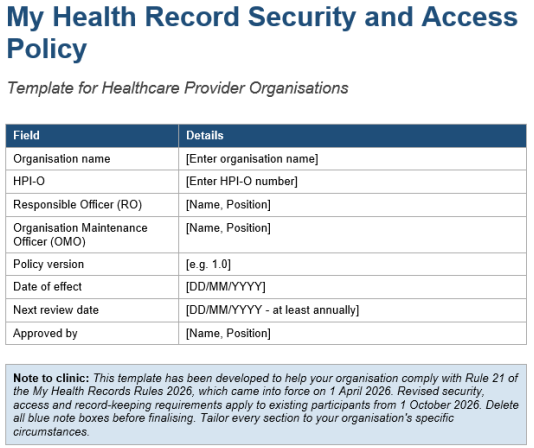
- The healthcare provider organisation must keep a record of each iteration of the policy for 5 years starting the day the iteration comes into effect.

Advance care planning

- For healthcare provider organisations that upload advance care planning information, it is now a requirement to keep a record of the recipient's instructions and how their instructions were provided.

Sample MHR templates

1. MHR Security & Access Policy
2. MHR User Access Register
3. MHR Staff Training Register
4. MHR Data Breach & Incident Response
5. MHR Annual Review Checklist

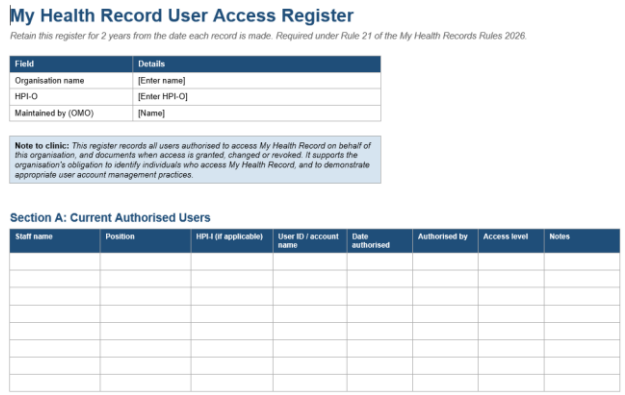


My Health Record Security and Access Policy

Template for Healthcare Provider Organisations

Field	Details
Organisation name	[Enter organisation name]
HPI-O	[Enter HPI-O number]
Responsible Officer (RO)	[Name, Position]
Organisation Maintenance Officer (OMO)	[Name, Position]
Policy version	[e.g. 1.0]
Date of effect	[DD/MM/YYYY]
Next review date	[DD/MM/YYYY - at least annually]
Approved by	[Name, Position]

Note to clinic: *This template has been developed to help your organisation comply with Rule 21 of the My Health Records Rules 2026, which came into force on 1 April 2026. Revised security, access and record-keeping requirements apply to existing participants from 1 October 2026. Delete all blue note boxes before finalising. Tailor every section to your organisation's specific circumstances.*



My Health Record User Access Register

Retain this register for 2 years from the date each record is made. Required under Rule 21 of the My Health Records Rules 2026.

Field	Details
Organisation name	[Enter name]
HPI-O	[Enter HPI-O]
Maintained by (OMO)	[Name]

Note to clinic: *This register records all users authorised to access My Health Record on behalf of this organisation, and documents when access is granted, changed or revoked. It supports the organisation's obligation to identify individuals who access My Health Record, and to demonstrate appropriate user account management practices.*

Section A: Current Authorised Users

Staff name	Position	HPI-I (if applicable)	User ID / account name	Date authorised	Authorised by	Access level	Notes

My Health Record Staff Training Register

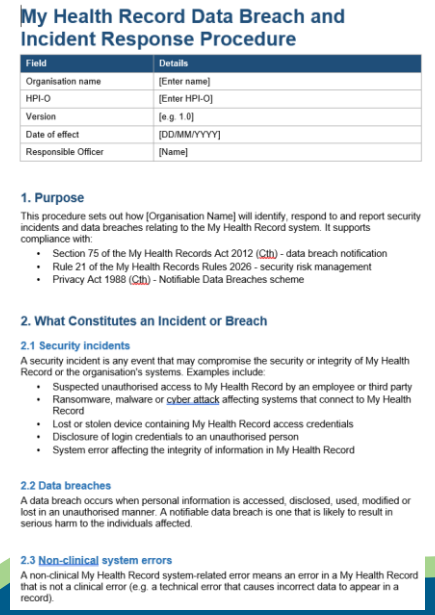
Retain all training records for 5 years from the date of training. Required under Rule 21 of the My Health Records Rules 2026.

Field	Details
Organisation name	[Enter name]
HPI-O	[Enter HPI-O]
Maintained by	[RO / OMO name]

Note to clinic: *This register documents My Health Record training completed by all staff and authorised users. A 5-year retention period applies under the My Health Records Rules 2026 - this is a new requirement. Training records must be available for inspection by ADHA or the OAIC on request.*

Training Log

Staff name	Position	Training type / module	Training provider / method	Date completed	Expiry / next refresh due	Staff sign-off	Supervisor sign-off



My Health Record Data Breach and Incident Response Procedure

Field	Details
Organisation name	[Enter name]
HPI-O	[Enter HPI-O]
Version	[e.g. 1.0]
Date of effect	[DD/MM/YYYY]
Responsible Officer	[Name]

1. Purpose

This procedure sets out how [Organisation Name] will identify, respond to and report security incidents and data breaches relating to the My Health Record system. It supports compliance with:

- Section 75 of the My Health Records Act 2012 (Cth) - data breach notification
- Rule 21 of the My Health Records Rules 2026 - security risk management
- Privacy Act 1988 (Cth) - Notifiable Data Breaches scheme

2. What Constitutes an Incident or Breach

2.1 Security incidents

A security incident is any event that may compromise the security or integrity of My Health Record or the organisation's systems. Examples include:

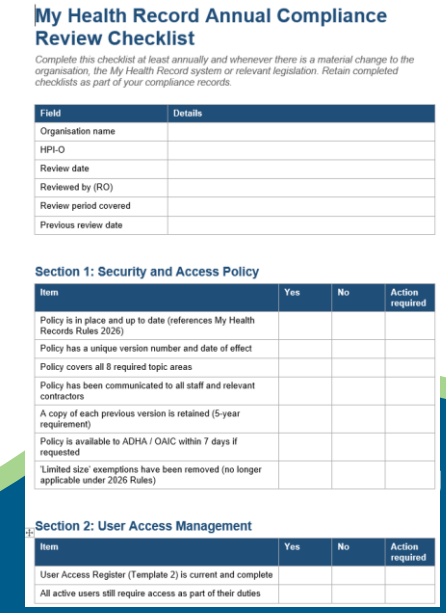
- Suspected unauthorised access to My Health Record by an employee or third party
- Ransomware, malware or cyber attack affecting systems that connect to My Health Record
- Lost or stolen device containing My Health Record access credentials
- Disclosure of login credentials to an unauthorised person
- System error affecting the integrity of information in My Health Record

2.2 Data breaches

A data breach occurs when personal information is accessed, disclosed, used, modified or lost in an unauthorised manner. A notifiable data breach is one that is likely to result in serious harm to the individuals affected.

2.3 Non-clinical system errors

A non-clinical My Health Record system-related error means an error in a My Health Record that is not a clinical error (e.g. a technical error that causes incorrect data to appear in a record).



My Health Record Annual Compliance Review Checklist

Complete this checklist at least annually and whenever there is a material change to the organisation, the My Health Record system or relevant legislation. Retain completed checklists as part of your compliance records.

Field	Details
Organisation name	
HPI-O	
Review date	
Reviewed by (RO)	
Review period covered	
Previous review date	

Section 1: Security and Access Policy

Item	Yes	No	Action required
Policy is in place and up to date (references My Health Records Rules 2026)			
Policy has a unique version number and date of effect			
Policy covers all 8 required topic areas			
Policy has been communicated to all staff and relevant contractors			
A copy of each previous version is retained (5-year requirement)			
Policy is available to ADHA / OAIC within 7 days if requested			
'Limited size' exemptions have been removed (no longer applicable under 2026 Rules)			

Section 2: User Access Management

Item	Yes	No	Action required
User Access Register (Template 2) is current and complete			
All active users still require access as part of their duties			

Source: Medical Business Services

MHR Security & Access Policy – 2026 Rules

Highest priority – do now

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

- Verify key contact details including your Responsible Officer (RO) and Organisation Maintenance Officer (OMO)
- Review your third-party IT provider arrangements & apply software vendor updates promptly
- Include details on:
  - Authorised users
  - Account creation & removal
  - Cybersecurity & data protection measures
  - User training arrangements
  - Risk management
  - Annual review
  - Version control - this policy & your previous policies
  - Retain all policies for 5 years
- Refer to sample MHR Security & Access Policy Template
- Conduct an annual compliance review of the Policy

You may already perform many of these activities, but the 2026 changes now require them to be formally documented, evidenced, monitored ongoingly & shared with the Australian Digital Health Agency (ADHA) if requested to assess compliance.

4. Authorising and Managing User Access

4.1 Authorisation process

Only individuals who require access to My Health Record as part of their duties will be authorised. The RO or OMO must authorise each user before they are granted access.

The authorisation process is:

1. The manager or RO identifies the need for a staff member to access My Health Record.
2. The staff member completes required training (see Section 5).
3. The RO or OMO creates or assigns a unique user account in [clinical software name / National Provider Portal] linked to the individual's HPI-I or unique internal identifier.
4. The user is added to the organisation's User Authorisation Register.
5. The RO or OMO confirms the registration is in place in PRODA.

4.2 Account suspension and deactivation

A user account must be suspended or deactivated promptly in the following circumstances:

- The user leaves the organisation - deactivate within [e.g. 1 business day] of departure
- The user's credentials are compromised or suspected to be compromised - suspend immediately
- The user changes role and no longer requires My Health Record access - deactivate within [e.g. 5 business days]

The process for deactivation is:

6. The RO or manager notifies the OMO of the change.
7. The OMO disables the user account in [clinical software / NPP] and removes access.
8. The User Authorisation Register is updated with the date of deactivation.

> **Note to clinic:** *Records of user access management - including how access was granted, modified and revoked - must be retained for 2 years under Rule 21 of the My Health Records Rules 2026. Maintain these records in the User Access Register (Template 2).*

4.3 Regular access reviews

The RO or OMO will review the user access register at least every [e.g. 6 months] to confirm all listed users still require access. Accounts for users who no longer require access will be deactivated.

The organisation will regularly verify that all individuals accessing My Health Record on its behalf hold a current, unconditional healthcare provider registration (HPI-I not suspended, cancelled, conditional or lapsed).

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

MHR Security & Access Policy – 2026 Rules

SNHN.ORG.AU

5. Training for Authorised Users

5.1 Training requirement

No user may be authorised to access My Health Record until they have completed training covering:

- How to use My Health Record accurately and responsibly
- The legal obligations of the organisation and individuals who access the system
- The consequences of breaching those obligations

5.2 Training delivery

Training type	Details
Initial training	[Describe method - e.g. ADHA e-learning module, induction session, etc.]
Refresher training	[Frequency and method - e.g. annually]
Training on policy updates	[How staff are notified and trained when this policy changes]

5.3 Training records

Records of training completed must be retained for 5 years. Training is recorded in the Staff Training Register (Template 3).

> **Note to clinic:** *The 5-year training record retention period is a new requirement under the My Health Records Rules 2026. Under the previous Rules 2016, no specific retention period was prescribed for training records.*

6. Identifying the Individual Who Accesses a Record

Each time My Health Record is accessed on behalf of this organisation, the system logs the user identifier and the activity. Our organisation's process for identifying which individual corresponds to a logged user ID is:

- [Describe: e.g. clinical software assigns each staff member a unique user ID linked to their name and HPI-I; access logs are maintained in the clinical software and can be queried by the RO]

If the Australian Digital Health Agency (ADHA) requests the identity of a user who accessed My Health Record, the process is:

9. The RO receives the request from ADHA.
10. The RO or OMO queries the [clinical software / NPP] access logs using the user ID or date/time provided.
11. The RO identifies the staff member associated with that user ID.
12. The RO communicates the identity to ADHA within the required timeframe.

> **Note to clinic:** *This process must be documented here in sufficient detail to allow your organisation to respond to ADHA requests. Failure to comply may result in regulatory action.*

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

MHR Security & Access Policy – 2026 Rules

SNHN.ORG.AU

7. Physical and Information Security

7.1 Physical security measures

The following physical security measures are in place to prevent unauthorised access to My Health Record:

- [e.g. Computer screens positioned away from public view / privacy screens installed on workstations used to access MHR]
- [e.g. Devices used to access MHR are located in secure areas not accessible to patients or the public]
- [e.g. Screen lock activates automatically after [X] minutes of inactivity]
- [Add/remove as applicable to your organisation]

7.2 Information and cyber security measures

The following information security measures are in place:

- [e.g. Access to MHR requires unique login credentials - shared accounts are not permitted]
- [e.g. Multi-factor authentication (MFA) is required to access MHR / clinical software]
- [e.g. Passwords must comply with the organisation's password policy: minimum [X] characters, complexity requirements, changed every [X] months]
- [e.g. Clinical software and operating systems are kept up to date with security patches]
- [e.g. Remote access to systems that connect to MHR is protected by VPN and MFA]
- [e.g. Access to MHR is restricted to authorised devices only]

Note to clinic: *The My Health Records Rules 2026 adopt a technology-neutral approach to security - specific technologies such as access flags are no longer prescribed. Your policy should describe the actual controls your organisation uses, which may include multi-factor authentication, modern identity and access management (IAM), or role-based access controls. The key requirement is that each user is uniquely identified and protected by a robust authentication mechanism.*

7.3 User account management

The organisation employs the following user account management practices:

- Access is restricted to personnel who require it as part of their duties
- Each individual is uniquely identified in our IT systems and in My Health Record
- Unique identities are protected by a password or equivalent authentication mechanism
- Passwords and authentication mechanisms are sufficiently secure to prevent unauthorised access
- User accounts are disabled promptly when a person is no longer authorised to access the system
- User accounts are suspended immediately if a compromise of credentials is suspected or confirmed

Note to clinic: *All organisations must comply with these baseline security requirements regardless of size. The limited-size exemption that applied under the My Health Records Rule 2016 has been removed. Small practices and sole traders must now meet the same minimum standards as larger organisations.*

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

MHR Security & Access Policy – 2026 Rules

SNHN.ORG.AU

8. Identifying, Responding to and Reporting Security Risks

8.1 Identifying security risks

The organisation uses the following measures to identify system-related security risks:

- [e.g. Regular review of audit logs in clinical software to identify unusual access patterns]
- [e.g. Staff are required to report suspected security incidents immediately to the RO]
- [e.g. Annual security review conducted by RO or nominated IT provider]

8.2 Responding to security incidents

On becoming aware of a security incident, the RO will:

13. Contain the incident - e.g. suspend compromised accounts, disconnect affected systems if appropriate
14. Assess the nature and scope of the incident
15. Document the incident in the Incident Register
16. Notify relevant parties as required (see 8.3 below)
17. Remediate the cause of the incident
18. Review policies and controls to prevent recurrence

8.3 Reporting obligations

The organisation will notify ADHA and, where relevant, the OAIC as soon as practicable after becoming aware of a potential or actual data breach relating to My Health Record, in accordance with Section 75 of the My Health Records Act 2012.

The organisation will notify ADHA within 2 business days of becoming aware of:

- A non-clinical My Health Record system-related error in a record
- A material change to the organisation (e.g. change of ownership, cessation of business)

The organisation must notify ADHA within 14 days if it ceases to be eligible for My Health Record registration.

Note to clinic: *See Template 4 (Data Breach and Incident Response Procedure) for the full breach notification procedure.*

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

MHR Security & Access Policy – 2026 Rules

SNHN.ORG.AU

9. Assisted Registration

Note to clinic: *Complete this section if your organisation offers assisted registration (helping patients register for My Health Record). If your organisation does not offer assisted registration, state this clearly and retain the section.*

[Select one option and delete the other:]

Option A - Organisation DOES NOT provide assisted registration:

[Organisation Name] does not provide assisted registration services. Staff are not authorised to register patients for My Health Record on their behalf.

Option B - Organisation DOES provide assisted registration:

Where [Organisation Name] offers assisted registration, the following procedures apply:

- Only staff specifically authorised by the RO may provide assisted registration
- Staff must complete training on assisted registration before being authorised
- Consent from the patient (or authorised representative) must be confirmed and documented before registration proceeds
- The patient's identity must be verified according to the following process: [describe verification process, e.g. sighting Medicare card and photo ID]
- Assisted registration is conducted in accordance with the My Health Records Act 2012

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

MHR Security & Access Policy – 2026 Rules

10. Policy Implementation and Maintenance

10.1 Communication

This policy will be communicated to all employees and relevant contractors by:

- [e.g. Provided to all staff as part of induction]
- [e.g. Available on the practice intranet / shared drive]
- [e.g. Reviewed with all staff at the annual staff meeting]

10.2 Review

This policy must be reviewed:

- At least annually
- When material new or changed risks are identified
- When there is a significant change to the My Health Record system, legislation, or the organisation's operations

10.3 Record-keeping

Under Rule 21 of the My Health Records Rules 2026, the following records must be retained:

Record type	Retention period	Stored location
Copies of each version of this policy	5 years	[e.g. Practice management system / shared drive]
Staff training records	5 years	[e.g. Training Register - Template 3]
User access management records (how access was granted, modified, revoked)	2 years	[e.g. User Access Register - Template 2]

Note to clinic: *These retention periods are new under the My Health Records Rules 2026. The previous Rules 2016 did not specify a time limit for retaining policy versions or training records. Under the new rules: policy copies must be kept for 5 years; training records must be kept for 5 years; and operational security records (user access management, security measures) must be kept for 2 years. ADHA may request a copy of the current or a previous version of this policy at any time, and the organisation must respond within 7 days.*

10.4 Version control

Each version of this policy must have a unique version number and date of effect. A record of all versions must be maintained:

Version	Date of effect	Summary of changes	Approved by
1.0	[DD/MM/YYYY]	Initial policy - updated for My Health Records Rules 2026	[Name]

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

MHR Security & Access Policy – 2026 Rules

SNHN.ORG.AU

11. Providing Healthcare Regardless of My Health Record Status

This organisation provides healthcare services to all patients regardless of whether they have a My Health Record or have applied access controls to their record. Access controls applied by a patient (including emergency access override situations) are respected in accordance with the My Health Records Act 2012.

12. Information Quality

The organisation takes reasonable steps to ensure that any information uploaded to My Health Record is:

- Accurate and up to date at the time of upload
- Easily understood
- Not defamatory or subject to copyright
- Prepared by registered healthcare providers holding a current, unconditional HPI-I

Before uploading clinical documents, staff must confirm the information is current and that the authoring clinician has a valid, active registration.

13. Consumer Notifications

Patients may elect to receive notifications when their My Health Record is accessed by this organisation or a nominated representative. The organisation supports and respects patient notification preferences as set within their My Health Record account.

14. Policy Approval

Field	Details
Approved by (RO)	[Name and signature]
Position	[Position title]
Date	[DD/MM/YYYY]
Next review due	[DD/MM/YYYY]

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

MHR Security & Access Policy – 2026 Rules

SNHN.ORG.AU

User Access

- Review all your current users – only authorised access
- Deactivate accounts immediately if MHR access is no longer required
- Ensure unique user logins & prohibit shared accounts
- Use Multi-factor authentication
- Conduct an annual access review
- Keep an updated user access register for all active & deactivated users in your practice

Staff Training

- Establish annual refresher MHR training for clinicians & staff
- Ensure MHR training is done for new staff inductions, prior to use
- Keep all attendance & competency completion records in a MHR training register
    - Recommended MHR Training factsheet is available here: My Health Record for healthcare providers

Data breaches & incident reporting

- Create a procedure to notify relevant authorities of data breaches, security incidents or organisational changes within required timeframes
  - Clinical incident or error – report ASAP to ADHA - call My Health Record Helpline 1800 723 471 (24 hours a day, 7 days a week)
  - Data breach – report ASAP to ADHA & OAIC
  - Non-clinical incidents or material organisational changes – within 2 business days
  - Organisation cease to be eligible for MHR registration – within 14 business days
- Maintain an audit log & incident register
- Perform an annual risk assessment, document findings & controls

Advance care planning – 2026 Rules

- You may upload advance care planning information only if instructed by the patient.
- You must retain records of patient instructions and how instructions were provided.

Recognition of Cert IV Aboriginal & Torres Strait Islander Primary Care practitioners – 2026 Rules

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

- Is now a prescribed class of nominated healthcare provider

<u>ACCHOs & Aboriginal Health Services</u>

- Review workforce roles
- Consider if practitioners should be utilised as nominated healthcare providers within MHR workflows
- Update local governance & clinical guidance, where relevant

Data quality

- Take reasonable steps to ensure all records uploaded to MHR by your clinicians (e.g. Shared Health Summaries) contain correct, accurate, not out of date & non-defamatory information
- Review current workflows & upload quality checks
- Educate clinicians on data accuracy responsibilities & have data correction pathways

Other providers are looking at your data to help inform their patient care

Audit expectations & record keeping

- Ensure all the documentation are securely stored & centrally accessible by your staff
- Retain training & user management records for 5 years
- Retain security control records for 2 years
- Prepare for potential ADHA compliance reviews
- Nominate responsible staff who will assist in audits

How to get support on this

- Consult your 2026 MHR Security & Access Policy
- Contact your organisation's OMO or RO
- Contact SNHN Digital Health team – digitalhealth@snhn.org.au
- Contact the ADHA - My Health Record Helpline 1800 723 471 or help@digitalhealth.gov.au
- Office of the Australian Information Commissioner (OAIC) – Call 1300 363 992 or online enquiry form

Additional Resources

Scan QR code to access Digital Health eLearning

Scan QR code to access factsheets and materials

Scan QR code to access information for healthcare providers

Scan QR code to access Agency YouTube channel

Sydney North Health Network

Questions

Thank you for participating in todays webinar.

Please remember to use your phone to complete the evaluation by QR code

phn NORTHERN SYDNEY
An Australian Government Initiative

Sydney North Health Network

Understanding My Health Record
2026 Changes for your Practice

SNHN.ORG.AU