My Health Records Rules: 2016 vs 2026

A summary of key changes and actions for registered organisations.

Registered before 1 April 2026
Update your security and access policy by 1 October 2026, in line with the 2026 Rules.

Registering from 1 April 2026
Develop your security and access policy in accordance with the 2026 Rules from the outset.

Area	2016 Rule	2026 Rules	Action for your home	Status	Already in your Quality Standards systems
Data breach response	No requirement to have a documented breach response process in the policy. Notification obligation existed under s.75 of the MHR Act only.	Policy must now explicitly document the processes for ensuring your home does not contravene s.74 or s.75 of the MHR Act, including how it will identify, manage and respond to MHR data breaches (Rule 21(2)(c)).	**Action required** Add a specific MHR data breach response process to your policy. A generic organisational breach policy is not sufficient as MHR breaches must be explicitly addressed.	New	Partly. Your risk management system (Outcome 2.4) and incident management system (Outcome 2.5) already cover identifying and responding to incidents. The MHR breach process can extend these rather than being built separately.
Record keeping: access records	No specific retention period defined for audit logs, access records or training records.	Rule 45 sets retention periods: user account and training records 5 years; records of security measures and of the s.74/s.75 processes 2 years. Access logs are given as an example without a stated period.	**Action required** Check what retention your aged care clinical or care management software applies to audit logs and access records. Set to 5 years to be safe. This may require a configuration change, so confirm settings with your software vendor.	New	Partly. Outcome 2.7's information management system covers records generally, but audit log retention is an MHR-specific technical setting to confirm with your vendor.
Training	Required training before users access the system, and annually or after significant changes. No defined period for keeping training records.	These records must be kept for 5 years.	**Action required** Training is required for all staff accessing MHR before the transition period end date of 1 October 2026. This can be built into your existing training system under Standard 2 (Outcome 2.9) of the Quality Standards. Keep this record for 5 years.	Updated	Yes. Outcome 2.9 already requires a training system with records of worker training and competency. Add MHR as a tracked training item within it.
Record keeping: policy versions	Each version of the policy must be retained, but no defined time limit.	Policy versions must now be retained for a minimum of 5 years (Rule 43(4)).	**Action required** Formalise how and where you store old policy versions. 5 years is a minimum, so check your Aged Care	Updated	Yes. Outcome 2.7 already requires an information management system for policies and procedures. Apply the 5-year rule within that existing system.

			Act and state records obligations before disposing of anything.		
Size exemption	Small organisations could self-select out of certain policy requirements if judged not applicable due to limited size.	Size exemption removed. All organisations regardless of size must meet the same baseline requirements. This applies to every registered HPI-O, including small or single-site locations, with no size-based exemption.	**Action required (small homes)** If your policy previously excluded any sections on the basis of size, those sections must now be included. Standalone and single-site homes are not exempt.	**Updated**	No direct equivalent. This is an MHR-specific administrative rule rather than a Quality Standards requirement.
User account management	Rule 43 set out user account management requirements: restricting access to those who need it, unique user identification, password protection, and deactivating accounts. Policy content sat in Rule 42.	Rule 21(2)(a) now requires the policy to cover the full account lifecycle, including procedures for creating and modifying accounts, not just suspending and deactivating them. Rule 21(4) retains the account management practices and requires them to be reviewed at least annually.	**Action required** Add procedures for creating and modifying user accounts to your policy, and cover what happens when an individual healthcare provider ceases to be linked to your home. Confirm you review your account management practices annually.	**Updated**	Partly. Outcome 2.9's workforce and role-based systems support who should have access, but MHR account controls themselves sit outside the Quality Standards.
Physical and information security	Required physical and information security measures. Referenced specific technologies as forms of access control.	Same requirement, updated to reflect contemporary cyber security expectations. No specific technologies prescribed.	*No action if security practices are current.* Review policy wording to remove references to outdated or overly specific technologies.	**Updated**	Partly. Outcome 2.7's information management system covers security of records generally, though MHR-specific cyber security expectations go further.
Access flags	Access flags were a consumer-side control. Healthcare recipients used them to control which organisations could see their record. They sat in the System Operator rules, separate from the provider user account requirements.	Reference removed. The Rules now describe access controls generically (Rules 8 and 9). Consumers keep the same ability to restrict access and lift a restriction on a particular occasion.	*No action.* If your policy references access flags by name, update the wording but nothing changes for staff or residents.	**Updated**	No direct equivalent. This is an MHR technical/legislative detail.
Annual policy review	Policy must be reviewed annually and when material risks change.	Rule 43(3)(c) retains both triggers and adds a third: review on request by the System Operator. Rule 43(3)(d) sets out what a review must consider.	**Action required** Add review on request by the System Operator as a trigger. Make sure your review considers unauthorised access, misuse or unauthorised disclosure, accidental disclosure, changes to the MHR system, and legal or regulatory changes since the	**Updated**	Yes. Outcome 2.3's continuous improvement and quality system review cycle already covers regular policy review.

			last review. Use your next scheduled annual review to fold in all 2026 Rule updates by 1 October 2026.		
Security and access policy rules	Rule 42 set out policy content requirements. Rule 44 required a copy to be provided within 7 days of a request. Rule 43 dealt with user account management.	Rules 42 and 44 are replaced by Rules 21 and 43. The 7 day request obligation is now Rule 44. Core purpose and content requirements remain the same.	*No action.* Update any internal documents that cite the old rule numbers.	**Same**	No direct equivalent. This is a rule renumbering only.
Policy submission on request	Organisation must provide a copy of their policy within 7 days of a request from the System Operator (Rule 44).	Same 7 day obligation retained under Rule 44. New organisations must also attest a policy is in place at time of registration.	*No action for existing homes.* New registrants must confirm their policy exists upfront.	**Same**	No direct equivalent. This is a System Operator reporting obligation specific to MHR.
Consumer controls	Residents could set access codes, view access history, and configure notifications.	No change. All resident-facing functionality continues unchanged.	*No action.* Nothing to communicate to residents or families about how they use their My Health Record.	**Same**	No direct equivalent, though it supports the resident choice and control principles under Standard 1.

Steps for existing registered residential aged care homes

▶ **Deadline: 1 October 2026**

Action steps

The changes that need action, and where each one fits in your existing Quality Standards systems. The comparison table below covers every change, including those needing no action.

Step 1: Update your security and access policy

▶ Add a MHR data breach response process

TIES INTO: Outcomes 2.4 & 2.5: risk management & incident management

Policy must now specifically document the processes your home will use to ensure it does not contravene s.74 (unauthorised collection, use or disclosure) or s.75 (data breach notification) of the MHR Act. This means naming who is responsible, what steps they take, and when the System Operator is notified.

▶ Update user authorisation procedures

TIES INTO: Outcome 2.9: workforce, role-based access

Add the processes for creating and modifying user accounts, not just suspending and deactivating them. Include what happens when an individual healthcare provider ceases to be linked to your home. This must now cover the full lifecycle of a user account. Confirm that you review your account management practices at least annually.

▶ Expand security measures section

TIES INTO: Outcome 2.7: information management system

Add cybersecurity, encryption, regular back-up, system maintenance, and monitoring and review measures. Physical and information security alone is no longer sufficient.

▶ Size exemption: check if this applies

If your policy previously excluded any sections on the basis of limited size, those sections must now be included. The size exemption has been removed. Standalone and single-site homes are not exempt. If your organisation operates multiple homes, confirm the policy applies to each one.

Step 2: Training

▶ Train all staff accessing MHR before 1 October 2026

TIES INTO: Outcome 2.9: workforce training & competency

Due to the change in legislation, training is required by all staff accessing MHR before the transition period end date of 1 October 2026. Keep this record for 5 years. MHR Recommended Training: https://www.digitalhealth.gov.au/sites/default/files/documents/my-health-record-recommended-training-list.pdf

Step 3: Check your audit log and access record settings

▶ Check that your systems retain audit logs and access records

TIES INTO: Outcome 2.7: information management system

Rule 45 requires records of creating, modifying, suspending and deactivating user accounts to be kept for 5 years, and gives logs of individual access to the MHR system as an example of a record to keep. The Rules do not state plainly which retention period applies to access logs, so set your systems to the longer 5 year period unless your vendor or the Agency advises otherwise. This may require a configuration change in your clinical or care management software (for example, systems such as iCareHealth, Leecare, StorePoint or Autumn Care). To be completed by your nominated Responsible Officer or Organisation Maintenance Officer.

Step 4: Record keeping: what to retain and for how long

Authorising access: retain 5 years. ALREADY EXISTS

Every time you create, change, suspend or deactivate a staff member's MHR access, keep a record of that. This is already part of your Outcome 2.9 access records; just confirm it's kept for the full 5 years. **Ties into: Outcome 2.9**

Training: retain 5 years. ALREADY EXISTS

Keep a record of all training provided to staff before first access, annually, and following significant changes. This is already part of your Outcome 2.9 training records; just confirm MHR is tracked within it and kept for the full 5 years. **Ties into: Outcome 2.9**

Processes for not contravening s.74 or s.75: retain 2 years. ADD

Keep records showing you applied the processes in your policy for not contravening s.74 (unauthorised collection, use or disclosure) or s.75 (data breach notification), including evidence of documented processes and any action taken on a breach. This record only exists once your Step 1 process is in place. Rule 45(1)(c) and 45(3). **Ties into: Outcome 2.7**

Security measures: retain 2 years. ALREADY EXISTS

Keep records showing how your home has implemented physical security, information security, cybersecurity, and technical and organisational measures. This is already covered by your Outcome 2.7 security evidence; just confirm it addresses MHR specifically. **Ties into: Outcome 2.7**

Each version of the policy: retain 5 years. ALREADY EXISTS

Every time your policy is updated, keep a copy for at least 5 years from the date it came into effect. This is already part of your Outcome 2.7 document control; just confirm the 5 year minimum is applied. **Ties into: Outcome 2.7**

Advance care planning: retain no time period specified. ADD

Your home may upload advance care planning information only if the resident instructs it to (Rule 41(1)). Where you do, keep a record of the resident's instructions and how those instructions were provided (Rule 41(2)). **Ties into: Outcomes 3.1 & 5.7**