My Health Records Rules: 2016 vs 2026

A summary of key changes and actions for registered organisations.

Registered before 1 April 2026	**Registering from 1 April 2026**
Update your security and access policy by 1 October 2026 in line with the 2026 Rules.	Develop your security and access policy in accordance with the 2026 Rules from the outset.

Area	2016 Rule	2026 Rules	Action for your organisation	Status
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.	Rule 21(2)(c) requires the policy to document the processes the organisation 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.	**Action required** Add processes covering both s.74 and s.75. Name who is responsible, what steps they take, and when the System Operator is notified. A generic organisational breach policy is not sufficient.	New
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 software applies to audit logs and access records. Set to 5 years to be safe, since user account records are explicitly 5 years. This may require a configuration change.	New
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** 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.	Updated
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 other retention obligations before disposing of anything.	Updated
Size exemption	Small organisations could self-select out of certain policy	Size exemption removed. All organisations regardless of size must	**Action required (small orgs)**	Updated

Area	2016 Rule	2026 Rules	Action for your organisation	Status
	requirements if judged not applicable due to limited size.	meet the same baseline requirements. This requirement now applies to every registered HPI-O, including small or single-site locations within a multi-site practice, with no size-based exemption.	If your policy previously excluded any sections on the basis of size, those sections must now be included. Sole traders are not exempt. If your practice has multiple HPI-Os (e.g. network organisations under a seed org), confirm the policy applies to each one.	
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 organisation. Confirm you review your account management practices annually.	**Updated**
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**
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 patients.*	**Updated**
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. Use your next scheduled annual review to incorporate all 2026 Rule updates by 1 October 2026.	**Updated**
Security and access policy rules	Rule 42 set out policy content requirements. Rule 44 required a copy to be provided within 7 days	Rules 42 and 44 are replaced by Rules 21 and 43. The 7 day request obligation is now Rule 44. Core	*No action. Update any internal documents that cite the old rule numbers.*	**Same**

Area	2016 Rule	2026 Rules	Action for your organisation	Status
	of a request. Rule 43 dealt with user account management.	purpose and content requirements remain the same.		
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 organisations. New registrants must confirm their policy exists upfront.*	**Same**
Consumer controls	Healthcare recipients could set access codes, view access history, and configure notifications.	No change. All consumer facing functionality continues unchanged.	*No action. Nothing to communicate to patients about how they use their MHR.*	**Same**

Steps for existing registered MHR practices

- **Deadline: 1 October 2026**

Step 1: Update your security and access policy

▶ Add a MHR data breach response process

Policy must now specifically document the processes your organisation 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

Add the processes for creating and modifying user accounts, not just suspending and deactivating them. Include what happens when a healthcare provider ceases to be linked to your organisation. This must now cover the full lifecycle of a user account.

▶ Expand security measures section

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 organisational size, those sections must now be included. The size exemption has been removed. Sole traders are not exempt. If your practice has multiple HPI-Os, check each one, small sites are no longer exempt.

Step 2: Training

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

Step 3: Check your audit log and access record settings

Check that your systems retain audit logs and access records for at least 5 years. Rule 45 sets user account records at 5 years and does not state a period for access logs, so 5 years covers both. This may require a configuration change in your clinical or practice management software. To be completed by your nominated Responsible Officer or Organisation Maintenance Officer.

For Best Practice Software (Bp Premier):

https://kb.bestpracticesoftware.com/bppremier/spectra/Integrations/MyHealthRecord/ViewingMyHealthAuditTrail.htm

- Go to View > Patients (or press F10)
- Select View > Health Identifier Audit Trail
- Set the Operation field to Consumer SearchIHI: shows all lookups performed by all users in the practice
- Filter by date as needed

Note: this audit trail records Healthcare Identifier lookups sent to the HI Service. Confirm with your vendor which log records staff access to a patient's My Health Record, and how long it is retained.

For other software, contact your vendor to confirm audit log retention settings.

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

Authorising access: **retain 5 years** Every time you create, change, suspend or deactivate a staff member's My Health Record access, you must keep a record of that.

Training: **retain 5 years** Keep a record of all training provided to staff before first access, annually, and following significant changes to legislation or the system.

Processes for not contravening s.74 or s.75: retain 2 years 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. Rule 45(1)(c) and 45(3).
Security measures: retain 2 years Keep records showing how your practice has implemented physical security, information security, cybersecurity, and technical and organisational measures.
Each version of the policy: retain 5 years Every time your policy is updated, keep a copy of that version for 5 years from the date it came into effect.
Advance care planning: no time period specified (new) Your practice may upload advance care planning information only if the patient instructs it to (Rule 41(1)). Where you do, keep a record of the patient's instructions and how those instructions were provided (Rule 41(2)).