Australian Government
Department of Health, Disability and Ageing

My Health Records legislative instruments

Frequently Asked Questions

Contents

About My Health Record

The My Health Record (MHR) system is a secure national digital health record that stores key health information such as medicines, allergies, test results, and hospital summaries in one place. It helps healthcare providers access important information quickly, supporting safer and more coordinated care. Individuals can also view their own MHR, set privacy controls, and choose what information is shared. The MHR system is operated by the Australian Digital Health Agency (System Operator) and is designed to provide access to key health information when it is needed, particularly in an emergency or when seeing a new healthcare provider.

Background to the review The *My Health Records Regulation 2012* and *My Health Records Rule 2016* made under the *My Health Records Act 2012* (Cth) (MHR Act), were due to sunset on 1 April 2026 in accordance with the *Legislation Act 2003* (Cth). A review and a public consultation undertaken in 2025 confirmed that the regulatory framework remains appropriate; however, minor amendments were recommended to modernise the Regulations and Rules, improve clarity, and address technical matters to support the ongoing operation of the MHR system.

This Frequently Asked Questions (FAQ) document provides a high-level overview of the remade My Health Records Rules and Regulations, focusing on key changes arising from the recent review and consultation process. The review was limited to remaking existing instruments due to sunsetting requirements and making targeted updates to improve clarity, consistency and operational effectiveness; it did not revisit the underlying policy settings of the My Health Record framework or propose substantive changes to the *My Health Records Act 2012*. Matters raised during consultation that fell outside the scope of the review, such as broader policy reform or future system enhancements have been noted but were not progressed through

these instruments. Further detail on consultation feedback and how it was considered is available in the Consultation Summary.

This FAQ aims to help stakeholders understand the nature of the updates and what, if anything, they may need to do in response.

Summary of changes

The My Health Record (MHR) regulatory framework has been updated to ensure the system remains contemporary, clear and aligned with modern digital health practices. Key elements of earlier rules have been consolidated into a single instrument, while outdated or unnecessary provisions have been removed to support a simpler and more streamlined regulatory structure.

These updates deliver necessary technical adjustments, improve clarity across the Regulations and Rules, and strengthen alignment with the *My Health Records Act 2012* and broader digital health legislation. The new *My Health Records Regulations 2026* incorporate targeted updates to definitions, governance references and the application of state and territory privacy provisions. The *My Health Records Rules 2026* modernise and clarify operational requirements, including security, access, recordkeeping and registration obligations, while improving readability and supporting practical implementation across the sector.

Importantly, the changes do not alter the purpose of the MHR system, reduce privacy or security protections, or change how consumers or providers interact with My Health Record. Strong safeguards remain in place, and existing consumer-facing functionality continues unchanged.

These updates support ongoing system reliability, simplify regulatory expectations, and help providers and system users more easily locate and apply requirements. The changes commenced on 1 April 2026, with revised security, access and recordkeeping requirements applying from 1 October 2026 for existing participants, to allow organisations sufficient time to adjust.

My Health Records Regulations 2026

1. Why were some definitions updated in the new MHR Regulations?

The MHR system relies on the national Healthcare Identifiers Framework, governed by the *Healthcare Identifiers Act 2010* (HID Act). To ensure consistency across digital health legislation, key definitions used in the HID Act have been incorporated into the new Regulation. This avoids duplication, supports modern drafting practice, and ensures consistent interpretation across

related legislation. The 2012 Regulation previously reproduced a number of definitions from the Healthcare Identifiers Regulations.

2. Why were governance references updated?

The 2012 Regulation referenced the Australian Health Ministers' Advisory Council (AHMAC) as a relevant subcommittee of the Ministerial Council. The head of power enabling this provision was later removed from the MHR Act, meaning the provision no longer has legal effect. The new Regulation removes this outdated reference to reflect the current legislative framework.

3. What changes were made to the preserved State and Territory privacy provisions?

The new Regulations update the list of preserved privacy provisions to reflect amendments made by States and Territories since the preserved provisions were agreed and included in the 2012 Regulations. Some provisions previously preserved have since been repealed in their local jurisdictions, and the updated Regulations align with these changes.

4. What do the preserved privacy provisions do?

Preserved privacy provisions act as an exception to the MHR Act's standard settings which allow information to be shared to an individual's My Health Record, unless the individual has expressly requested that the information not be shared. While the MHR Act generally allows information to be uploaded unless a person directs that specific information not be shared, the preserved provisions require the application of local laws, which require explicit consent from the individual before certain information can be uploaded.

5. Why weren't the remaining preserved privacy provisions removed?

As part of work to implement the Share by Default program, the Department consulted with states and territories on the possible removal of the remaining preserved provisions. Several jurisdictions indicated that their provisions remained appropriate and should continue to be preserved. As a result, the preserved privacy provisions remain in place. The Department continues to work with jurisdictions toward a nationally consistent approach to what information may be uploaded to the MHR. Any future changes would be considered through inter-jurisdictional processes and communicated with appropriate lead time.

My Health Records Rules 2026

6. What's actually changed?

Several provisions of the MHR Rules have been updated to make them clearer, more modern and easier to apply. The changes focus on simplifying concepts that are no longer needed,

removing outdated language, and aligning the rules with how the MHR system operates today. Many provisions were originally written for a very early version of the MHR system. The revisions support more modern security practices and give the System Operator flexibility to introduce new capabilities as technology and healthcare needs evolve. Importantly, these updates do not change how people use MHR day-to-day, and there is no reduction in privacy protections or consumer controls. The Rules are now more technology-neutral, avoiding prescription of specific mechanisms so the system can adopt contemporary safeguards without legislative amendment.

7. Why were the Rules updated?

The rules were written more than a decade ago, and while they were amended over time, some provisions were no longer suitable for supporting the MHR system over the next decade. Technology, cyber security, clinical workflows, and digital health policy have all changed significantly, and the rules need to evolve as well. The updates remove elements that are outdated or unused, which makes the rules significantly easier for healthcare providers, vendors, and consumers to understand. They also modernise security and data-retention settings, so they align with contemporary government information-management practices. Overall, the updates ensure the legislative framework remains "fit for purpose" as the MHR system grows and adapts. The new rules reflect a renewal and modernisation, not a change in policy intent or system direction. The intent is clarity and currency, not the introduction of new obligations beyond those necessary to maintain security and operational integrity.

8. Why were some definitions updated in the new MHR Rules?

Removal of outdated, prescriptive or redundant definitions

A substantial number of 2016 definitions have been removed because they were either:

- no longer required due to changes in system architecture,
- already defined in the *My Health Records Act 2012* or the *Healthcare Identifiers Act 2010* (HID Act), or
- operational matters that do not need to be prescribed in subordinate legislation.

Removed definitions include:

- *access control mechanisms*, *advanced access controls*, *default access controls*
- *access flag*, *record code*, *document code* - These are no longer prescribed forms of access control. This supports technology-neutral drafting and will enable use of

contemporary identity, authentication and authorisation approaches (e.g. MFA, modern IAM, role-based access)

- *operator*, *portal operator*, *repository operator*, *provider portal*
- *intermediate system roles*: *identified healthcare provider*, *national registration authority*, *network organisation* (definitions now derived directly from the HID Act)
- *effectively remove*, *restore*, *taking control*, *verified healthcare identifier* - These operational concepts are now addressed directly within their relevant operative provisions rather than defined separately.

Simplification or modernisation of existing terms

Some key definitions have been streamlined to make them clearer and more aligned with current digital health practice:

- *access list* now references a specific operative provision (paragraph 9(2)(b)), simplifying the definition.
- *advance care planning information* reflects language in the Privacy Act, to provide broadly for inclusion of documents stating a healthcare recipient's expressed wishes.
- *healthcare recipient-entered health summary* modernised to *healthcare recipient-entered personal health summary* with clearer wording.
- *material change*, *network*, *organisation maintenance officer*, *professional representative*, *linked* - these have been clarified or aligned with definitions in the HID Act.

Continued reliance on Act-based definitions

Several definitions are unchanged because they continue to rely on definitions in the *My Health Records Act 2012* or the *Healthcare Identifiers Act 2010*:

- *Act*, *healthcare identifier*, *seed organisation*, *service operator*

New or expanded definitions

The 2026 rules introduce new definitions to reflect the contemporary system design:

- *opt-out model*: now explicitly defined, and reflecting that the provision for national application of the opt-out model has now been incorporated into the MHR Rules, rather than a stand-alone instrument.
- *support service*: adopts meaning from the HID Act.
- Additional cross-references updated to reflect the 2026 rule structure.

9. What happened to access flags?

Reference to the concept of access flags has been removed from the new Rules. This does not remove the concept entirely from the MHR system; access flags will continue to exist as a technical variable within MHR and may be used internally to manage inherited permissions across seed and network organisation structures. The change reflects that having them defined in legislation adds unnecessary complexity without changing behaviours in practice, as to date access flags have not been implemented in a way that was meaningfully different from how seed and network structures already manage access. Removal of the concept will allow for more flexible and technology-neutral implementation of controls.

For users, nothing changes. Healthcare recipients continue to retain strong, meaningful privacy controls, including access codes, the ability to see their access history, and configurable notification settings. Removing reference to access flags in the rules simply removes an outdated legislative reference. This approach is consistent with the broader shift away from prescribing specific technical implementations in rules. Existing settings will continue, but the rules will now support other options for managing access in future.

10. Are access codes still available?

Yes. Access codes remain a core privacy mechanism in MHR and continue to operate as they always have. The updated rules provide greater scope for the System Operator to introduce more modern or flexible privacy features over time without being constrained by older, prescriptive drafting. This means the system can evolve as new technology or user needs emerge, while still preserving the underlying function and purpose of access codes. While current access-code functionality will continue upon commencement of the new rules, user-facing access-code features will continue to be supported unless or until supplemented or replaced by other options for managing access.

11. Have privacy protections changed?

No. The privacy framework governing MHR remains the same or stronger than before. The changes focus on improving clarity by simplifying wording, removing duplication, and updating references that no longer reflect modern practice. The strengthened guidance around security and operations ensures that privacy protections will continue to improve as the MHR system evolves. Consumers retain full control over who can see their information, including the ability to set access controls, track access events, and restrict or remove documents at any time. These changes neither broaden who can access information nor reduce consumer control; they make the existing framework easier to understand and apply.

12. What's changed about consumer notifications?

Consumers can choose to be notified in relation to certain situations where their My Health Record is accessed by a healthcare provider organisation or a nominated representative. The Rules provide for the minimum options that must be made available by the System Operator. Additional options for consumers may be offered above the minimum requirements provided for in the Rules.

Previously, there was uncertainty as to the application of the requirement to permit a healthcare recipient to be alerted when their My Health Record was accessed by a third party. The updated provision clarifies the minimal notifications that a consumer must be able to elect to receive. These improvements are about clarity and consistency rather than introducing new types of notifications or changing how existing notifications behave in practice. However, the drafting, with provision of a minimum set of notifications that a consumer may select, operates so that the System Operator has flexibility and may offer additional options in future.

13. What is the new security and access policy application record-keeping requirement?

The updated rules specify that certain categories of operational information must now be retained for either two or five years. This requirement brings MHR into alignment with broader Australian Government information-management standards and reflects modern expectations for accountability and auditing. Examples of "operational information" include system audit logs, security events, and support records (not clinical documents)

Under the old rules, there was a requirement for entities to ensure each iteration of their security policy, for the purposes of the MHR requirements, contained a unique version number and the date when each iteration came into effect, and a record of each iteration of the policy was required to be kept in accordance with the record keeping obligations applicable to the entity. Entities were also required to be able to provide a copy of their policy, or a policy in force on a specified date, if requested by the System Operator.

The requirement to provide a copy of the existing or a previous version of a security and access policy is retained in the new Rules. However this is time-limited, providing greater certainty for participants in the MHR system, as the new Rules are clear the obligation to retain copies of a security and access policy is limited to a 5 year period.

The change aligns with key privacy principles and government security, assurance, and integrity frameworks. Retaining operational information for five years supports these objectives while still upholding data-minimisation principles by avoiding unnecessary long-term storage.

Records of the training undertaken in relation to the MHR system, as required to comply with the security and access policy requirements, must also be retained for 5 years under the new Rules.

Records relating to how an entity has applied required security measures, such as management of user access, system maintenance, data protection, encryption and back-up processes, must be retained, and produced on request, for a period of 2 years.

These changes clarify the application of the record-keeping retention requirements for MHR security policy purposes, providing certainty as to the period of retention, by comparison to the ongoing and non-time limited requirements under the previous rules.

Importantly, the change does not affect how long clinical documents remain available in a healthcare recipient's MHR. Further, the rules do not impact any other record-keeping obligations for entities in relation to clinical information.

14. Has security been strengthened?

The rules have been modernised to better reflect current expectations regarding cyber security standards and remove references to outdated technologies and processes. Entities providing healthcare and managing sensitive health information are already subject to a range of obligations, including requirements such as adherence to the Privacy Act and Australian privacy principles. The updates to the rules reflect contemporary expectations regarding the application of physical, information and cyber security, and technical and operational measures, by entities accessing information from or connecting to the My Health Record system. Under the new rules, some entities are required to provide evidence of their security and access policy in the course of applying to register with the MHR system, in addition to the existing requirement to provide this if requested by the System Operator.

The updated rules remove the previous 'limited-size' exemptions, meaning that all system participants regardless of their size, scale, or technical capability must now comply with the same baseline security requirements. Policies and practices to meet the security and access policy requirements in the new Rules may be tailored according the size and nature of service delivery by a particular entity, however an entity cannot simply elect that the obligations are not applicable to them. The intent is to require a minimum standard of protection across the entire MHR ecosystem, addressing gaps in the previous Rules, as smaller organisations had been able to self-select not to comply with some of all of the security policy requirements under the previous rules. The removal of 'limited-size' exemptions ensures consistent expectations and reduces ambiguity about minimum controls.

In addition, specific technologies are no longer prescribed as forms of access control, supporting a technology-neutral framework that will support new approaches and the ability to integrate more contemporary safeguards such as multi-factor authentication and modern identity and access management.

The reforms give the System Operator more flexibility to adopt new security safeguards and access controls as digital health risks evolve, without needing to revise the legislation every time technology changes. These updates reinforce the security of the MHR system and provide clearer guidance on organisational responsibilities.

No existing security requirement has been weakened. The modernised rules strengthen the overall security posture and ensure a more uniform and contemporary approach to protecting health information.

15. Do healthcare providers or healthcare software vendors need to change how they operate?

In most cases, healthcare providers and healthcare software vendors do not need to change anything immediately. The amendments include a six-month grandfathering period to support an orderly transition. Under the transitional arrangements, the relevant sections of 2016 Rule, as in force immediately before 1 April 2026, continue to apply to an entity from 1 April 2026 until immediately before 1 October 2026. This ensures that organisations have sufficient time to understand the changes and update their internal processes, governance documents, and software configurations if required.

The updates reduce unnecessary complexity in the rules and make responsibilities clearer, which should make compliance easier rather than more burdensome. The revised drafting also removes the previous 'limited-size' exemptions, meaning that all entities regardless of organisational size must comply with the same minimum security and governance standards. This provides a more consistent baseline across the MHR ecosystem and closes historical gaps where smaller entities may not comply with all requirements, based on a self-selection approach to determine that some policies were not applicable.

The modernised language aligns more closely with contemporary cyber security practices, clinical software capabilities, Australian privacy principles and current organisational workflows. This reduces the reliance on interpretation and supports a more uniform understanding of what "good practice" looks like.

Any future changes that directly affect providers' or vendors' day-to-day practice, including new solutions that may support more contemporary approaches to the exercise of access controls by consumers, will be communicated and implemented separately and with

appropriate lead time. Stakeholders should continue to monitor communications from the system operator and their clinical software vendors.

16. Does this change how healthcare recipients use their My Health Record?

No. These amendments do not change how healthcare recipients use MHR or access their information. Healthcare recipients can continue to view their MHR, adjust their privacy and access settings, see who has accessed their information, receive notifications, and control what is uploaded. The updates focus on clarity and system modernisation behind the scenes, not on altering consumer functionality. All existing features remain available and continue to operate as they did under the previous rules. If new consumer features are introduced in future, they will be communicated with clear guidance and support.

17. Why are the Assisted Registration Rules not being remade? Does assisted registration still continue?

The Assisted Registration Rules are not being remade because they are no longer required as a standalone legislative instrument. This review confirmed that legal authority to support assisted registration is sufficiently provided through the *My Health Records Act 2012* itself and related arrangements administered by the System Operator. As a result, the absence of provisions on assisted registration in the new Rules does not signal a change in policy or the discontinuation of assisted registration as an option. Assisted registration may continue to be offered in accordance with the Act and operational arrangements.