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The **My Health Records Rule 2016 (the 2016 Rule)** has been replaced by the **My Health Records Rules 2026 (the 2026 Rules)**, which came into effect on **1 April 2026**.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.

Topics	Key Changes
Training (rule 21(2)(b) of the 2026 Rules)	In addition to training authorised users before they access the My Health Record system (already required under rule 42(2)(b) of the 2016 Rule), organisations must now also provide refresher training annually and whenever there are significant changes to the system or governing legislation. The explanatory statement for the 2026 Rules also allows organisations to recognise training completed with another provider where it is considered appropriate and sufficient by the organisation.
Process(es) for ensuring the organisation complies with section 75 of the Act (in relation to management of My Health Record data breaches) (rule 21(2)(c) of the 2026 Rules)	In addition to existing process(es) for ensuring that the organisation complies with section 74 of the *My Health Records Act 2012* in relation to identifying a person who requests access to a healthcare recipient's My Health Record and communicating the person's identity to the System Operator (already required under rule 42(4)(c) of the 2016 Rule), the policy must now outline the process(es) for ensuring the organisation complies with its data breach obligations under section 75 of the Act.
Security measures (rule 21(2)(d) of the 2026 Rules)	In addition to physical and information security measures (including user account management) (required under rule 42(4)(d) of the 2016 Rule), the policy must now also detail cybersecurity, technical and organisational measures (including, data protection, encryption and back-up and regular system maintenance) that are implemented, monitored and reviewed by the organisation.

Rule 43 — Security and access policy—general

Topics	Key Changes
Communicating and making the policy accessible (rule 43(1) of the 2026 Rules)	In addition to communicating and ensuring the policy remains readily accessible to all employees and any healthcare providers to whom the organisation supplies services under contract (required under rule 42(2) of the 2016 Rule), the organisation must now also ensure that the policy is communicated and made readily accessible to any individual healthcare provides linked to the organisation. It is recommended that a statement to this effect is included in the policy.

Topics	Key Changes
Keeping the policy-up-to date (rule 43(3) of the 2026 Rules)	In addition to reviewing the policy at least annually and when any material new or changed risks are identified (required under rule 42(6)(c) of the 2016 Rule), the organisation must now also review the policy on request by the System Operator. It is recommended that a statement to this effect is included in the policy.
Record-keeping (rule 43(4) of the 2026 Rules)	Rather than keeping a record of each iteration of the policy (required under Rule 42(6)(d) of the 2016 Rule) in accordance with the record keeping obligations (if any) applicable to the organisation, the organisation must now ensure that these records are retained for 5 years, starting on the day the iteration comes into effect. It is recommended that a statement to this effect is included in the policy.

Rule 45 — Security and access policy—application record-keeping

In addition to the policy itself, the 2026 Rules introduce new record-keeping requirements whereby organisations must keep records showing how their security and access policy has been applied. It is recommended that the organisation's policy specifically lists the records that will be retained by the organisation as well as the applicable retention period. The below table provides a summary of the topics and the retention periods outlined in Rule 45.

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

For more information on how to establish a My Health Record security and access policy, please refer to Australian Digital Health Agency website: My Health Record participation obligations.