

Policy requirements

There are specific topics that must be covered in your organisation's security and access policy. The topics are set out in Rule 21 of the [My Health Records Rules 2026](#). To learn more about this requirement, please see the topics outlined below.

I employ few or no staff other than myself – Do I need to cover all of the required topics in my security and access policy, even if they don't apply to my organisation?

1. Healthcare provider organisation policies

- A written security and access policy is in place prior to the healthcare provider organisation registering to participate in the system.
- The organisation must comply with the policy and ensure the following people comply with the policy as well: the organisation's employees, linked individual healthcare providers and those to whom the organisation supplies services under contract.
- The policy is communicated with, and remains accessible to, all employees as well as any healthcare providers to whom the organisation supplies services under contract and any individual healthcare providers linked to the organisation.
- For example, a healthcare provider organisation that supplies information technology services to individual healthcare providers to enable them to access the system, must communicate the policy to these providers.

Do I need a policy if staff in my organisation don't use My Health Record or use it infrequently?

2. Manner of authorising and process for suspending and deactivating user accounts

- The policy details the procedures that will be used to authorise a person to access, or use information in the My Health Record system, via or on behalf of the healthcare provider organisation, including creation and modification of user accounts.
- 'Access' refers to both viewing and uploading information to My Health Record. This means organisations that register with My Health Record for the purpose of uploading documents only (but do not intend to view any information in My Health Record) are still required to address this element in their policy and outline how access to

relevant users will be authorised.

- **Uploading Only:**
 - If staff members will only be uploading information to My Health Record and will not be viewing My Health Record information, this should be clearly stated in the policy. The policy should also outline how users will be authorised to upload documents to My Health Record.
 - Where documents are uploaded to My Health Record as part of a bulk upload process, this should be specified in the policy. If all bulk uploads are to take place through a single authorised user, this should be outlined in the policy, in addition to the process for authorising this user.
- **Viewing Only (via the National Provider Portal (NPP)):**
 - The NPP enables healthcare providers to view information in My Health Record. The organisation's RO or OMO/s is responsible for authorising staff who require access to My Health Record and linking or removing individual healthcare providers using Health Professional Online Services (HPOS), as needed. Further information on linking and removing healthcare providers in HPOS is available [here](#).
- **Viewing and Uploading:**
 - If conformant software is used at the organisation which enables both viewing and uploading of information in My Health Record, the policy must outline how the organisation will authorise staff to view and upload information, as well as the individual(s) responsible for granting and managing access (such as the Responsible Officer (RO) or Organisation Maintenance Officer (OMO)).
- The policy outlines the ways a user account will be suspended and/or deactivated in specific circumstances. This includes identifying the person responsible for these actions (e.g. RO or OMO) and setting out the process for immediate action where:
 - A user leaves the organisation
 - A user's security is compromised
 - A user has changed duties and no longer requires access to the system

- A user is an individual healthcare provider that ceases to be linked to the organisation

I don't know how my organisation will access My Health Record yet – do I need to specify this in my security and access policy?

-
-
-

3. Training for authorised users, before they access the system

- The policy includes a requirement that, before a user is authorised to access the system, they receive training covering:
 - how to use the system accurately and responsibly
 - legal obligations of the healthcare provider organisation and individuals using the My Health Record system
 - consequences of breaching those legal obligations.
- The policy includes a requirement that a user will receive training annually and following any significant changes to the My Health Record system or the governing legislation.
- Organisations must maintain records of the training provided to users, such as a register of staff training and/or completion certificates. The organisation must retain training records for 5 years, starting on the day the training record was created.
- View [recommended My Health Record training \(PDF, 133.26 KB\)](#).

4. Process for identifying the individual who accesses a person's record (on each occasion)

- The policy outlines how the organisation will meet its obligations under section 74 of the *My Health Records Act 2012* in relation to identifying the individual who accessed a person's record and communicating the person's identity to the Australian Digital Health Agency (System Operator), where requested.
- Each time an organisation interacts with My Health Record, this activity is logged. Conformant software and the NPP (if used) automatically communicate this information to the System Operator. This includes the user identifier (user ID) of the person accessing My Health Record. An organisation must be able to confirm which person the user ID belongs to and ensure this information is communicated

to the System Operator, if requested. This process should be detailed in the security and access policy.

- For example, an organisation could:
 - check the user ID of the person who accessed My Health Record at a particular time (by checking the transaction log, or referring to details included in the request from the System Operator)
 - confirm who the relevant user ID is assigned to
 - have a process where the organisation's Responsible Officer (RO) or Organisation Maintenance Officer (OMO) provides the user's identity to the System Operator when requested to do so.
- All relevant processes (whether automated or manual) should be outlined in your policy.

5. Process for ensuring compliance with My Health Record data breach obligations

- The policy outlines how the organisation will meet its obligations under section 75 of the *My Health Records Act 2012* with regard to managing My Health Record data breaches.
- Under the *My Health Records Act 2012*, a data breach involves:
 - unauthorised collection, use or disclosure of health information in an individual's My Health Record has or may have occurred; or
 - an event has or may have occurred, or any circumstances have or may have arisen, that compromise, have compromised or may have compromised, the security or integrity of the My Health Record system.
- The policy also outlines how the organisation will notify the Australian Digital Health Agency (System Operator) and, where relevant, the Office of the Australian Information Commissioner (OAIC) of the breach, contain the breach and mitigate future breaches. Refer to [data breach notification obligations](#) for more information.

6. Physical security, information security, cybersecurity, and technical and organisational measures, including user account management processes

The policy details the physical security, information security, cybersecurity, and technical and organisational measures that are in place to mitigate information security risks and prevent unauthorised access, **including**:

- The **user account management practices** for information technology systems that are used by users to access the My Health Record system via or on behalf of the organisation, such as:
 - Restricting access to those persons who require access as part of their duties
 - Uniquely identifying individuals using the healthcare provider organisation's information technology systems
 - Having that unique identity protected by a password or equivalent protection mechanism
 - Ensuring password and/or other access mechanisms are [sufficiently secure and robust](#) to mitigate the security and privacy risks associated with unauthorised access to the system
 - Disabling the user accounts of persons no longer authorised to access the system
 - Suspending a user account as soon as practicable after becoming aware that the account or its password or access mechanism has been compromised.
 - Ensuring that practices are reviewed at least annually
 - Ensuring that users are aware of, and trained in, the above practices.
- The **regular system maintenance** that will be carried out by the organisation such as installing software updates and security patches in a timely manner and checking systems for errors, vulnerabilities or unusual behaviour.
- The **data protection**, including data encryption and regular back-up measures implemented by the organisation.
- The **regular monitoring and review** of the above security measures carried out by the organisation.
- **Technical** and **organisational measures** may complement each other and can overlap. They may also encompass existing controls, including physical security, information security, and cybersecurity measures.

What is a physical security measure?

What is an information security measure?

What is a cybersecurity measure?

What are technical and organisational measures?

7. Strategies for identifying, responding to, and reporting system-related security risks

- The policy describes the strategies used by the healthcare provider organisation to ensure the system-related security risks can be:
 - promptly identified
 - acted upon
 - reported to the healthcare provider organisation's management.
- To assist with monitoring use of the system, audit logs should record the user identity, date and time of access, whose record was accessed and the type of information that was accessed. Conducting regular checks of My Health Record audit logs for any unusual access or unauthorised behaviour will ensure risks are promptly identified and mitigated.

Policy implementation and maintenance

- The My Health Record security and access policy must be reviewed annually (at a minimum), when any material new or changed risks are identified (such as a change within the system, organisation, or regulation; or factors that might result in unauthorised access, use or disclosure of information in a record), and when requested by the System Operator.
- The policy must include a unique version number and date of effect.
- A copy of each version of the policy must be retained by the organisation for 5 years starting on the day the iteration comes into effect.

Note: The Agency or the Office of the Australian Information Commissioner (OAIC) may request a current or previous version of your organisation's security and access policy at any time. Where a healthcare provider organisation receives a request from the Agency, the legislation specifies that a copy of the policy must be provided within 7 days.