Australian Government
Australian Digital Health Agency

My Health Record

My Health Record security and access policy checklist

This checklist supports healthcare organisations to establish a My Health Record security and access policy

Healthcare organisations must operate in accordance with relevant policies and legislation when participating in the My Health Record system. They must establish, review, update, maintain, enforce and promote policies that ensure the system is used safely and responsibly by staff.
Prior to registering to participate in the system, your organisation will need to have a My Health Record security and access policy in place. Once registered, you will also need to comply with a number of ongoing participation obligations, including keeping your security and access policy up to date.
To assist organisations with meeting security and access policy requirements, the Australian Digital Health Agency has developed a security and access policy checklist.

Policy Requirements Checklist

The checklist is a guide only and should be assessed against the needs and risks that may apply to your organisation.
Healthcare provider organisations need to ensure the policy includes and addresses the topics outlined in Rule 42 of the My Health Records Rule as outlined below.

1. Healthcare provider organisation policies

☐	A written My Health Record security and access policy is in place prior to the healthcare provider organisation registering to participate in the system, and the policy is maintained on an ongoing basis.
☐	The policy is communicated and remains accessible to all employees.
☐	The policy is communicated with any healthcare providers to whom the organisation supplies services under contract and remains accessible to these providers. 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.
☐	The policy is enforced in relation to all employees and any healthcare providers to whom the organisation supplies services under contract.

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

☐	The policy details the manner of authorising persons accessing the system via or on behalf of the healthcare provider organisation.
☐	The policy outlines the ways a user account is suspended and/or deactivated in the following circumstances: ○ A user leaves the organisation ○ A user's security is compromised ○ A user has changed duties and no longer requires access to the system

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 people who access the system on behalf of the organisation ○ Consequences of breaching those obligations

☐	You may wish to refer to the Agency's recommended training list to support your organisation in meeting this legislative requirement.
☐	It is recommended that organisations maintain a register of staff training.

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

☐	The policy outlines the process for identifying a person who requests access to a healthcare recipient's record and communicating the person's identity to the My Health Record System Operator (Australian Digital Health Agency). Generally, this would occur via clinical information systems used, where: ○ the clinical software is used to assign and record unique internal staff member identification codes, including a Healthcare Provider Identifier-Individual (HPI-I); and ○ the unique identification code, or the provider's HPI-I, is recorded by the clinical software and automatically provided to the System Operator for each instance of system access. Where the National Provider Portal is being used to access the My Health Record system, it is recommended that organisations maintain a register of authorised users containing their name and HPI-I. This list can be accessed via HPOS.
	Note: The System Operator may request information regarding an organisation's access to the My Health Record system. See the legislative obligations for communicating to the System Operator under Section 74 of the My Health Records Act.

5. Physical and Information Security Measures, including user account management processes

☐	The policy details the physical and information security measures that are in place to mitigate information security risks and prevent unauthorised access.
☐	People accessing the system via or on behalf of the healthcare provider organisation understand and adhere to the physical and information security measures.
☐	The healthcare provider organisation employs reasonable user account management practices, including: ○ 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.
	Note: See the Australian Digital Health Agency's cyber security resources for more information. Additional guidance is provided in the Guide to Securing Personal Information and the Guide to Health Privacy on the Office of the Australian Information Commissioner website.

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

☐	The policy describes the mitigation 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.
☐	This should include processes for identifying and reporting: ○ unauthorised access to the system ○ any matters that may compromise the security or integrity of the system, for example, a security incident, such as ransomware, that has affected a healthcare provider organisation.
☐	Organisations should ensure processes are in place to comply with data breach notification obligations outlined in section 75 of the My Health Records Act. Learn more about how to manage a data breach here.
☐	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.

7. Assisted Registration (if offered)

☐	Where the healthcare provider offers assisted registration, this topic is required within the policy. If the organisation does not offer assisted registration, it is recommended that this is noted in the policy. Assisted registration is where a healthcare provider assists healthcare recipients to register for a record.
☐	The policy needs to outline the methods for: ○ Authorising employees of the organisation to provide assisted registration ○ Providing training before a person is authorised to provide assisted registration ○ Confirming a healthcare recipient's consent to be registered ○ Identifying a healthcare recipient for the purposes of assisted registration, including the process and criteria that must apply
	Note: See the legislative requirements for confirming a healthcare recipient's consent under Rule 9 of the My Health Records (Assisted Registration) Rule.

8. Policy implementation and maintenance

☐	The My Health Record security and access policy must be reviewed annually (at a minimum) and 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).
☐	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.
	Note: The Agency or the Office of the Australian Information Commissioner may request a current or previous version of your organisation's security and access policy at any time. The legislation specifies that a healthcare provider organisation must comply with a request to provide a copy of the policy within 7 days of receiving the request.

More information

The Office of the Australian Information Commissioner (OAIC) provides Rule 42 guidance outlining points for healthcare provider organisations to consider when developing their My Health Record security and access policy. A My Health Record security and access policy template has also been developed by the OAIC, in collaboration with the Australian Digital Health Agency, to assist you in developing a policy for your organisation.

- Guidance and policy template

You may also wish to complete the Australian Digital Health Agency's "Developing a My Health Record security and access policy for your organisation" e-Learning module for an overview of the practical steps that should be followed when developing a security and access policy.

General guidance is also available from the OAIC to help you protect health information.