My Health Record system security and access policy template

## Background

This My Health Record system security and access policy template provides guidance for healthcare provider organisations on meeting the requirements set out in Rule 42 of the [*My Health Records Rule 2016*](https://www.legislation.gov.au/Series/F2016L00095).

Under Rule 42, healthcare provider organisations must establish a security and access policy prior to registering with the My Health Record system. The policy must be communicated to all employees and any healthcare providers to whom the organisation supplies services under contract. The policy must be enforced in relation to all employees and healthcare providers to whom the organisation supplies services under contract. Healthcare provider organisations must also ensure that the policy is kept up to date by reviewing it, at least annually, as well as when any material new or changed risks are identified.

The policy must cover the following matters:

* the manner of authorising people to access the My Health Record system, and deactivating or suspending access
* training that will be provided to employees before they access the My Health Record system
* the process for identifying a person who requests access to a healthcare recipient’s My Health Record and communicating the person’s identity to the System Operator[[1]](#footnote-1)
* physical and information security measures that will be established and adhered to by the healthcare provider organisation and people accessing the My Health Record system
* mechanisms for the prompt identification and mitigation of My Health Record system-related security risks
* where the healthcare provider organisation provides assisted registration, information about the authorisation of employees, training, confirmation of consent and process and criteria for identifying a healthcare recipient for that purpose.

If, in the reasonable opinion of a healthcare provider organisation, any of the above matters do not apply to the organisation due to the limited size of the organisation, the organisation’s security and access policy need not address that requirement. The policy should include a statement justifying the absence of such a matter(s).

Examples provided in this template are suggestions only. If a suggested example is not applicable it is the responsibility of the healthcare provider organisation to meet the mandatory requirements by providing alternative detail in their policy.

If an organisation is part of a wider ‘network hierarchy’ under the responsibility of a Seed Organisation consider whether a separate security and access policy is required for the Network Organisation.[[2]](#footnote-2)

The policy underpins the security and access governance for end-users of the My Health Record system and is therefore critical to ensure sensitive information is protected. It also reinforces staff awareness of their obligations under My Health Record legislation.

In addition to the requirements in Rule 42, healthcare provider organisations have privacy obligations set out in the Australian Privacy Principles (APPs) under the [*Privacy Act 1988*](https://www.legislation.gov.au/Series/C2004A03712). Healthcare provider organisations must take reasonable steps to comply with APPs 1.2 (open and transparent management of personal information) and 11 (security of personal information).[[3]](#footnote-3)

Use of this template does not guarantee compliance with Rule 42 and is intended for use as a guide of a general nature only. Persons using this template should seek appropriate legal or other professional advice as required.

The Office of the Australian Information Commissioner (OAIC) may commence regulatory action in the event that an organisation is found to be non-compliant with their Rule 42 obligations under [*My Health Records Rule 2016*](https://www.legislation.gov.au/Series/F2016L00095).

### Glossary

Please refer to the Australian Digital Health Agency’s website for a [glossary of terms](https://www.digitalhealth.gov.au/support/glossary) contained in this template.

# [Organisation name]**[[4]](#footnote-4)**

# My Health Record system security and access policy

## Key information

|  |  |
| --- | --- |
| **Policy owner** | [Organisation name, branch/team responsible] |
| Contact details  | [Email][Phone] |
| **Responsible officer (RO)** | [Responsible officer's name, position]  |
| Contact details | [Email][Phone] |
| **Organisation maintenance officer[s] (OMO)[[5]](#footnote-5)** | [Organisation maintenance officer's name(s), position(s)]  |
| Contact details | [Email(s)][Phone number(s)] |
| **Version no.****Date of last review** | [Document version no.][Date of last review] This is also the date the current version of this security and access policy came into effect. |
| **Date of next review** | [Date of next review] This policy will be reviewed at least annually as well as when any material new or changed risks are identified. |
| **Other relevant documents** | [List other relevant documents and policies such as: * privacy policy
* policy and procedure manual
* data breach response plan
* training register]
 |

### Document version history

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Release comments | File location |
|  |  | Approved by [name] and released via [e.g., email, intranet, hard copy] |  |
|  |  |  |  |
|  |  |  |  |

## Communicate and enforce the security and access policy

This security and access policy applies to all employees who access the My Health Record system on behalf of [organisation name]. For the purposes of this policy, ‘employees’ include contractors and volunteers.[[6]](#footnote-6)

[Organisation name] uses [e.g. conformant clinical software (such as a clinical information system(s), practice management system(s) or dispensary system(s))[[7]](#footnote-7), the National Provider Portal, a combination of conformant clinical software and the National Provider Portal, the Healthcare Information Provider System (HIPS), or HIPS mobile] to access the My Health Record system.

This security and access policy is enforceable and is communicated to all employees by [e.g., communicating the policy in employee training and inductions].

This security and access policy can be accessed via [e.g., intranet, hard copies provided, or regular reminder emails to employees attaching policy].

### Provision of services to healthcare providers under contract

[Organisation name] **Choose an item.** supplies services to healthcare providers under contract,[[8]](#footnote-8) including [list the healthcare providers to which the organisation supplies services under contract].

**If organisation does supply services to healthcare providers:**

This security and access policy is communicated to these healthcare providers by [e.g., by communicating the policy in training and inductions].

This security and access policy can be accessed via [e.g., intranet, hard copies provided, or regular reminder emails attaching policy].

This security and access policy is also enforced in relation to these healthcare providers by [describe how the policy is enforced, e.g., contract requiring healthcare providers to comply with the policy].

## Authorising, suspending and deactivating access

[Organisation name] authorises individuals to access the My Health Record system on behalf of the organisation by:

* [outline the organisation’s process for authorising access to the My Health Record system, including how access is limited to those who need it for their duties]

**Example (non-exhaustive) list**:

* requiring employees to complete training and sign a user agreement before accessing the My Health Record system
* providing staff with unique log in details that can be used to access the My Health Record system
* setting and maintaining access levels for all employees who require access to the My Health Record system
* keeping a register of authorised users and access levels.

When an authorised individual leaves the organisation or they no longer require access to the My Health Record system, **Choose an item.** suspends or deactivates their user account by:

* [outline steps taken (including updating ICT systems), employee responsible, and timeframes for suspension/deactivation]

**Example (non-exhaustive) list**:

* deactivating the authorised user account and Healthcare Provider Identifier – Individual (HPI-I) of the authorised user in the clinical software as soon as practical, within [specify timeframe]
* removing the link between the organisation and the provider entry in the Health Professional Online Services (HPOS) as soon as practical, within [specify timeframe]
* revising the register of authorised users as soon as practical, within [specify timeframe].

If the security and access of an authorised user account has been compromised, **Choose an item.** suspends or deactivates their user account by:

* [outline steps taken (including updating ICT systems), employee(s) responsible, and timeframes for suspension/deactivation]

**Example (non-exhaustive) list**:

* deactivating their local account as soon as practical, within [specify timeframe] upon becoming aware of the security breach
* deactivating the user account in the clinical software as soon as practical, within [specify timeframe] and issuing a new login
* revising the register of authorised users as soon as practical, within [specify timeframe].

## Training

[Organisation name] provides training to individuals before they are authorised to access the My Health Record system. Training will be organised by **Choose an item.**, and will cover:

* how to use the My Health Record system accurately and responsibly
* legal obligations on organisations and individuals using the My Health Record system
* consequences of breaching those legal obligations.

**Optional**: additional training details

[Enter further details regarding training, including key information covered by training, training provider, whether the training is online or face to face, external resources (if applicable)[[9]](#footnote-9), frequency of training, and training register maintained by the organisation.]

## Identification of users

In order to identify individual users who access the My Health Record system [organisation name] has put in place the following process:

* [Outline the organisation’s process for identifying individual users]

**Example (non-exhaustive) list**:

* unique identifier is assigned to users by the clinical software
* clinical software records the user’s **Choose an item.** each time they access the My Health Record system, including the user identity, date and time of access, whose My Health Record was accessed and the type of information that was accessed
* maintaining a register of authorised users containing their **Choose an item.**.

The above processes allow **Choose an item.** to communicate the user’s identity to the System Operator when required.[[10]](#footnote-10)

## Physical and information security measures

[Organisation name] implements physical and information security measures to control access to the My Health Record system,[[11]](#footnote-11) including:

* [List the organisation’s relevant physical and information security measures with reference to the requirements in Rule 44]

**Example (non-exhaustive) list**:

* maintaining a register of authorised users containing their **Choose an item.**
* employee must use their individual login and passphrase to access the My Health Record system
* employees are required to change their passphrase every **Choose an item.**
* employee passphrases must be at least **Choose an item.** characters and contain a combination of upper-case and lower-case letters, numbers, and symbols
* employees are locked out of their accounts after **Choose an item.** failed login attempts
* employees access the My Health Record system on their desktop computers and must unlock their computers by **Choose an item.**
* automatically locking computers and mobile devices left inactive after **Choose an item.** minutes
* devices used to access the My Health Record system are located in secure areas under appropriate surveillance
* devices used to access the My Health Record system are fitted with privacy screens where appropriate
* devices are positioned such that screens cannot be viewed by unauthorised persons.

### Remote access

**Option 1**:

[Organisation name] **does** have remote access functionality to access the My Health Record system.[[12]](#footnote-12)

Remote access to the My Health Record system is enabled via **Choose an item.**

When accessing the My Health Record system, employees unlock their devices by **Choose an item.**.

**Option 2:**

[Organisation name] **does not** have remote access functionality to access the My Health Record system.

## Mitigation strategies

[Organisation name] implements mitigation strategies to ensure that My Health Record system-related privacy and security risks are promptly identified, mitigated and reported to management, including:

* [List the organisation’s mitigation strategies]

**Example (non-exhaustive) list**:

* incident response management process
* patient complaints process
* data breach response plan
* review of relevant internal polices every **Choose an item.**
* conducting relevant risk assessments every **Choose an item.**
	+ record and maintenance of audit logs:
	+ the clinical software records [**information recorded by the audit log**] when a My Health Record is accessed
	+ audit logs are reviewed every **Choose an item.** to identify potential privacy and security risks
	+ audit logs are retained for **[retention period]**.

[Organisation name] has a process for identifying and responding to security or privacy issues, or breaches of the My Health Record system.[[13]](#footnote-13) This includes:

* [Describe the organisation’s process identifying and responding to security or privacy issues, or breaches of the My Health Record system].

**Example (non-exhaustive) list**:

* reporting the issue or breach to **Choose an item.**
* **Choose an item.** responds by:
	+ keeping detailed records of and assessing the issue or breach
	+ containing the issue or breach by [describe actions taken to contain breach]
	+ reporting the issue or breach to the System Operator and the Information Commissioner
* recording actual or suspected breaches into an incident log containing [**information recorded by in the incident log**]

**Optional:** further detail on data breach management is contained in the data breach response plan.[[14]](#footnote-14)

**Optional**: patient complaints process

Patient complaints relating to unauthorised access to their My Health Record are handled:

* [In accordance with the organisation’s complaints policy or describe the organisation’s complaints handling procedure]

Where the patient complaint cannot be managed via the organisation’s complaints handling procedure, [organisation name] may advise patients to contact the My Health Record Helpline (1800 723 471) or the OAIC.

## Assisted Registration

**Option 1**:

[Organisation name] does not provide assisted registration.

[If an organisation does not provide assisted registration individuals who wish to register for a My Health Record can also access assistance via the Agency website, telephone line, Medicare offices.]

**Option 2:**

[Organisation name] authorises employees to provide assisted registration by:

* [outline the organisation’s process for authorising employees to provide assisted registration]

[Organisation name] provides training to individuals before a person is authorised to provide assisted registration. The training covers:

* [list key information covered]

[Organisation name] confirms the relevant healthcare recipient’s consent to be registered for the purposes of rule 9 of the *My Health Records (Assisted Registration) Rule 2015* through the following process:

* [outline the organisation’s process for confirming the relevant healthcare recipient’s consent]

[Organisation name] identifies the relevant healthcare recipient for the purposes of assisted registration through the following processes and criteria:

* [outline the organisation’s process and criteria for identifying the relevant healthcare recipient for the purposes of assisted registration]
1. This will enable the healthcare provider organisation to meet their obligations under s 74 of the [*My Health Records Act 2012*](https://www.legislation.gov.au/Series/C2012A00063). [↑](#footnote-ref-1)
2. For more information on network hierarchy, seed organisation and network organisation see [Registering your healthcare provider organisation to use the Healthcare Identifiers (HI) Service - Healthcare Identifiers (HI) Service for health professionals - Services Australia](https://www.servicesaustralia.gov.au/registering-your-healthcare-provider-organisation-to-use-healthcare-identifiers-hi-service). [↑](#footnote-ref-2)
3. More information on the APPs is available in the OAIC’s [Australian Privacy Principles guidelines](https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines) and [Guide to health privacy](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-health-privacy). Guidance on how to meet your ongoing compliance obligations under Australian Privacy Principles (APPs) 1.2 and 11 is available at the OAIC’s [Privacy management framework](https://www.oaic.gov.au/privacy/guidance-and-advice/privacy-management-framework-enabling-compliance-and-encouraging-good-practice) and [Guide to securing personal information](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information), respectively. [↑](#footnote-ref-3)
4. The name of your organisation, consistent with your registration for the Healthcare Identifiers Service and the My Health Record system. [↑](#footnote-ref-4)
5. Rule 27 of the [*My Health Records Rule 2016*](https://www.legislation.gov.au/Series/F2016L00095) provides that healthcare provider organisations must ensure that their organisation maintenance officers (OMOs) establish and maintain with the System Operator an accurate and up-to-date list of all identified healthcare providers who are individuals who are authorised to access the My Health Record system via or on behalf of the organisation using the provider portal. [↑](#footnote-ref-5)
6. ‘Employee’ is defined in section 5 of the [*My Health Records Act 2012*](https://www.legislation.gov.au/Series/C2012A00063). [↑](#footnote-ref-6)
7. Where a conformant clinical software is used to access the My Health Record system, please provide the name of the system(s) used. [↑](#footnote-ref-7)
8. Healthcare provider organisations must communicate and enforce the security and access policy to any healthcare providers to whom the organisation supplies services under contract. For example, if a healthcare provider shares its premises, reception and IT systems with other healthcare providers under contract, including providing access to the My Health Record system, it must communicate, and enforce this policy to those other healthcare providers. [↑](#footnote-ref-8)
9. Resources and support for training and education relating to My Health Record is available on the [Digital Health online learning portal](https://training.digitalhealth.gov.au/). [↑](#footnote-ref-9)
10. This process relates to your organisation’s obligation to ensure certain information is given to the System Operator under section 74 of the [*My Health Records Act 2012*](https://www.legislation.gov.au/Series/C2012A00063). If your organisation is unable to provide sufficient information, it may be liable for a civil penalty under that legislation. [↑](#footnote-ref-10)
11. See the Australian Digital Health Agency’s [Establishing policies checklist](https://www.digitalhealth.gov.au/healthcare-providers/initiatives-and-programs/my-health-record#register-and-set-up-access) and the OAIC’s [Guide to securing personal information](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information) for more resources on information security measures. Some mitigation strategies (such as audit logs) may also be considered information security measures. [↑](#footnote-ref-11)
12. Although an organisation may not use the My Health Record system remotely, it is possible that their systems are able to be accessed remotely without authorisation. Organisations should review their systems to check whether remote access is enabled and secure devices using access processes such as unique logins or multifactor authentication. [↑](#footnote-ref-12)
13. Organisations must report potential or actual contraventions involving unauthorised collection, use or disclosure of health information, and events or circumstances that may compromise the security of the My Health Record system to the OAIC and the System Operator under section 75 of the [*My Health Records Act 2012*](https://www.legislation.gov.au/Details/C2019C00337). Please note that the data breach notification scheme under s 75 is distinct from the broader Notification Data Breaches (NDB) scheme under the [*Privacy Act 1988*](https://www.legislation.gov.au/Series/C2004A03712)*.* [↑](#footnote-ref-13)
14. More information about notifiable data breaches under the [*My Health Records Act 2012*](https://www.legislation.gov.au/Series/C2012A00063)and how to report a potential breach can be found in the OAIC’s [video](https://www.oaic.gov.au/privacy/guidance-and-advice/my-health-record/?a=3516), [flow chart](https://www.oaic.gov.au/privacy/guidance-and-advice/my-health-record/?a=752) and [Guide to mandatory data breach notification in the My Health Record system](https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-mandatory-data-breach-notification-in-the-my-health-record-system). [↑](#footnote-ref-14)