Australian Government

Office of the Australian Information Commissioner

My Health Record system security and access policy template

18 September 2026

OAIC

Contents

Introduction

Managing access to My Health Record within healthcare provider organisations is essential to protecting the security and privacy of patients' health information. Healthcare organisations are responsible for ensuring that only authorised staff members can access a patient's record, and only when it is necessary to support the delivery of healthcare. Effective access management reduces the risk of unauthorised collection, use or disclosure of sensitive information, helping organisations meet their legal, regulatory, and professional obligations while maintaining patient trust in the healthcare system and digital healthcare services, including My Health Record.

Strong access controls also strengthen the overall security of My Health Record by limiting use to appropriate roles and responsibilities within an organisation. By regularly reviewing user permissions, promptly removing them when staff change roles or leave, and monitoring record activity, healthcare provider organisations can reduce the risk of privacy breaches, cyber threats, and human error. These measures help safeguard the confidentiality, integrity, and availability of health information, ensuring it remains protected while being available to authorised clinicians when needed to provide safe and effective care.

Purpose

The My Health Record system security and access policy template provides guidance for healthcare provider organisations that intend to register, and remain eligible for registration with, the My Health Record system on meeting the requirements set out in rule 21, rule 43 and rule 45 of the My Health Records Rules 2026 (the Rules).

Rule 21

Under rule 21 of the Rules, healthcare provider organisations must establish a security and access policy prior to registering with the My Health Record system. The policy must cover the following matters:

- the procedures used for authorising people (users) to access or use My Health Record information via or on behalf of the organisation, including procedures for creating and modifying user accounts, and deactivating or suspending user accounts
- training that will be provided to users before they are authorised to access the My Health Record system, annually and following relevant regulatory or system changes
- the process(es) that the organisation will use to ensure that it complies with section 74 of the My Health Records Act 2012 (the Act), such as 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
- the process(es) that the organisation will use to ensure that the organisation complies with section 75 of the Act, which requires healthcare providers, as soon as practicable, to contain

potential and actual My Health Record data breaches[1] , assess any risks associated with the breach and notify the System Operator and/or Office of the Australian Information Commissioner (OAIC) of the potential or actual breach

- physical security, information security, cybersecurity and technical and organisational measures that will be implemented, monitored and reviewed by the organisation and people accessing the My Health Record system
- strategies for ensuring My Health Record system-related security risks are promptly identified, acted upon and reported to the organisation's management.

Rule 43

Under rule 43 of the Rules, healthcare provider organisations must:

- communicate the policy to all employees, any healthcare providers to whom the organisation supplies services under contract, and individual healthcare providers that are linked to the organisation
- take all reasonable steps to ensure that the above individuals comply with the policy, and
- ensure that the policy is kept up to date by reviewing it, at least annually, when any material new or changed risks are identified and on request by the System Operator.

Rule 45

Rule 45 of the Rules requires healthcare provider organisations to keep records showing how the organisation has implemented each of the matters that must be addressed in the policy.[2] This includes records demonstrating:

- how user accounts are managed
- training records
- process(es) for identifying users
- process(es) for managing My Health Record data breaches, and
- records of applying physical security, information security, cyber security, technical and operational measures.

The retention period for these documents varies. Generally, organisations will meet their record-keeping requirements by retaining documents for 5 years, although the Rules permit certain documents to be retained for 2 years.

---

[1] A My Health Record data breaches include any contravention of the *My Health Records Act 2012* in a manner involving an unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record, or any event or circumstances that have or may have occurred, or that compromise, may compromise, has compromised or may have compromised the security or integrity of the My Health Record system, in which the organisation is involved.

[2] See rule 45 of the Rules.

The Office of the Australian Information Commissioner (OAIC) may commence regulatory action if an organisation is found to be non-compliant with their rule 21, rule 43 or rule 45 obligations.

Privacy obligations under the *Privacy Act 1988*

In addition to the requirements in rule 21 and rule 43, most healthcare provider organisations have privacy obligations set out in the Australian Privacy Principles (APPs) under the *Privacy Act 1988*.[3] In particular, 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).[4]

How to use this policy template

The following features can be found throughout this policy template:

Red text should be updated by the organisation

Where drop-down lists are provided, the organisation should select the appropriate option for their circumstances

Text boxes shaded in yellow are optional and should only be included by organisations to which they are applicable. Please ensure that any optional information that is not applicable is removed from the policy prior to finalisation

Examples are provided in the grey boxes throughout each section and are suggestions only. Examples that do not apply should be deleted, and additional organisation-specific examples should be added where appropriate.

Text boxes shaded in blue contain explanatory notes to assist organisations to complete each section. Please ensure that any explanatory notes are removed from the policy prior to finalisation

[3] The Privacy Act generally applies to all organisations that provide a health service, including an organisation that is a small business. Further information, including in relation to the definition of 'health service' can be found here.

[4] More information on the APPs is available in the OAIC's Australian Privacy Principles guidelines and 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 and Guide to securing personal information, respectively.

It is important that your security and access policy is appropriately tailored to the circumstances of your organisation. This applies to all organisation types, including those that may have only a small number of staff accessing My Health Record (such as sole traders that do not employ staff) or that do not view information within My Health Record (such as pathology or diagnostic imaging organisations that upload but do not view patient results). Specific examples are provided for these organisation types throughout the policy, where the way such organisations interact with My Health Record may differ from other organisation types.

Additional guidance notes are provided in orange boxes throughout the policy template and should be deleted prior to finalisation of the policy.

Use of this template does not guarantee compliance with rule 21, rule 43 and rule 45 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.

Glossary

Term	Meaning
Employee	An individual who provides services for the entity under a contract for services or an individual whose services are made available to the entity (including services made available free of charge) (e.g. volunteers) (section 5 of the *My Health Records Act 2012*)
Healthcare Provider Identifier – Individual (HPI-I)	A unique identifier assigned to an individual healthcare provider through the Healthcare Identifiers Service. The HPI-I uniquely identifies a healthcare provider in digital health systems.
Healthcare Provider Identifier – Organisation (HPI-O)	A unique identifier assigned to a healthcare provider organisation through the Healthcare Identifiers Service. The HPI-O identifies the organisation and can be linked to individual healthcare providers for access to digital health services such as My Health Record.
Healthcare Provider Organisation	An entity, or part of an entity, that conducts, has conducted, or will conduct an enterprise that provides healthcare, including healthcare provided free of charges (section 5 of the *My Health Records Act 2012*)
Health Professional Online Services (HPOS)	Services Australia's secure online portal that enables healthcare organisations and healthcare providers to manage Healthcare Identifiers Service details and access a range of digital health services.
Linked Individual Healthcare Providers	(in addition to employees) includes any individual to whom the organisation provides services or facilities, to facilitate the provision of healthcare by the individual healthcare provider (section 5 of the *Healthcare Identifiers Act 2010*)
Network Organisation	A healthcare provider organisation that is linked to a Seed Organisation within a Healthcare Identifiers Service network

Term	Meaning
	hierarchy. A Network Organisation may rely on the Seed Organisation for certain administrative functions.
Organisation Maintenance Officer (OMO)	A person appointed by a healthcare provider organisation to assist with maintaining organisation details and managing access arrangements within the Healthcare Identifiers Service. An organisation may have 1 or more OMOs.
Responsible Officer (RO)	The person nominated by a healthcare provider organisation to act as the primary authority for the organisation in the Healthcare Identifiers Service. The RO is responsible for authorising and maintaining the organisation's participation in national digital health systems, including My Health Record. The RO may also act as the OMO.
Seed Organisation	The principal healthcare provider organisation in a Healthcare Identifiers Service network hierarchy. The Seed Organisation is responsible for managing the network and may establish and maintain links with Network Organisations.
System Operator	The entity responsible for the operation of the My Health Record system. Under the *My Health Records Regulations 2026*, the Australian Digital Health Agency is prescribed as the System Operator.

Organisation Name[5]

My Health Record system security and access policy

Key Information

Policy owner	[Organisation name, branch/team responsible]
Contact details	[Email] [Phone]
Organisation name(s) as registered with the HI Service	[Organisation name(s)]
Trade name(s) (if different to the above)	[Trade name(s)]
HPIO number(s)	[HPIO number(s)]
Responsible officer (RO)	[Responsible officer's name, position]
Contact details	[Email] [Phone]
Organisation maintenance officer[s] (OMO)	[Organisation maintenance officer's name(s), position(s)]
Contact details	[Email(s)] [Phone number(s)]
Version no.	[Document version no.]
Date of last review	[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 or on request of the System Operator.
Other relevant documents	[List other relevant organisation documents and policies e.g. privacy policy, data breach response plan, training register)

[5] The name of your organisation, consistent with your registration for the Healthcare Identifiers Service and the My Health Record system.

Document version history

Version	Name	Changes	Date
V1.0	*1 October 2026*	*Approved by [name] and released via [e.g., email, intranet, hard copy]*	*H:\Example*

Scope[6]

This policy applies to all organisations listed in the 'Key Information' section of this policy, above.

[Organisation name] uses [e.g. conformant clinical software (insert name of clinical software)) [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 allows authorised users to [upload to / view information within / both upload to and view information within] My Health Record, [both on and offsite / onsite only].

Where the organisation has enabled offsite access to My Health Record:

[Where access occurs offsite, the security and access requirements set out in this policy also apply.]

Communicating and enforcing

This security and access policy applies to, and is enforceable against, all employees who use the above system(s) to access the My Health Record system on behalf of the organisation(s) listed above. For the purposes of this policy, 'employees' include contractors and volunteers.

Optional: This policy is also applicable to all healthcare providers to whom [Organisation name] provides service under contract, [8] as well as all other individual healthcare providers linked to the organisation.

This includes [list the healthcare providers to which the organisation supplies services under contract, or healthcare providers who are linked to the organisation e.g. organisations with shared premises or

[6] If an organisation is part of a wider 'network hierarchy' under the responsibility of a Seed Organisation, the network organisation may be covered by the Seed Organisation's policy provided that the policy makes specific reference to the network organisation and is appropriately tailored to the network organisation's circumstances. If this is not the case, the network organisation should develop its own security and access policy. 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.

[7] Where conformant clinical software is used to access the My Health Record system, please provide the name of the system(s) used. Conformant clinical software includes clinical information system(s), practice management system(s) or dispensary system(s).

[8] For example, if a healthcare provider shares its premises, reception or 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.

IT systems, visiting medical officers, sessional healthcare providers, locum or Agency healthcare providers, student placements].

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 provider to comply with the policy].

This security and access policy is communicated to all [list relevant healthcare provider engagement types e.g. employees, healthcare providers to whom the organisation provides services under contract, and linked individual healthcare providers] by [e.g., by communicating the policy in training and inductions]. A copy of the policy can also be accessed via [e.g., intranet, hard copies provided, or regular reminder emails to employees attaching policy].

Managing user access

[Organisation name] authorises individuals to access or use information in the My Health Record system via or 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].

Examples (non-exhaustive) list:

- requiring users to complete training and sign a user agreement before accessing the My Health Record system.
- keeping a register of authorised users and access levels.
- keeping a register of role descriptions and access profiles, mapping job functions to authorised system access.
- *single member companies / sole traders that do not employ staff:* by authorising their own access in their capacity as the Responsible Officer for the organisation, where access is required for the performance of their duties.
- *organisations that only upload to My Health Record:* keeping a register of authorised users that outlines which roles are authorised to upload different document types and, where appropriate or necessary, sets out separate authorisations for viewing My Health Record information OR stating that all documents will be uploaded to My Health Record via a bulk upload process which occurs from a sole user account with appropriate access permissions.

Creating and modifying user accounts

Once a user is authorised to access the My Health Record system **Choose an item.**, will create a user account by:

- [outline the organisation's process for creating user accounts with access to the My Health Record system].

Examples (non-exhaustive) list:

- obtaining approval for creating a user account.
- creating the user account/raising a request for creation of the user account in [system name] following completion of mandatory onboarding training.
- providing staff with unique login details that can be used to access the My Health Record system.
- linking the organisation's Healthcare Provider Identifier – Organisation (HPI-O) number to the individual's Healthcare Provider Identifier – Individual (HPI-I) number in Health Professional Online Services (HPOS).
- revising the register of authorised users within [specify timeframe].

When an authorised individual's access to the My Health Record system needs to be modified, [Organisation name] will modify a user account by:

- [outline the organisation's process for modifying user accounts with access to the My Health Record system][9].

Examples (non-exhaustive) list:

- modifying the user account/raising a request in [system name] to modify the user account in the organisation's Information Technology team, within [specify timeframe].
- updating the register of authorised users and associated roles/access levels, within [specify timeframe].

Suspending and deactivating user accounts

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 IT systems), employee responsible, and timeframes for suspension/deactivation].

Examples (non-exhaustive) list:

- deactivating the user account in the organisation's clinical software, within [specify timeframe].
- removing the link between the organisation's HPI-O number and the individual's HPI-I in HPOS, within [specify timeframe].
- revising the register of authorised users, 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 IT systems), employee(s) responsible, and timeframes for suspension/deactivation].

Examples (non-exhaustive) list:

- deactivating the user account in the organisation's clinical software, within [specify timeframe].
- removing the link between the organisation's HPI-O number and the individual's HPI-I in HPOS within [specify timeframe].
- revising the register of authorised users within [specify timeframe].

[9] A user account may need to be modified, as opposed to suspended or deactivated, where the user's authorisation, role or access level has changed but some level of access to My Health Record is still required.

Training

My Health Record training will be undertaken by [e.g. all individuals who are required to [upload to / access] My Health Record as part of their duties / name of sole trader that does not employ staff] at the following frequencies:[10]

- before [e.g. he / she / they] are authorised to access the My Health Record system; and,
- annually; and,
- following significant change to My Health Records legislation or the My Health Record system.

Training will be organised by **Choose an item.**, and will cover[11]:

- 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, recognition of prior learning, external resources (if applicable).] (Note: Resources and support for training and education relating to My Health Record, including for specific organisation types, is available on the Digital Health online learning portal.)

Note:

Where a user completes training with another healthcare provider organisation, this may be sufficient to meet the training requirements. Your organisation would need to determine whether training undertaken with another organisation is appropriate and sufficient and keep relevant records as evidence that the relevant training requirements have been met. If your organisation chooses to recognise prior learning from another organisation, this section can be adapted to reference this process.

[10] Note that the training frequency set out in this policy is the minimum training required by legislation. Organisations are encouraged to assess their organisation's training needs and implement additional training requirements where necessary.

[11] Wherever possible, training should be tailored to the organisation's circumstances and incorporate content specific to the type of healthcare provider organisation. A recommended My Health Record Training fact sheet has been developed to support organisations to meet the requirements of the Rules. Refer to: Recommended My Health Record Training .

Identification of users

[Organisation name] has a process in place to ensure it does not contravene section 74[12] of the *My Health Records Act 2012.* This process allows [Organisation name] to identify individual users who access patient My Health Records via or on behalf of the organisation. Specifically, individual users are identified by:

- [Outline the organisation's process for identifying individual users].

Examples (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, Individual Healthcare Identifier (IHI) of the patient whose My Health Record was accessed and the type of information that was accessed.
- a register of authorised users is maintained containing the user's **Choose an item.**.
- *single member companies / sole traders that do not employ staff:* the organisation's software records the user ID of the sole practitioner working at the organisation, and who can be easily identified as the only person accessing the My Health Record system on behalf of the organisation.
- *organisations that only upload to My Health Record:* the organisation's software records the user ID of the person performing the upload, including in situations where uploads occur via a bulk upload process.

[12] 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*. If your organisation is unable to provide sufficient information to identify the individual using/accessing the My Health Record system, it may be liable for a civil penalty under that legislation.

Data Breaches

[Organisation name] has a process in place to ensure it complies with section 75[13] of the *My Health Records Act 2012.* This process ensures that [organisation name] notifies **Choose an item.**[14] after it becomes aware that the breach has, or may have, occurred (regardless of whether the data breach has been confirmed).[15]

It is the role of **Choose an item.** to:

Examples (non-exhaustive) list:

- identify and assess all actual or potential My Health Record data breaches
- take steps to contain the breach and take further steps to mitigate any risks that are related to or arise from the breach or a potential breach
- notify the System Operator and, where relevant, the OAIC as soon as practicable after becoming aware
- where necessary[16], request that the System Operator notify any affected healthcare recipients if applicable

Identification of a data breach

[Organisation name] monitors My Health Record activity to identify potential or actual data breaches by:

- [outline the organisation's process for monitoring My Health Record system activity, including authorised access and cyber risks]

Examples (non-exhaustive) list:

- periodic review of clinical information system audit logs.
- reviewing software alerts and cybersecurity notifications.

---

[13] This process relates to your organisation's obligations to manage data breaches section 75 of the *My Health Records Act 2012*. If your organisation fails to notify the system operator or the information commissioner of a potential or actual data breach, it may be liable for a civil penalty under that legislation. More information can be found on the OAIC website: Guide to mandatory data breach notification in the My Health Record system

[14] My Health Record data breach notification requirements depend on the type of entity: state or territory authority healthcare providers must report breaches to the System Operator only, while non-government (private) healthcare providers must report breaches to both the System Operator and the Information Commissioner.

[15] More information about notifiable data breaches under the *My Health Records Act 2012*, including steps that should be taken once a breach has been identified and how to report a potential breach can be found in the OAIC's video, flow chart and Guide to mandatory data breach notification in the My Health Record system.

[16] A reporting entity must ask the System Operator to notify any affected healthcare recipients where they become aware of either a confirmed notifiable data breach, or a likely data breach that may have serious effects on at least 1 healthcare recipient.

- incident management processes for staff reporting of self-identified potential or actual data breaches.
- *single member companies / sole traders that do not employ staff:* reviewing audit logs, access records, software alerts, cybersecurity notifications and any complaints or enquiries relating to My Health Record access. As [organisation name] does not employ staff, these monitoring activities are undertaken directly by [name].
- *organisations that only upload to My Health Record:* reviewing audit logs, upload records and system-generated alerts relating to the upload of information to My Health Record.

Containment and risk evaluation following a data breach

Following the identification of an actual or potential data breach **Choose an item.** will take steps to contain the breach to limit further unauthorised access or impact. This may include:

Examples (non-exhaustive) list:

- revoking or changing computer access privileges.
- changing passwords and other authentication credentials.
- addressing weaknesses in physical or electronic security, e.g. disabling any remote access.
- stopping the unauthorised practice or shutting down the repository or portal that was breached, if it does not result in the loss of evidence.

Following initial containment, **Choose an item.** will conduct an initial risk assessment which will consider:

Examples (non-exhaustive) list:

- the nature, extent and cause of the breach.
- whether the effects of the breach may be serious for any healthcare recipients (in instances of both potential and actual data breaches).
- other harms, including to the entity that suffered the breach.

Notification of a data breach

Choose an item. will notify Choose an item. of a data breach that has or may have occurred as soon as practicable after becoming aware of the event or circumstances.

If following the completion of the risk assessment it is determined that either of the following has occurred, **Choose an item.** will ask the System Operator to notify all affected healthcare recipients:

- a data breach has occurred, or
- a data breach is reasonably likely to have occurred, and the effects of the event or circumstances might be serious for at least 1 healthcare recipient.

Notification will be made utilising the following mechanisms:

Examples (non-exhaustive) list:

- the OAIC My Health Record Data Breach form
- the Australian Digital Health Agency Data Breach Webform
- the Australian Digital Health Agency Data Breach PDF notification form
- In the event of total system outage, contact the My Health Record Helpline – 1800 723 471 followed by an electronic notification as soon as practicable.

Security Measures

Note:

To be compliant with rule 21(2)(d), please ensure you include at least one of each of the following kinds of security measure: Physical security, information security, cybersecurity, technical and organisational[17] measures. If your organisation engages an external IT service provider, you should liaise directly with that provider to document the relevant security measures and record-keeping requirements applicable to the services they deliver.

[Organisation name] implements physical security, information security, cybersecurity, technical and organisational measures to control access to the My Health Record system,[18] including:

- [List the organisation's relevant physical security, information security, cybersecurity, technical and organisational measures with reference to the user account management requirements set out in rule 21(4)].[19]

Examples (non-exhaustive) list:

- employees must use their individual login and passphrase to access the My Health Record system.
- passphrases must be changed every **Choose an item.** and must be at least **Choose an item.** characters, including a combination of upper-case and lower-case letters, numbers, and symbols.
- automatically locking computers and mobile devices left inactive after **Choose an item.** minutes.
- employees complete cybersecurity awareness training including identifying and reporting phishing attacks and suspicious activity.
- devices used to access the My Health Record system are in secure areas under appropriate surveillance.
- devices are positioned such that screens cannot be viewed by unauthorised persons and are fitted with privacy screens where necessary.

---

[17] The 2024 legislative reforms to the *Privacy Act 1988* introduced APP 11.3, which clarifies that the reasonable steps an organisation must take to protect personal information include both technical and organisational measures. The purpose of this addition is to provide further guidance and clarification for entities in meeting their obligations.

Technical and organisational measures may complement each other and can overlap. They may also encompass existing controls that already meet the requirements set out in rule 21(2)(d) of the Rules, including physical security, information security, and cybersecurity measures. For further guidance on the application of APP 11, refer to the OAIC website: Chapter 11: APP 11 Security of personal information | OAIC

[18] See the Australian Digital Health Agency's participation obligations and the OAIC's Guide to securing personal information for more resources on information security and cybersecurity measures. Some mitigation strategies (such as audit logs) may also be considered information security measures.

[19] Where controls are managed by external providers or vendors, organisations should identify those controls and describe the arrangements in place to ensure they are implemented and maintained appropriately.

- anti-malware and endpoint protection controls are implemented to detect, block and contain malicious software.
- encryption is applied to devices and systems storing health information.
- a schedule is maintained for ongoing regular system maintenance.
- controls are implemented to prevent unauthorised input of My Health Record data into AI systems[20].
- risk assessments are completed prior to the deployment of software updates and subsequent risks to the My Health Record system are monitored.
- policies for access, use and disclosure of My Health Record system data are maintained.
- procedures to identify, contain, manage, escalate and report cyber security incidents are maintained.

[Organisation name] will monitor and review the effectiveness of these measures, including an annual review of user account management practices by:

- [Outline the organisation's process and frequency for monitoring and reviewing the effectiveness of these measures].

Examples (non-exhaustive) list:

- conducting reviews of controls to confirm they remain effective and aligned with current risks and compliance obligations.
- reviewing and updating policies, procedures and risk assessments following any security incident, identified vulnerability, or material change to systems or operations.
- implementing remediation actions arising from audits, reviews and incident investigations, with oversight by senior management.
- undertaking an annual review of user account management practices, including verifying user identities, confirming appropriate access levels, reviewing account activity, and removing or modifying access for users who no longer require it.

[20] For further information on the use of AI in health care refer to the Australian Commission on Safety and Quality in Healthcare – AI Clinical Use Guide

Managing security risks

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

- [List the organisation's strategies].

Examples (non-exhaustive) list:

- patient identification procedures prior to opening.
- patient complaints process.
- data breach response plan.
- review of relevant internal polices every **Choose an item.**.
- conducting relevant risk assessments every **Choose an item.**.
- periodic review of audit logs.
- *single member companies / sole traders that do not employ staff:* maintaining and reviewing audit logs and system activity records, following patient identification procedures before accessing or uploading information, maintaining patient complaint and data breach management processes, and undertaking periodic reviews of relevant policies and procedures. With regard to reporting incidents to the organisation's management, as [insert name] is also responsible for the management of the organisation, identified privacy and security risks, incidents, audit findings, complaints and corrective actions are recorded and reviewed by [insert name] to ensure appropriate action is taken and ongoing compliance obligations are met
- *organisations that only upload to My Health Record:* As [organisation name] only uploads to My health Record, the organisation's strategies for ensuring My Health Record system-related privacy and security risks are promptly identified, acted upon and reported to management are focused on the secure handling, preparation and transmission of information uploaded to the My Health Record system. This includes maintaining incident response and data breach response processes, reviewing upload activity, maintaining a process for receiving and investigating complaints, and conducting periodic risk assessments of systems, software and processes used to upload information to My Health Record.

[Organisation name] has a process for identifying and responding to security or privacy issues, or breaches of the My Health Record system.[21] This includes:

- [Describe the organisation's process identifying and responding to security or privacy issues].

Examples (non-exhaustive) list:

[21] 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*. 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.*

- reporting the issues to **Choose an item.**.
- **Choose an item.** responds by:
  - keeping detailed records of and assessing the issue or breach.
  - following the data breach containment and notification measures outlined in the 'Data Breaches' section of this policy, above.
- recording actual or suspected breaches into an incident log containing [information recorded by in the incident log]

OPTIONAL FOR ORGANISATIONS THAT PROVIDE ASSISTED REGISTRATION

Assisted Registration[22]

Note:

It is no longer a requirement of the Rules that assisted registration is to be addressed in an organisation's security and access policy. However, if your organisation provides Assisted Registration, the below information can be included in your organisation's security and access policy or other policy documents within your organisation. Delete this section if your organisation does not provide Assisted Registration

[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 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]

[22] Organisations that are connected to the My Health Record system can help their patients who don't already have a My Health Record to register for one. This is referred to as Assisted Registration. Refer to: Help your patients to register

Record keeping

Choose an item. will keep each iteration of this policy for 5 years starting the day the iteration comes into effect. The document will be stored [identify where the document will be stored e.g. shared drive, policy software program, SharePoint, archived storage requiring IT access].

To evidence implementation of the security and access controls outlined in this policy, **Choose an item.** will also keep the following records for **5 years** starting the day the record was created:

User account management records

Examples (non-exhaustive) list:

- register of authorised user accounts and access levels (including the date on which accounts were created, modified, suspended or deactivated and the reason)
- register of role descriptions and access profiles, mapping job function to authorised system access
- audit logs from the clinical software of user account creation, modification and deactivation

Training records

Examples (non-exhaustive) list:

- training materials
- training register documenting training completed, date of completion, and evidence of successful completion or acknowledgement
- attendance records for train-the-trainer led sessions
- training completion certificates.

In addition, **Choose an item.** will keep the following records for **2 years** starting the day the record was created:

User identification records

Examples (non-exhaustive) list:

- audit logs detailing instances of My Health Record system access
- register of authorised user accounts and access levels
- documentation in the organisation's local clinical information system identifying the date(s) on which the patient's My Health Record were accessed, by whom, and the reason for the access.

Data breach management records

Examples (non-exhaustive) list:

- incident reports documenting unauthorised collection, use or disclosure of health information contained in the My Health Record system, or cybersecurity incidents that pose a risk to the security and integrity of the My Health Record system
- copies of preliminary risk assessments following an actual or potential data breach
- copies of notifications sent to the System Operator and the Information Commissioner
- copies of policies and procedures related to reporting and responding to incidents (e.g. data breach management policy).

Records related to security measures

Examples (non-exhaustive) list:

- IT policies stating that employees must change their passphrases at least every 6 months, lock their workstations when not in use, and that privacy screens/appropriate device positioning must be used.
- system logs showing enforcement of account lockout after 5 unsuccessful login attempts and/or automatic device lock settings after 3 minutes of inactivity.
- records of employee completion of cybersecurity awareness training, including phishing and suspicious activity reporting.
- a maintained register of all authorised users, including name, unique identifier, HPI-I and position.
- reports demonstrating operation of filtering controls to mitigate phishing and malicious content including instances of detection and response.
- backup schedules, logs and reports confirming regular backups of business and clinical data.
- documentation confirming encryption is applied to devices and systems storing health information.
- records of scheduled and completed system maintenance activities.
- documentation of risk assessments conducted prior to software updates and records of ongoing risk monitoring.
- current and archived versions of policies covering access, use, disclosure and storage of My Health Record data.