My Health Record Security and Privacy

My Health Record system security

- The Australian Digital Health Agency, as the System Operator, has established **bank strength security** to **protect the system** from cyber attack.

Strong encryption

Firewalls

Secure login / authentication mechanisms
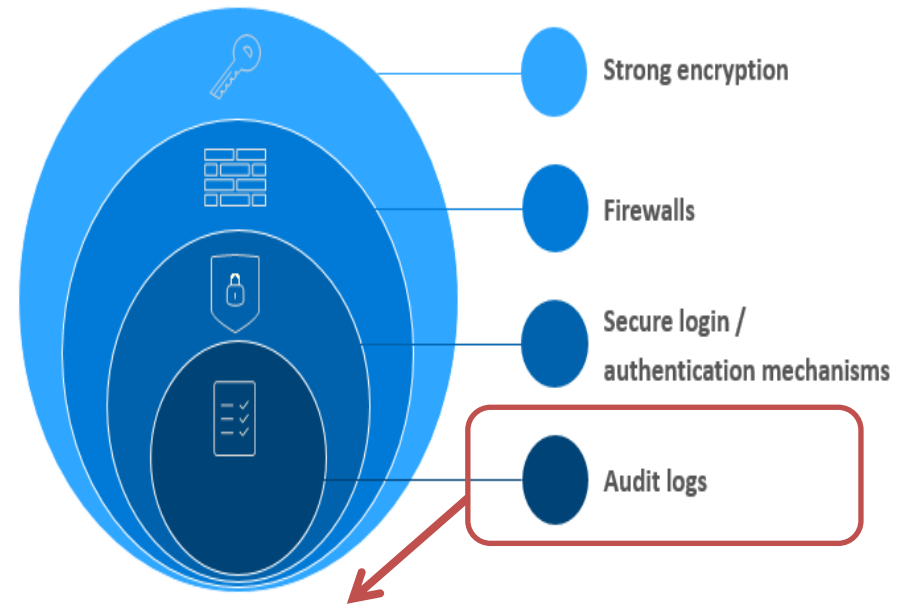
Audit logs

- The audit logs allow an individual to see who has accessed their information (including self and representatives), what they did (including view, upload and 'breakglass') as well as the time and date this occurred.

- After the initial access, a healthcare provider will be added to the consumer's 'Approved Provider List'.

My Health Record - audit log

Access history is recorded, including who accessed the record, when it was accessed and what actions were taken

My Health Record – approved providers list

Access by Healthcare Providers

e.g. GPs, hospitals, dentists, nurses, etc.

All healthcare providers involved in your care can access this record. You can control access to your entire My Health Record by setting a record access code.

Close ⌃

Healthcare providers involved in your care can access your record

Provider can access your record

Provider also has access to Restricted documents

Documents from this provider are uploaded to

Healthcare Provider Access List ⓘ

No Healthcare Provider Organisations have accessed this record yet.

All Other Healthcare Providers

All Healthcare Providers involved in your care can access this record.

Advanced Settings   **Manage Access**

My Health Record privacy obligations

- MHR is protected by the *My Health Record Act 2012* and the *Privacy Act 1988*. There are **penalties for misuse** such as, imprisonment and/or fines.

- When using the MHR, you should manage it the same way you manage personal and health information, i.e. you should take:

  'Reasonable steps to protect information from misuse, interference and loss, as well as unauthorised access, modification or disclosure' - Australian Privacy Principle 11.1 (read more about your MHR privacy obligations)

- You should only access the MHR to assist in your clinical decision-making whilst providing care to the patient.

- The **Digital Health Agency** continually assesses the cyber security risks to the system and **monitors the system** for evidence of **suspicious behaviour**.

Ways you can interact with the access controls

Consumers can…

Withdraw consent for upload of information into My Health Record; a **clinician must comply with the request to override upload**

They can subscribe to SMS or email alerts that report in real time when registered provider organisations access their My Health Record for the first time

Set up a code to restrict access to the whole My Health Record file (**Record Access Code**)*

Choose to restrict access to specific documents in their My Health Record (**Limited Document Access Code**)* OR remove specific documents completely

Clinicians can…

In an emergency, exercise a 'break glass' facility – a notification will be sent to ADHA and the consumer in these instances*

ADHA will…

Monitor all instances of access to My Health Record

Key information

- The system is **secure, private** and **personally-controlled**.

- The same privacy obligations apply for collection, use and disclosure of health information within the My Health Record as with any other health information you already use.

- You should only access the information if you are providing direct care to the individual.

- **If patients have questions about MHR**, you can direct them to detailed online consumer guides or they can phone **1800 723 471** to speak with a dedicated customer service representative.

- Find out more on the My Health Record system's **Privacy Policy** or refer to your local policies and procedures.