



Australian Government

Office of the Australian Information Commissioner



Strach Oncology

My Health Record system security and access policy

Key information

Policy owner	Strach Oncology, ABN: 41956253539
Contact details	info@strachoncology.com (02) 5520 2225
Responsible officer (RO)	Dr Madeleine Strach
Organisation maintenance officer[s] (OMO)¹	Dr Madeleine Strach
Version no.	1.0
Date of last review	16/01/2026
Date of next review	16/01/2027
Other relevant documents	Privacy Policy Cyber Security Policy (Churchill Specialist Services)

¹ Rule 27 of the [My Health Records Rule 2016](#) 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.

Document version history

Version	Date	Release comments	File location
1.0	16/01/2026	Approved by Dr Madeleine Strach and released via intranet	

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 Strach Oncology. For the purposes of this policy, 'employees' include contractors and volunteers.²

Strach Oncology uses conformant clinical software (Magentus Gentu) to access the My Health Record system.

This security and access policy is enforceable and is communicated to all employees by communicating the policy in employee training and inductions.

This security and access policy can be accessed via intranet or hard copies provided at reception.

Provision of services to healthcare providers under contract

Strach Oncology does supply services to healthcare providers under contract,³ including to trainees/registrars and locum doctors.

This security and access policy is communicated to these healthcare providers by communicating the policy in training and inductions.

This security and access policy can be accessed via intranet and hard copies provided at reception.

² 'Employee' is defined in section 5 of the [My Health Records Act 2012](#).

³ 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.

This security and access policy is also enforced in relation to these healthcare providers by contract requiring healthcare providers to comply with the policy.

Authorising, suspending and deactivating access

Strach Oncology authorises individuals to access the My Health Record system on behalf of the organisation by:

- 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, the RO suspends or deactivates their user account by:

- 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 7 days
- removing the link between the organisation and the provider entry in the Health Professional Online Services (HPOS) as soon as practical, within 7 days
- revising the register of authorised users as soon as practical, within 7 days.

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

- deactivating their local account as soon as practical, within 24 hours upon becoming aware of the security breach
- deactivating the user account in the clinical software as soon as practical, within 24 hours and issuing a new login
- revising the register of authorised users as soon as practical, within 24 hours.

Training

Strach Oncology provides training to individuals before they are authorised to access the My Health Record system. Training will be organised by the RO, 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.

Identification of users

In order to identify individual users who access the My Health Record system Strach Oncology has put in place the following process:

- unique identifier is assigned to users by the clinical software
- clinical software records the user's unique identifier 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 name.

The above processes allow the RO to communicate the user's identity to the System Operator when required.⁴

Physical and information security measures

Strach Oncology implements physical and information security measures to control access to the My Health Record system,⁵ including:

- maintaining a register of authorised users containing their name and unique identifier
- employee must use their individual login and passphrase to access the My Health Record system
- employees access the My Health Record system on their desktop/laptop computers and must unlock their computers by using their username and password.

Remote access

Strach Oncology **does** have remote access functionality to access the My Health Record system.⁶

Remote access to the My Health Record system is enabled via clinical software

When accessing the My Health Record system, employees unlock their devices by using multifactor authentication.

⁴ 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, it may be liable for a civil penalty under that legislation.

⁵ See the Australian Digital Health Agency's [Establishing policies checklist](#) and the OAIC's [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.

⁶ 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.

Mitigation strategies

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

- incident response management process
- patient complaints process
- review of relevant internal policies every 2 years
- record and maintenance of audit logs.

Strach Oncology has a process for identifying and responding to security or privacy issues, or breaches of the My Health Record system.⁷ This includes:

- reporting the issue or breach to the RO
- the RO responds by:
 - keeping detailed records of and assessing the issue or breach
 - containing the issue or breach by immediately deactivating any authorised user account(s) suspected to be compromised
 - reporting the issue or breach to the System Operator and the Information Commissioner
- recording actual or suspected breaches into an incident log.

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

- in accordance with the organisation's complaints policy

Where the patient complaint cannot be managed via the organisation's complaints handling procedure, Strach Oncology may advise patients to contact the My Health Record Helpline (1800 723 471) or the OAIC (1300 363 992).

Assisted Registration

Strach Oncology does not provide assisted registration.

⁷ 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](#).