Privacy and Security

All healthcare providers in Australia have professional and legal obligations to protect their patients' health information. Establishing and maintaining information security practices is an essential professional and legal requirement for using electronic health in the delivery of healthcare.

Privacy law

All private healthcare providers are covered by the Australian Privacy Principles (APPs) under the federal Privacy Act 1988. Two important APPs that an organisation must consider with their management of health information, including via the My Health Record system, are:

- APP 1: You must take reasonable steps to implement practices, procedures and systems to ensure that you comply with the APPs and that you can deal with privacy inquiries or complaints.
- APP 11: You must take reasonable steps to protect your records of personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Public sector healthcare providers are covered under State and Territory legislation, and these can require ensuring that health information is kept secure.

Importantly, the My Health Record system and other NEHTA specifications built by General Practice and pharmacy software vendors have been designed to promote compliance with privacy laws.

Healthcare Identifier and My Health Record system security obligations

Use of Healthcare Identifiers, and access to the My Health Record system, are governed by the Healthcare Identifiers Act (HI Act) and the My Health Records Act, the My Health Records Rules and Regulation.

The HI Act requires that an organisation take reasonable steps to protect healthcare identifiers from misuse and loss, and unauthorised access, modification or disclosure.

The My Health Records Rules set out the security requirements that participating organisations must comply with to be eligible to be registered and to remain registered under the My Health Record system. Non-compliance with the My Health Records Rules can result in cancellation of participation and other penalties.

RACGP Computer and Information Security Standards (CISS)

The CISS is a practical guide for General Practices to develop systems and policy to meet their professional and legal obligations in computer and information security. While the CISS is tailored to General Practice, it is a helpful tool for all healthcare organisation to understand and implement good security practice.

Implementing security practices and policies

An organisation should document and implement internal practices and procedures that it uses to protect personal information when using electronic health to deliver healthcare.

The following worksheet can be used as a guide to implementing security practices and policies in your organisation for when staff use electronic health and/or access the My Health Record system. It covers the requirements that must be incorporated in a My Health Record system security policy, and those that are best privacy and security practice, including standards set out in the RACGP CISS. The worksheet is a guide only and should be individualised to meet the needs of your organisation.

More information

- The RACGP Computer and Information Security Standards (CISS) (includes policy templates)
- CISS Addendum: Compliance Indicators for the Australian Privacy Principles
- OAIC Fact Sheet 17: Australian Privacy Principles
- Comlaw: My Health Records Act, My Health Records Rules, My Health Records Regulation
- OAIC Fact Sheet 18: the OAIC and the eHealth Record system
- OAIC Business resources: Individual Healthcare Identifiers—Compliance obligations of private healthcare providers
- National eHealth Security and Access Framework

My Health Record System Security Policy	✓ The organisation has an My Health Record system security policy in place ✓ The policy is communicated to all staff and is readily accessible to all staff and any healthcare providers to whom the organisation supplies services under contract ✓ The policy is enforced in relation to all staff ✓ The policy is regularly reviewed (at least annually) to ensure relevance and accuracy, in particular where any new material or changed risks are identified and where changes in eHealth legislation or the structure of the organisation occur ✓ Each iteration of the policy contains a unique version number and the date when that iteration came into effect ✓ The organisation is able to provide a copy of the policy on request to the System Operator within 7 days ✓ The policy sets out: o The organisation's user account management measures and manner of authorising staff to access the My Health Record system (see 'Managing User Accounts') o The training that will be provided to users who access the My Health Record system (see 'Staff Training') o The process for identifying staff who request access to the My Health Record system (see 'Identification of staff') o The process for destroying My Health Record system document and record codes in a secure manner o The mitigation strategies to ensure My Health Record system related security risks can be identified, acted upon and reported (see 'Handling of Privacy Breaches and Complaints' and 'Risk Assessments')
Managing User Accounts	✓ The names and position of staff who are authorised to access the My Health Record system are recorded and kept up-to-date ✓ Practice software controls limit access to the My Health Record system to those staff required by the duties of their role to access the system ✓ Staff are provided a unique user account with individual login ✓ Staff passwords are regularly reviewed, changed and sufficiently complex ✓ Users are required to enter their user name and password to deactivate screensavers ✓ A user account is immediately suspended or deactivated where a user leaves the organisation, has the security of their account compromised or whose duties no longer require them to access the My Health Record system ✓ A user account is inactivated/deleted after the departure of staff members as part of the organisation's off-boarding process ✓ Where My Health Record system Provider Portal access is required, the organisation maintains a list of up-to-date authorised providers and communicates this with the System Operator
Identification of Staff	✓ Clinical software is used to assign and record unique internal staff member identification codes (including an HPI-I for those providers with an HPI-I) ✓ The unique identification code, or the provider's HPI-I, is recorded by the clinical software against any My Health Record system access
Staff Training	✓ All staff requiring My Health Record system access undergo training before accessing the system ✓ Training is provided in relation to how to use the My Health Record system accurately and responsibly, the legal obligations on organisation and individuals using the system and the consequences of breaching these obligations ✓ Training is provided to staff on a regular and ongoing basis ✓ A register of staff who have attended training is maintained
Handling of Privacy Breaches and Complaints	✓ The organisation has a reporting procedure to allow staff to inform management regarding any suspected security or privacy issue or breach of the My Health Record system ✓ An incident register/log is kept of any suspected breach including details of the date and time of the breach, the user account that was involved and which patient's information was accessed (if known) ✓ A process is in place for the RO or OMO to report a breach to the System Operator ✓ If a patient raises an issue in relation to unauthorised access to their digital health record, the organisation has a complaints management process to take steps to investigate the issue
Risk Assessments	✓ The organisation undertakes periodic, privacy and security risk assessments of staff use of the My Health Record system and the organisation's ICT systems generally, and implement improvements as required ✓ All risk assessments are documented appropriately