

Cricket Australia My Health Record policy

Current as of: 17/6/2026

Version no: 1.1

Dr John Orchard Cricket Australia Chief Medical Officer, in conjunction with Pip Inge, Miranda Menaspa and Tom Cramer.

This policy provides guidance for doctors about access to and use of My Health Record within the CA virtual practice on MediRecords platform. It also provides guidance in the use of information technology in our practice as it relates to My Health Record.

This practice's My Health Record policy is:

- drafted so that our practice can be audited against it to determine that the practice is in compliance with the policy
- kept up to date and reviewed annually and also when any new or changed risks are identified
- version-controlled so that each iteration contains a unique version number and the date when it came into effect
- inclusive of definitions of the roles of responsible officer and organisation maintenance officer.

Responsible officer (RO) and organisation maintenance officer (OMO)

The following roles are responsible for implementation and compliance monitoring of My Health Record policy in our practice:

- Our RO, John Orchard AM, oversees our practice's legal compliance and sets up procedures to facilitate compliance with My Health Record legislation.
- Our OMO, Miranda Menaspa, is responsible for maintenance of the policy within our medical service.

How My Health Record is accessed in this practice

At our (virtual) practice we access My Health Record via the MediRecords software

Registration for individuals (doctors) authorised access to My Health Record is by way of the doctor being registered for a MediRecords account by the Platform Manager, High Performance (after being nominated by Head of Performance Services). Connection to the Cricket Australia HPI-O is a responsibility of John Orchard (CA CMO) & Tom Cramer (Platform Manager)

John Orchard maintains the currency of our Health Provider Identifier – Organisation (HPI-O) and our information on the National Health Services Directory according to the requirements of the *Health Identifiers Act 2010*.

In our practice we collect and record the Healthcare Provider Identifiers (HPI-Is) of our healthcare providers by these doctors applying individually to PRODA. The doctors can then have their HPI-I linked to the Cricket Australia HPI-O via MediRecords. Doctors also then need to apply for a provider number through PRODA for Cricket Australia 20 Greg Chappell St Albion 4010 Qld.

We have a system in place to authorise access for users to access My Health Record by the doctors only logging in to MediRecords via their AC or personal laptop. All logins are via SSO with 2FA. There are no shared terminals, and no one other than doctors uses MediRecords or has a login.

Access to My Health Record is not audited as there are no practice computers, only the doctors' individual laptops. The practice therefore cannot audit logins as there is no ability to access a doctor's personal computer by anyone else. The practice would provide reasonable assistance to the System Operator or the Office of the Australian Information Commissioner (OAIC) to obtain this information should it be required.

Our practice does not give permission for health practitioners other than the designated CA Doctors to view My Health Record via their own National Authentication Service for Health (NASH) certificates or Provider Digital Access (PRODA) credentials, under the practice's registration for access of My Health Record. There is no access for any non-doctors (i.e. a practice manager or physiotherapist) other than the Platform Manager who has limited administrator rights but cannot access patient records.

When an individual who is authorised to access My Health Record in our practice leaves our practice, we deactivate their local account by :

- removing the link between the practice and the provider entry in the healthcare provider directory via the Healthcare Identifier (HI) service on the Health Professional Online Service (clinical staff only) where you provide access to the provider portal on MediRecords
- revising the register of authorised users.

If the access security of one of our individuals authorised to use My Health Record has been compromised, their account will be de-activated by:

- de-activating local account immediately when the practice becomes aware of the security breach
- de-activating relevant user logon to MediRecords and issuing new user logon to MediRecords for the concerned doctor
- keeping record of the details surrounding the event
- discerning who the account belongs to and why the security breach happened
- notifying My Health Record System Operator of the breach.

My Health Record user training

In our practice we ensure that all authorised individuals who access My Health Record have accessed comprehensive training that is current and provided by a credible source. This training includes how to use the system accurately and responsibly, the legal obligations of healthcare provider organisations and individuals using the system, and the consequences of breaching those obligations.

Dr Orchard provides training to each doctor who receives a MediRecord connection to the HPI-O, including a manual.

Assisted registration

Our practice does not provide assisted registration for patients. We do not currently encourage athletes to have a MediRecords account. The purposes of using MediRecords are to enable E-scripts to be written, to receive Radiology and Pathology reports, to access My Health Record accounts, to write referrals on

CA letterhead, to occasionally receive specialist letters via Healthlink, to check details of immunisations on the AIR and to add to the AIR when new vaccines are given.

Requests to access a patient's My Health Record

Our practice has established processes for identifying a person who requests access to a patient's My Health Record, being that if an athlete wanted to access their own My Health Record, one of the doctors would assist.

We will explore transfer of information to and from the Cricket AMS (TeamWorks) and MediRecords. This policy will be re-written when information transfer is occurring to cope with security of TeamWorks AMS.

Physical and information security measures

In our practice we have established the following physical and information security measures. These should be adhered to by everyone accessing our practice system.

- restricting access to only persons who require access as part of their duties (ie doctors and no other health professionals)
- not logging in using CA shared terminals (ie doctors only log in on their own computers which are 2FA protected and which other SSSM members do not use)
- having 2FA/passkey and/or other access mechanisms that are sufficiently secure and robust to ensure security and privacy risks associated with unauthorised access to the system are adequately covered
- implementing screensaver settings on doctor computers so that users are required to re-enter their passkey to login after shutting down or hibernating.
- ensuring that individuals no longer authorised to access My Health Record via or on behalf of the healthcare provider organisation are not able to do so via their user accounts
- suspending a user account that enables access to My Health Record as soon as practical after becoming aware that the account has been compromised

Mitigation strategies

To ensure that My Health Record system-related security risks can be promptly identified, acted upon and reported to the relevant authority, our practice will:

- continue to only allow access to doctors using passkey-protected entry to the system