Policy

Our practice has systems in place to protect the privacy, security, quality and integrity of the data held. All staff are educated and regularly trained in our computer security policies and procedures. Our policies and procedures are a source of information to clarify roles and responsibilities, and to facilitate the orientation of new practice team members.

The RACGP Computer and Information Security Standards provide information and explanations on the safeguards and procedures that need to be followed by general practices in order to meet appropriate legal and ethical standards concerning privacy and security of patient health information. These documents also contain suggestions for additional security procedures.

Our practice has a *My Health Records* policy that covers the specific requirements of *My Health Records Act 2012* and *My Health Records Rule 2016*

Our practice has the following information to support the computer and information security policies and procedures:

- current asset register documenting hardware and software specifications and locations, network information, technical support
- logbooks/print-outs of maintenance, backup including test restoration, faults, virus scans
- folder with warranties, invoices/receipts, maintenance agreements.

Procedures

Practice Team Agreements

Upon employment, every practice team member is given confidentiality and privacy agreements to sign, together with an appropriate computer use agreement. These act to protect the owners of the practice in the event of legal action against the practice arising out of a security breach.

These agreements are used to ensure that practice team members and other people working in a practice who may have access to confidential patient or business information comply with privacy and security of information as required under legislation, including the *Privacy Act 1988* and the Australian Privacy Principles.

External Service Provider Agreements

Unique contractual arrangements are made with all external service providers including information in relation to:

- data confidentiality
- remote access

- backups and restoration procedures
- response times
- costs
- regular maintenance
- audit logs
- secure disposal of information assets
- cloud services

My *Health Records* Policy

The following information is taken from *My Health Records Rule 2016*:

The Practice will enforce the following in relation to all its employees and any Organisation with whom we engage under an agreement/contract:

- The manner by which the Practice authorises persons accessing the *My Health Records* system via or on behalf of the practice
- The manner of suspending and deactivating the user account of any authorised person:- who leaves the practice,
- The manner of suspending and deactivating the user account of any authorised person whose duties no longer require them to access the *My Health Records* system,
- The manner of suspending and deactivating the user account of any authorised person whose security has been compromised.

Our practice ensures the following:

- Training will be provided before a person is authorised to access the *My Health Records* system, including in relation to how to use the *My Health Records* system accurately and responsibly, the legal obligations on the practice and our staff members using the *My Health Records* system and the consequences of breaching those obligations.
- The process for identifying a person who requests access to a patient's *My Health Records* is clear and followed and the person's identity is communicated to the System Operator so that the healthcare provider and the practice is able to meet its obligations.
- Physical and information security measures are established and adhered to by the healthcare provider, the practice and people accessing the *My Health Records* system via or on behalf of the healthcare provider, the practice, including that user account management measures are implemented.
- Mitigation strategies to ensure *My Health Records* related security risks can be promptly identified, acted upon and reported to the Practice Manager.

The Practice will authorise the staff members within its team that require access to the *My Health Records* system by:

- Generating and maintaining an authorised employee register, which includes the name and HPI-I for all health care professionals working at the Practice or on behalf of the practice.

- Registering both our HPI-O and the HPI-Is of our practitioners for publication in the Healthcare Provider Directory (HPD)
- Recording and keeping current the credentials of all our staff who require access to the *My Health Records* system

For a staff member who leaves the Practice we will deactivate their account by:

- De-activating the HPI-I in our clinical software and removal of individual login details.
- Revising our Authorised Employee Register
- Keeping a local record of the revised Authorised Employee Register for audit trail purposes.

For a staff member whose duties no longer require them to access the *My Health Records* system we will deactivate their account by:

- De-activating the HPI-I in our clinical software and removal of individual login details.
- Revising our Authorised Employee Register
- Keeping a local record of the revised Authorised Employee Register for audit trail purposes.

For a staff member whose security has been compromised we will immediately deactivate their account by:

- De-activating the HPI-I in our clinical software and removal of individual login details.
- Revising our Authorised Employee Register
- Keeping a local record of the revised Authorised Employee Register for audit trail purposes.
- Keeping record of the details surrounding the event (e.g. who and why).
- Pursuing the necessary disciplinary action if necessary

Training will also be conducted as new functionality is introduced into the system. We will utilise the training resources made available by the System Operator, as a minimum. To assist in ensuring training completion and audit purposes, a record is kept confirming the training completed by each authorised staff member and the date completed.

Notwithstanding any action the System Operator may take with regard to data breaches, the practice will continue to implement local staff conduct and disciplinary policies with regard to any staff unauthorised access to the *My Health Records* system.

Our practice will also ensure the following:

- staff members that we authorise to access the system can be identified by either a unique local identifier or system log-in
- the Practice has current and adequate IT system anti-viral software
- our Disaster Recovery Plans are current and executable

- ensure our IT systems and hardware is physically protection against unauthorised access or hacking
- that each authorised user of the system has a secure password

We regularly review our security and procedures for accessing the *My Health Records* system, report the findings to management and revise our procedures accordingly.

The practice has set out a risk reporting procedure to allow staff to inform management regarding any suspected security issue or breach of the system.

All staff in the practice and any healthcare providers to whom the organisation supplies services under contract have access to this Policy. The practice will notify all personnel of changes to these Policies and Procedures when they occur.