



## Information security

Computerised patient health information in the Practice shall be kept secure at all times. Not all staff need full access to this information. Different levels of access, documented in the policy and procedures manual, are therefore required for each staff position. Staff shall have individual passwords to obtain patient information.

### RACGP Standards

**4.2.2D** *If our practice uses computers to store patient health information, our practice ensures that:*

- *our GP(s) and staff have personal passwords to authorise appropriate levels of access to health information*
- *screensavers or other automated privacy protection devices are enabled*
- *backups of electronic information are performed at a frequency consistent with a documented information disaster recovery plan*
- *backups of electronic information are stored in a secure offsite environment*
- *antivirus software is installed and updated*
- *all internet connected computers have hardware/software firewalls installed*

**4.2.2E** *If our practice uses computers to store personal health information, our practice has an information disaster recovery plan that has been developed, tested and is documented*

### Assessment methods

- Document review of practice systems or policy and procedure manual

Surveyors speak to staff and ask to view the policy and procedures manual to verify that security procedures for patient health information are in place.

- Documentary evidence of backup system and other security measures

Evidence will be required regarding the procedure for backups and security measures for the computer system.

### Meeting the standards

The Practice shall have different levels of access for each staff position and should be documented in the policy and procedures manual. Staff shall have individual passwords.

Other protective measures to be in place include antivirus and firewall protection, screen savers and the removal of the daily backup tape from the premises to a secure location.

The Practice should keep a record of their daily backups (recorded daily and initialed).

Practices shall have a documented information disaster recovery plan in place in the event of an emergency, such as power failure, fire or flooding, to prevent computer-stored information being destroyed and/or damaged

### Best practice:

- A daily, initialed record is kept of all backups.
- Backups are kept off site and proven to be usable.
- The Practice involves a reputable computer technician/company in the design of the IT system when available and financially viable.
- Screen savers will be password protected.