Information Security

Computerised patient health information in the Practice will be kept secure at all times. Not all staff members 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 will have individual passwords to obtain patient information.

RACGP 4th Edition Standards

4.2.2B *Our practice ensures that our practice computers and servers comply with the RACGP computer security checklist and that:*

- *computers are only accessible via individual password access to those in the practice team who have appropriate levels of authorisation*
- *computers have screensavers, or other automated privacy protection devices are enabled to prevent unauthorised access to computers*
- *servers are backed up and checked at frequent intervals consistent with a documented business continuity plan*
- *back up information is stored in a secure off site environment*
- *computers are protected by antivirus software that is installed and updated regularly*
- *computers connected to the internet are protected by appropriate hardware/software firewalls.*

4.2.2C *If our practice uses computers to store personal health information, we have a business continuity 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 procedures for backups and security measures for the computer system.

Meeting the standards

The practice will have different levels of access for each staff position and should be documented in the policy and procedures manual. Staff will 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 initialled).

Practices shall have a documented business continuity 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, initialled record is kept of all backups.
- Backups are kept off site and proven to be usable.
- Screen savers will be password protected.

PO Box 83 Gundagai NSW 2722
Phone: 02 6944 4042 Fax: 03 8888 9988
Web: www.gpa.net.au
Email: info@gpa.net.au

GPA ACCREDITATION *plus*
is General Practice Australia ACCREDITATION plus
Quality Practice Accreditation Pty Ltd
ABN: 26 081 986 932

Accredited by Joint Accreditation System of Australia and New Zealand Acc No G2601102AS