RACGP

Governance roles and responsibilities

It is vital that all staff members are aware of the processes and requirements in the practice that directly impact their role. In the event of system failure or a security breach, the practice team members need to know what to do and what roles and responsibilities they have in order to confidently, safely and efficiently handle such situations.

Access control and management

Back-up systems management

Disaster recovery management

Development and implementation of policies and procedures

Internal and ongoing communication strategy – all policies should be in written format and communicated to relevant practice team members on an ongoing basis

Undertake a structured risk assessment of information security and identified improvements as required

For information on roles and responsibilities, refer to the RACGP's *Computer and information security standards* (CISS) Standard 1 at www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/standard-1/

For information on roles and responsibilities, refer to the CISS Standard 2 at www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/standard-2/

For information on developing policies and procedures, refer to the CISS Standard 3 at www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/standard-3/

For information on information back-up, refer to the CISS Standard 7 at www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/standard-7/

For a computer security checklist and videos on the CISS topics, refer to the RACGP's Digital Business Kits website at www.racgp.org.au/digital-business-kit/ciss-checklist/

It is recommended that you contact an IT professional for specific advice on hardware and software compliance.

Governance/roles and responsibilities in general practice checklist

Date of completion

Name of practice

All practice staff members are aware of the processes and requirements in the practice that directly impact their role. In the event of system failure or a security breach, practice team members are aware of what needs to be done and what roles and responsibilities they have in order to confidently, safely and efficiently handle such situations. Staff members are aware that some of the responsibilities include:

- [ ] Access control and management
- [ ] Back-up systems management
- [ ] Disaster recovery management
- [ ] Development and implementation of policies and procedures
- [ ] Internal and ongoing communication strategy – all policies should be in written format and communicated to relevant practice team members on an ongoing basis
- [ ] Undertake a structured risk assessment of information security and identified improvements as required

Notes