RACGP | *Security*

A secure computer and information management system is essential to protect business and clinical information. Secure systems are critical for the provision of safe, high-quality healthcare and the efficient running of a general practice. Below is a list of considerations regarding the security of your hardware, software and data, plus links to a number of helpful resources.

Physical and logical security

Logical security includes the placement of hardware and software in your practice room and around your general practice, ensuring it is not visible to outsiders.

For a more information, refer to the RACGP's *Computer and information security standards* (CISS) Standard 3 at www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/standard-3/

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

Access controls and authentication:

- **Personalised log in and passwords**
- **Digital credentials and tokens, eg. public key infrastructure (PKI)**

For a more information, refer to the CISS Standard 4 at www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/standard-4/

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

Security audits

Schedule security audits to ensure that your security systems are still providing the right level of protection needed.

For a more information refer to the CISS Standard 2 at www.racgp.org.au/your-practice/standards/computer-and-information-security-standards/standard-2/

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

Computer Security in general practice checklist

Date of completion

Name of practice

When implementing security systems in our general practice we have used the below checklist to guide us through what needs to be considered. We have consulted with an IT professional on the recommendations.

Physical and logical security

Theft, fraud and malicious attacks

Security Audits

Access controls and authentication

Personalised log in and passwords

Digital credentials and tokens, eg. Public Key Infrastructure (PKI)

Notes