# CLPN4.23 – COMPUTER INFORMATION SECURITY Policy

## Policy Statement

Our practice has systems in place to protect the privacy, security, quality and integrity of the data held electronically. All members of our practice team are trained in computer use and in our security policies and procedures. Updates to any computer security requirements are communicated to each team member at the time of the change.

The management of all practice computers and servers comply with the RACGP's Computer and information security standards {CISS) (2nd edition) https:/ / www.racgp .org.au/ your-practice/ standards/ computer-and -information-security-standards/ including:

- The ICT Co Ordinator is responsible for managing computer and information security, including the definition of this role and its responsibilities in their position description
- Undertaking an annual structured risk assessment of information security and identifying improvements as required
- Documented policies and procedures for managing computer and information security
- Well-established and monitored authorised access to health information
- Documented and tested plans for business continuity and information recovery
- Processes to ensure the safe and proper use of internet and email in accordance with practice policies and procedures for managing information security
- Reliable information backup systems to support timely access to business and clinical information
- Reliable protection against malware and viruses
- Reliable computer network perimeter controls
- Processes to ensure the safe and proper use of mobile electronic devices in accordance with practice policies and procedures for managing information security
- Managing and maintaining the physical facilities and computer hardware, software and operating system with a view to protecting information security, and
- Reliable systems for the secure electronic sharing of confidential information.

## Related Documents

ORGPN03 - Computer, Internet and Email policy