



The Royal Australian
College of General
Practitioners



OXYGEN
Intelligence in Practice

Frequently asked questions

RACGP Computer security guidelines (3rd edition)

What are the Computer security guidelines?

The RACGP *Computer security guidelines* (3rd edition) provide general practices and their staff with the tools and information to implement protection measures to ensure appropriate levels of security for the business of general practice and health information.

Who are they aimed at?

All general practices that use computers, including general practitioners, practice nurses, practice managers, allied health professionals and administration staff.

Who were they developed by?

The RACGP *Computer security guidelines* were developed by the RACGP with funding support from the National eHealth Transitional Authority (NEHTA). Additional development, review, and writing, was provided by Associate Professor Peter Schattner, the RACGP e-health Standards and e-health Working Groups, Associate Professor Ron Tomlins, Dr John W Bennett, and Dr Trish Williams (PhD).

Why are they needed?

There are an increasing number of threats where individuals are compromising, stealing, changing, or destroying information online, and the borderless, anonymous nature of the internet makes it hard to track down the source of these cyber attacks. With security threats proliferating globally in just minutes, it is no longer appropriate to implement reactive security policies. Proactive security policies are now essential.

The contribution of general practices as the primary medical point of care, is critical to the success of the healthcare system. However, rigorous information security within general practice is also crucial. Protecting all the practice's information requires security measures addressing technology, policy, and process issues. It is essential that staff are trained and aware of security activities. General practices are susceptible to the same threats and vulnerabilities as larger organisations and need to protect their information. In general practice there may be a lack of information technology expertise but a reliance on the internet and online resources. As general practice further embraces e-health initiatives, there will be a greater emphasis on secure messaging delivery (SMD) to send and receive patient information.

What information might be targeted by people wanting to breach my practice's computer security?

Cyber criminals target personal and business information, such as information about identity and finances. This information can include names, dates of birth, home addresses, bank account details, passwords, credit card details and logins. This is more likely to be targeted than clinical information.

What types of security breaches and computer crimes is my practice at risk from?

According to the Australian Institute of Criminology, from 2003–2006 the most common computer crimes and security breaches were virus/worm/Trojan infections, laptop theft, and computer system abuse. A 2009 US report showed that in the US there has been an increase in financial fraud and malware infection, while one third of respondent organisations were fraudulently represented in phishing scams.

What do the guidelines provide?

The guidelines provide:

- a checklist to determine whether reasonable security measures are established in a practice;
- a guideline for each security risk category; and
- proformas of useful information such as how to produce business continuity and disaster recovery plans.

What issues are covered in the computer security checklist?

It assesses the basic computer security processes currently in place.

The IT categories covered by the security checklist are:

- practice computer security coordinator
- practice computer security policies and procedures
- access control and management
- business continuity and disaster recovery plans
- backup
- malware and viruses
- network perimeter controls
- portable devices and remote access security
- computer and network maintenance
- secure electronic communication.

What technical issues do the guidelines cover?

The guidelines cover:

- backup
- malware and viruses
- network perimeter controls
- portable devices and remote access security
- computer and network maintenance
- secure electronic communication.

Can other computer security guidelines be used?

While many information security measures within general practice are similar to those required in other small businesses, there are added medico-legal and accreditation responsibilities, compliance requirements, and greater impacts and repercussions should clinical information be misused.

Do I need to follow these guidelines for successful accreditation?

The guidelines are aligned with the RACGP *Standards for general practices* (4th edition) which will support practices in gaining successful accreditation status.

Practices need to demonstrate a structured and risk analysis approach to ensuring security for the information that is held within the practice information systems. The *Computer security guidelines* are in excess of the requirements for accreditation.

What return do I get on my investment in security?

An investment in computer security is an investment in patient safety and the well being of the business. The investment will be dependent on the size of the practice, what IT and computer security needs the practice has, and whether or not the practice requires the assistance of an external IT consultant.

I only use my computer for sending and receiving emails – do the guidelines apply to me?

Electronic mail (email) is the most popularly used system for exchanging business information over the internet (or any other computer network). At the most basic level, the email process can be divided into two principal components:

1. mail servers – which are hosts that deliver, forward, and store email, and
2. mail clients – which interface with users and allow users to read, compose, send, and store email.

This document addresses the security issues of mail servers and mail clients, including web based access to mail.

Mail servers and user workstations running mail clients are frequently targeted by attackers. Because the computing and networking technologies that underlie email are ubiquitous and well understood by so many, attackers are able to develop attack methods to exploit security weaknesses. Mail servers are also targeted because they (and public web servers) must communicate to some degree with untrusted third parties. Additionally, mail clients have been targeted as an effective means of inserting malware into machines and of propagating this code to other machines.

As a result, mail servers, mail clients, and the network infrastructure that supports them must be protected.

The guidelines recommend that practices nominate a security coordinator. What sort of person is suited to this role, how often should the role of the nominated security coordinator be reviewed and who should train the coordinator?

The practice security coordinator is the person responsible for drawing together the computer security issues that confront the practice and is very much a leadership role. The coordinator might be one of the doctors, a nurse, a senior receptionist or the practice manager. A generic role description for the computer security coordinator is outlined in *Appendix A* of the guidelines. It is suggested that the role be reviewed annually.

The guidelines cover backups of data. How often should these backups be performed?

Backups of data should be performed daily, with weekly, monthly, and yearly copies retained both on and off site.

The guidelines mention encryption and authentication. What is the difference between encryption and authentication?

Encryption means data is electronically 'scrambled' so that it cannot be read unless the information is decrypted. Authentication means that one can verify whether the sender is who they say they are. This is done by using digital signatures.

I use a flash drive/USB to save electronic files and take them home with me. Do the guidelines mention portable devices?

Yes, the guidelines cover portable devices and remote access security with suggestions on how practices can widen computer security measures beyond the walls of the practice.

For further information please contact the RACGP e-health team by email ehealth@racgp.org.au