

www.gpcg.org

The GPCG Computer Security Self-Assessment Guideline and Checklist for General Practitioners

2nd edition January 2005



Contents

Acknowledgements	2
ONE Introduction	3
1.1 Why was this Guideline developed?	3
1.2 How was it developed?	3
1.3 How should you use this Guideline?	4
TWO Computer Security Checklist	5
THREE The 10-item IT Security Guidelines	6
A Organisational Issues	6
3.1 Practice computer security coordinator	6
3.2 Practice security policies and procedures manual	7
3.3 Access control	8
3.4 Disaster recovery plan	9
3.5 Consulting room and 'front desk' security	10
B Technical Issues	11
3.6 Back-ups	11
3.7 Viruses	12
3.8 Firewalls	13
3.9 Network maintenance	14
3.10 Secure electronic communication	15
FOUR Conclusion	16
FIVE Further Information	17
SIX Appendices	18

Acknowledgements

2

I wish to thank the following people and organisations for their contribution to the Computer Security Guideline and Checklist: The Australian Government Department of Health and Ageing; the General Practice Computing Group (especially its Privacy and Security Working Group); Ms Catherine Pleteshner (University of Melbourne); Ms Leslie Stanger and Dr Nathan Pinskiar (Monash Division of General Practice); Dr Britt Klein and Professor Jeff Richards (Monash University); Ms Deanne Keetelaar (Medical Defence Association of Victoria); and numerous experts who were consulted (from general practice, government, the IT and medical software industry, medical professional organisations, and consumers).

I acknowledge the work done by the RACGP, Frank Quinlan and the AMA, the GPCG, and Karen Young and Laurie Barrand from the Monash Division in developing earlier versions of this Guideline.

A/Prof Peter Schattner
Department of General Practice
Monash University

867 Centre Road
East Bentleigh VIC 3165

p: 03 8575 2222

f: 03 8575 2232

e: peter.schattner@med.monash.edu.au

ONE Introduction

1.1 Why was this Guideline developed?

There are two main reasons why data security in general practice is vital: to keep the business operations of a practice going and to maintain a health record system. The first is critical for the practice (and the income of the GP), but not immediately threatening to patient health. The second, however, may lead to a loss of patient clinical information, making medical care more difficult and prone to errors.

To maintain electronic data in general practice requires some planning and only a small degree of technical knowledge. This Guideline has been designed with the practice, that is, its staff and GPs, in mind. It is not a technical manual, but should assist practices to put in place a series of computer security strategies.

When reading this Guideline, bear in mind that it is only about computer security. That is, it refers to the following:

-] the availability of data (one can get it when one wants to);
-] the integrity of data (it is not degraded or lost); and
-] accessibility of data (only authorised people can see confidential data).

1.2 How was it developed?

The Security Guideline was developed by a number of experts who understand the needs of computer security in general practice and who know that if it were too complicated, it would not be useful. Nevertheless, it is difficult to produce a Guideline which will suit all practices. Large practices have different computer systems to solo ones; practices vary in their possession of in-house computer skills; 'paperless' practices will have different needs to those who only use computers for patient billing; rural practitioners may have less opportunity for obtaining technical support; and divisions of general practice vary in their ability to provide GPs with information technology (IT) support. We have good reason to consider that this Guideline strikes the right balance between simplicity and detail.

1.3 How should you use this Guideline?

There are three sections to this Guideline:

- (i) A **Checklist** which should easily help you to determine whether you have established reasonable computer security measures in your practice to counteract your IT security risk.
- (ii) The **Guideline** itself, with each IT risk category organised in the same way. We ask three questions to guide you through each item. These are:

What does this risk category mean? This involves an explanation of what it is, and usually a simple technical explanation is given.

Why is it important? Why should GPs spend time and money on the risk? What might happen if GPs ignore the recommendations?

What should be done about it? What are the step-by-step processes which should be followed to manage the risk?

- (iii) A series of **proformas** which provide useful lists such as how to produce a disaster recovery plan. One of these proformas has been made into a template which you can download from the GPCG website (www.gpcg.org). By adding information relevant to your practice, you can incorporate this template into your practice's policies and procedures manual.

TWO Computer Security Checklist

This is a Checklist for you to see whether you have put in place a number of computer security processes or systems. Please note that the list is restricted to security aspects of Information Technology (IT). This Checklist is available from the GPCG website (www.gpcg.org).

IT CATEGORY	TASKS	HAS THIS BEEN IMPLEMENTED: (TICK IF YES)
Practice computer security coordinator	<ul style="list-style-type: none"> Practice IT security coordinator's role description written (for GP, existing staff member or practice manager). Practice IT security coordinator appointed. IT security training for coordinator provided. Security coordinator's role reviewed on... 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="text" value="/ /"/>
Practice IT security policies and procedures	<ul style="list-style-type: none"> Person(s) (e.g. IT security coordinator) appointed to document (and revise) security policies and procedures (can be part of practice manual). IT security policies and procedures documented. IT security policies and procedures documentation last reviewed... Staff trained in IT security policies and procedures. 	<input type="checkbox"/> <input type="checkbox"/> <input type="text" value="/ /"/> <input type="checkbox"/>
Access control	<ul style="list-style-type: none"> Staff policy developed on levels of electronic access to data and systems. Staff have created personal passwords to access appropriate level. Passwords are kept secure. Consideration given to changing passwords periodically. 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Disaster recovery plan	<ul style="list-style-type: none"> Disaster recovery plan developed. Disaster recovery plan last tested... Disaster recovery plan last updated... 	<input type="checkbox"/> <input type="text" value="/ /"/> <input type="text" value="/ /"/>
Consulting room and 'front desk' security	<ul style="list-style-type: none"> Practice aware of need to maintain appropriate confidentiality of information on computer screens. Screensavers or other automated privacy protection device enabled. 	<input type="checkbox"/> <input type="checkbox"/>
Back-ups	<ul style="list-style-type: none"> Back-ups of data done daily. Back-ups of data stored offsite. Back-up procedure last tested (by performing a restoration of data)... Back-up procedure has been included in a documented disaster recovery plan. 	<input type="checkbox"/> <input type="checkbox"/> <input type="text" value="/ /"/> <input type="checkbox"/>
Viruses	<ul style="list-style-type: none"> Anti-viral software installed on all computers. Automatic updating of viral definitions enabled (daily if possible). Staff trained in anti-viral measures as documented in policies and procedures manual. 	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
Firewalls	<ul style="list-style-type: none"> Hardware and/or software firewalls installed. Hardware and/or software firewalls tested. 	<input type="checkbox"/> <input type="checkbox"/>
Network maintenance	<ul style="list-style-type: none"> Computer hardware and software maintained in optimal condition (includes physical security, efficient performance of computer programs, and program upgrades and patches). Uninterruptible Power Supply installed (to at least the server). 	<input type="checkbox"/> <input type="checkbox"/>
Secure electronic communication	<ul style="list-style-type: none"> Encryption systems considered. Encryption used for the electronic transfer of confidential information. 	<input type="checkbox"/> <input type="checkbox"/>

THREE The 10-item IT Security Guidelines

6

Computer security is as much about people and what they do as it is about technical matters. That is why organisational issues are presented before the technical ones. Good communication within the practice and basic training for staff and GPs are essential to the maintenance of computer security.

A Organisational issues

3.1 Practice computer security coordinator

What does this mean?

This is the person who is responsible for drawing together the computer security issues which confront the practice. This includes:

-] seeing that a security policies and procedures manual has been written (as part of a general practice manual);
-] ensuring that all the items in the Guideline are being followed;
-] arranging staff training;
-] clarifying the computer security roles and responsibilities of staff;
-] keeping the asset register up-to-date and making sure that all operating manuals, installation disks and protocols are catalogued and stored safely;
-] developing a policy on staff access to computer data and systems;
-] coordinating the application for storage and use of digital certificates, and training staff and GPs on the use of encryption; and
-] knowing how and when to seek the advice of an IT technical support person such as a systems administrator.

The practice security coordinator might be one of the doctors, one of the senior receptionists or the practice manager. The tasks can be allocated to more than one person. Most likely, the person will already be an existing member of the practice.

A 'generic' IT security coordinator's role description can be found in Appendix A.

Why is it important?

Without a coordinator, IT policies and procedures are likely to be developed in an ad hoc way. Most likely, this will lead to a lack of preparation for the inevitable computer system 'disaster'. A coordinator is responsible for overseeing computer security rather than being a technical 'fix-it' person. They should help to engender enthusiasm for an IT security 'culture' within the practice and ensure that there is adequate training for all.

What should be done about it?

- ___ Practice IT security coordinator's role description written.
- ___ Practice IT security coordinator appointed.
- ___ IT security training for coordinator provided.
- ___ Security coordinator's role reviewed (at specified intervals, e.g. annually).

7

3.2 Practice security policies and procedures manual

What does this mean?

Practices should document their computer security policies and procedures. A security manual should include the following:

-] the roles and responsibilities of the practice's staff (medical and non-medical), and in particular, the role of the practice IT coordinator (see previous section);
-] a disaster recovery plan to enable the practice to function when the computer system 'goes down';
-] who has access rights (via passwords) to various levels of the clinical and practice management software;
-] an IT assets register of hardware, software and support services; and
-] other aspects of computer security which are covered in this Guideline.

A generic computer security policies and procedures manual proforma can be found in Appendix B. A template version can be downloaded from the GPCG website (www.gpcg.org). Note that this manual should really be a part of a general practice manual.

Why is it important?

A procedures manual will help practices to access information when it is required, such as a list of phone numbers of software suppliers, or details about operating systems. It is a source of information for when staff are absent or leave the practice, and it helps clarify who does what.

This resource is a tool to encourage practices to study their computer systems and think through their requirements in both human and financial terms. The thought that is applied to developing a security manual and the communication within the practice is more important than producing something which will sit on a shelf.

The asset register should describe your equipment details, dates of purchase, warranty periods, locations in the practice, software, installation disks and manuals, and details about your technical service provider. An asset register template is included with the IT security policies and procedures template on the GPCG website (www.gpcg.org).

What should be done about it?

- ___ Person(s) (e.g. IT security coordinator) appointed to document (and revise) security policies and procedures (which can be part of the general practice manual).
- ___ IT security policies and procedures documented.
- ___ IT security policies and procedures documentation reviewed (at specified intervals, e.g. annually).
- ___ Staff trained in IT security policies and procedures.

3.3 Access control

What does this mean?

One of the key features of data security is that only certain people should see some types of information such as sensitive financial or clinical information. Practices should work out a policy on who can have access to specific data and systems. For example, what should the receptionists or medical assistants be able to see?

Once a policy has been determined, then practice staff can choose passwords (or other appropriate access controls such as 'smartcards') to provide them with their appropriate level of access. Passwords can be implemented for the operating system, application software, files within software and email.

Why is it important?

It is important to ensure the privacy of patient data and to comply with national privacy principles. Restricted access also protects the practice against misuse of financial data and lessens the risk of accidental change or deletion. The use of passwords is really only a part of a practice's 'right to know' policy.

Because of the level of trust that routinely exists within a practice, passwords are often not managed well – until someone without due authorisation abuses their privilege. It is best people remain responsible for their own passwords and do not share them with other members of the practice.

In some practices the systems administrator might keep a list of passwords although it is worth considering how much information you would want your technical support person to see. The IT security coordinator could be an alternative person. It is safest if everyone keeps their password secret.

What should be done about it?

- ___ Staff policy developed on levels of access to electronic data and systems.
- ___ Staff have created personal passwords to access appropriate level.
- ___ Passwords are kept secure.
- ___ Consideration given to changing passwords periodically.

3.4 Disaster recovery plan

What does this mean?

This is a written plan which explains what should be done when the computer system goes down. It is sometimes called a business continuity plan. Having a back-up of your data is an essential component of the recovery plan, but the procedure for back-ups is dealt with separately in this Guideline.

Some of the functions which need to continue when a computer 'disaster' occurs are:

-] making appointments for patients;
-] issuing patients with invoices and receipts;
-] enabling the doctors to provide adequate clinical care while not having access to electronic medical records;
-] knowing who to phone for technical advice on getting the system operational again;
-] knowing how to restore data using the back-up medium, and, together with technical support, ensuring that computer hardware and software are restored to normal working conditions; and
-] outlining any of the additional roles that staff might need to undertake while the 'disaster' is active.

Disasters can be due to a number of causes including human error, hardware failure, software glitches and interruptions to the power supply. There can also be major natural disasters, but these might be beyond the scope of this Guideline.

A disaster recovery proforma can be found in Appendix C. It should be reviewed at specified time intervals, e.g. annually or if something changes such as the back-up medium or procedure.

Why is it important?

Disasters don't happen very often. But when they do, they are – well, disasters! Unless you have planned for them, of course. A disaster in our terms means that the computer system has gone down and you have to revert to a paper-based system. A disaster recovery plan will help to minimise the disruption, the risk to the business, and the risk and inconvenience to the patient. It is therefore vital to define the critical functions for which computers are used in your practice.

What should be done about it?

- ___ Disaster recovery plan developed.
- ___ Disaster recovery plan tested at specified intervals (e.g. when a procedure changes, or at least annually).
- ___ Disaster recovery plan updated at specified intervals (e.g. when a procedure changes, or at least annually).

3.5 Consulting room and 'front desk' security

What does this mean?

Data security in the consulting room is more about doctors' behaviour than technical matters. For example, some doctors like their computer screens to be clearly visible to their patients during consultations.

However, doctors will have to decide if there might be sensitive information on the screen which should not be seen. Examples include parents seeing a sensitive past history of their teenage child such as a sexually transmitted disease, or patients viewing the clinical record of the person previously consulted.

Similarly, receptionists need to be careful that patients do not have visual access to confidential information on computer screens at the 'front desk'.

There are various methods by which the information can be kept confidential. Some have to do with screen positioning, but screensavers and the use of a function key which instantly closes down an open file are useful technical options.

A related matter is the need for a practice policy on the appropriate use of email with patients. Although 'e-consultations' are currently being conducted, most GPs should beware providing specific medical advice to individuals via email. It is also not advisable to send out clinical data without encryption. A suggested email and Internet policy can be found in Appendix D.

Why is it important?

This is essentially a privacy issue. Patients have the right to have their medical records kept confidential, and doctors need to take steps to ensure that this applies. This is important even if it appears unlikely that patients will maliciously use the information they happen to access.

Simply considering who should be able to view a screen, and using screensavers which appear with minimal delay (for example, after one minute of lack of computer use), should make this an easy matter to deal with. Password protected screensavers can be considered, but most would find this too cumbersome and not essential.

Another useful option is to create a desktop shortcut which turns on the screensaver immediately, or other automated privacy protection measures such as a function key which instantly clears the screen.

What should be done about it?

- ___ Practices should be aware of the need to maintain appropriate confidentiality of information on computer screens.
- ___ Screensavers or other automated privacy protection device enabled.

B Technical issues

3.6 Back-ups

What does this mean?

Data can be lost through human error, software crashes and hardware problems. It is critical to make regular back-ups of all your data in case any of these occur. In order to do a back-up, three things must be considered:

-] your back-up procedure;
-] back-up medium and software to be used; and
-] how your back-up data can be restored.

Restoration is really a part of a disaster recovery plan and has already been covered in a previous section. The recovery plan includes who phones the technical support person, who reinstalls the operating and application software, who reloads the data and what the practice should do to keep functioning in the meanwhile.

You will have to ask your technical support person about back-up software and hardware although you will want the back-up process to be as automated as possible. There are various types of back-up media which include DVDs, CD-ROMs, magnetic tape, zip drives, memory cards and portable hard disks. The use of RAID hard drives also merits consideration.

A related matter is the archiving of files that are no longer active. Remember that you might have to refer to this data in the future when computer hardware and software are quite different. Make sure that you 'future proof' your archived material so that it remains accessible.

Why is it important?

Having a successful back-up procedure is 'mission critical', that is, it is absolutely essential. Loss of patient financial data will cost the practice severely, and the loss of clinical data will be a significant time waster if records have to be reconstructed. In some cases, patients might be put at risk, for example, if previous medical conditions or drug allergies are no longer known about, particularly when the information has only been captured electronically.

As we become more dependent on computers, back-ups become a high IT security priority; they are one of the most important, if not the most important, items in this Guideline.

What should be done about it?

- ___ Back-ups of data done daily.
- ___ Back-ups of data stored offsite.
- ___ Back-up procedure tested (by performing a restoration of data) at specified intervals.
- ___ Back-up procedure included in a documented disaster recovery plan.

3.7 Viruses

What does this mean?

Viruses are programs that cause varying degrees of havoc with computer systems. They are generally 'caught' while communicating electronically with the outside world via email or the Internet. However, they can be transmitted via floppy disks, CD-ROMs and other portable media. There are various types of 'viruses' which are more correctly called 'malicious code' and they include viruses themselves, worms and trojan horses. They can cause minor annoyances or catastrophic system crashes.

The risk of virus infection can be minimised by two means:

-] having a process in place which minimises the risk of downloading a virus; and
-] using regularly updated anti-viral software.

Use of some software or email programs can increase the risk of downloading a virus and may also expose the computer to other security risks. People should ensure their computers are kept up-to-date with current versions and the latest security patches for the software they use.

There are other sorts of programs which can be considered together with viruses. These are spyware and spam. The former refers to small programs which download themselves onto a computer while you are viewing a web page. They can transmit information about your use of the computer to other sites. Spam is nuisance email. Spyware and spam can be annoying, are potentially threatening and can lead you to inadvertently broadcasting confidential information.

Procedures for minimising the risks associated with malicious code can be found in Appendix D.

Why is it important?

Viruses interfere with computer systems and can cause the whole system to crash. The more time one spends on the Internet, especially with a permanently connected broadband, the more likely one is to download viruses. This can have a major impact on the practice, especially if financial data are lost or altered. Viruses can also impede access to the Internet by clogging up the network and can damage the reputation of a practice if the virus distributes itself to everyone in the practice's electronic address book.

What should be done about it?

- ___ Anti-viral software installed on all computers.
- ___ Automatic updating of viral definitions enabled (daily if possible).
- ___ Staff trained in anti-viral measures as documented in the policies and procedures manual.

3.8 Firewalls

What does this mean?

A firewall is an electronic mechanism that blocks unauthorised access into a computer system. These can be in the form of software or hardware. Various programs, some of which are freely available on the Internet, can be installed to protect 'hackers' from getting into your computer network. Similarly, hardware can be added to your computer system so that it acts as a protective device between your computer and the Internet. It stops the inbound (and sometimes the outbound) passage of certain packets of data and can prevent unauthorised access from specific sites.

Unless you are using a standalone computer, it is advisable to install a hardware firewall for extra security. Another major advantage of hardware firewalls is that they provide a hub for a local area network.

Why is it important?

Hackers can steal information and can cause mischief within your computer system and this can lead to the loss of data. You should consider the need for a firewall in the same category as the need for anti-viral protection. They are essential for the long-term preservation of your data. Firewalls will help prevent patient information from appearing on the Internet.

Firewalls are essential for anyone using the Internet. Like viruses, unwanted intruders can crash your system. You might think it improbable that others would want to steal your data, but it is less likely that you will be specifically targeted by hackers than you being 'discovered' by their use of programs which 'roam' the Internet until they randomly find vulnerable computers (technically, those with open 'ports'). You would be surprised how often these programs will intrude. For those who spend a significant amount of time on the Internet, intrusions occur at least once a day, and often several times daily.

What should be done about it?

- ☐ Hardware and/or software firewalls installed.
- ☐ Hardware and/or software firewalls tested.

3.9 Network maintenance

What does this mean?

Computer and network maintenance is like servicing your car: you need to do some things routinely to prevent it from breaking down. It includes looking after the equipment itself, hardware and software. More specifically, maintenance includes the following:

-] physical protection of your computer, e.g. protection against theft by the use of a lock;
-] protecting your computer against environmental damage such as heat, water and dust; and
-] keeping your computer programs running efficiently.

This might mean performing 'maintenance' work on regular occasions such as: running a program which 'cleans up' file system errors and temporary files; running a 'defragmentation' utility program; updating software; and downloading operating system and other program patches. Computers can crash if they have inadequate residual memory left on their hard drives. You will most likely need technical advice on how to keep your computer functioning efficiently. Software also needs to be installed and maintained in accordance with the vendor's guidelines.

Installing an Uninterruptible Power Supply (UPS)

A UPS is a device that contains batteries to enable computers to shut down smoothly when the main electricity supply suddenly cuts out. This is important so that data being processed when the blackout occurs is not lost. The UPS will also help with power surges which can cause hardware damage. However, they do not generally generate sufficient power during a prolonged blackout. That requires an electric generator which is simply not appropriate or affordable for most practices. Your technical support person will advise you whether theoretical solutions are practical for you, such as the use of an 'inverter' which operates from a car battery.

Installing surge protectors on non-critical workstations

On the main sever a UPS should be installed, but on other workstations in the practice, a simple surge protector will suffice.

Why is it important?

The importance of some routine maintenance issues is self-evident. For example, not physically securing your server so that one day it is stolen will test your patience severely.

Power surges (or blackouts) can crash your system. A prolonged blackout is simply a disaster, and there is no reasonable protection against it as most practices cannot afford electric generators.

A UPS is a good insurance policy, at least to protect your server. Other housekeeping procedures such as running a file 'defragmentation' utility program and not spilling coffee on your keyboard do help with the smooth functioning of your computer system.

What should be done about it?

- ___ Computer hardware and software maintained in optimal condition (includes physical security, efficient performance of computer programs, and program upgrades and patches).
- ___ Uninterruptible Power Supply installed (to at least the server).

3.10 Secure electronic communication

What does this mean?

Patient information which is being exchanged between healthcare providers should be kept private. It is technically possible for a third party to intercept and read emails which were intended for someone else; more likely, sensitive information can be sent astray by inadvertently clicking on the wrong person in an electronic address book.

There are two aspects to secure electronic communication:

-] encryption;
-] authentication.

Encryption means that data is electronically 'scrambled' so that it cannot be read unless the information is unencrypted. Authentication means that one can verify whether the sender is who they say they are. This is done by using electronic 'keys' (i.e. identifying code).

There are currently a number of ways that data can be encrypted. One method, made available by the Department of Health and Ageing at no cost to the user, is called Public Key Infrastructure (PKI). There are other cost-free systems available. Unfortunately, there is not at the present time one system which is used universally, although it is important to choose one that conforms with current security standards, e.g. those published by Standards Australia.

Why is it important?

To prevent information being read by an unintended recipient, it is best to encrypt sensitive data. Clearly, phone calls can be tapped, faxes can go to the wrong person and letters can be opened by a range of people at a practice. Why is it then that electronic security sets higher standards? One reason is that electronic transmission makes it easier to inadvertently broadcast information to a wider audience.

Encryption is technically easy for the end-user, once the system has been installed. It is a simple click within an email program. However, until practices have access to encryption, it is best not to send confidential data via email or the Internet.

What should be done about it?

- ___ Encryption systems considered.
- ___ Encryption used for the electronic transfer of confidential information.

FOUR Conclusion

Remember that there are three components to computer security:

Availability – the data should be available when you want it. If the computer system crashes during normal clinic hours, then you have a disaster on your hands. Unless you have a suitable contingency plan, your business might come to a standstill, and patient care could suffer.

Integrity – the data should remain intact.

Access – only certain people should have access to sensitive patient clinical and financial information.

It is obvious that computer security is an important issue in the running of a practice and for patient care. However, because things do not go wrong all the time, it is an area which may be ignored until it is 'too late'.

This Guideline and Checklist will help you to maintain reasonable computer security standards in your practice. It is a fact of life that no-one can know everything, and this Guideline does not attempt to explain all the technical aspects of security that need to be known in order for your practice to have an appropriate system. You will need expert and up-to-date technical advice for that.

Improving computer security in your practice is about change management. That is why it is important that someone at the practice takes responsibility for computer security issues. They need to know who and when to call for expert advice. They also need to see that staff and GPs are aware of computer security issues, that security protocols are followed, and that appropriate training takes place. Does everyone in the practice know that the last person to leave the clinic in the evening is expected to lock the door? Similarly, everyone in the practice needs to be aware of the importance of computer security.

Yes, there is a financial cost. This Guideline has been developed by people who are very aware of the constraints faced by GPs. Computers are now a part of general practice and they must be built into its cost structure. Computer security is therefore not an option: it is, to use IT jargon once more, *mission critical*.

FIVE Further information

You can learn more about computer security from the following sources:

-] the General Practice Computing Group website (**www.gpcg.org**); and
-] your local division of general practice.

Specific advice on how to ensure that your own practice computer system is adequately secured should be sought from appropriately qualified people. Your computer supplier should be able to give you this advice. Just as GPs require an accountant, practices will have to have an IT technical support person to help with computer issues, including security.

As privacy of personal information is closely related to data security, you might find the following resources useful as well: the Handbook for the Management of Health Information in Private Medical Practice (written by the Royal Australian College of General Practitioners and the Committee of Presidents of Medical Colleges, with the support of the General Practice Computing Group) and the Australian Medical Association Privacy Kit. Details are available at the RACGP and AMA websites.

SIX Appendices

Appendix A:	Practice computer security coordinator role description	19
Appendix B:	Computer security policies and procedures manual proforma	20
Appendix C:	Disaster recovery plan	22
Appendix D:	Internet and email policy	24
Appendix E:	Computer security terms	26

Please note that a template for the computer security policies and procedures manual can also be downloaded from the GPCG website (www.gpcg.org).

Appendix A

Practice computer security coordinator role description

This person's role will vary in every practice, depending on the IT skills of available staff, the availability of technical support and the interest of other staff members. In some practices the principal GP will take up this role, although it is better if it is delegated to one of the senior administrative staff. Sometimes the practice manager might fulfil this role. Some of the tasks can be shared by two or more people. Most likely, the practice IT coordinator will also be responsible for computer security.

Please modify this role description to suit your purposes.

General characteristics

This position suits someone (or two people who share the position) who is enthusiastic about computers. They need not have advanced technical knowledge, although they should be reasonably comfortable with basic operating systems and relevant application software. They have to have management skills and be able to develop computer security policies in consultation with others in the practice. Quite likely, they will also be the general IT coordinator for the practice.

Tasks

The computer security coordinator will:

-] oversee the development of documented IT security policies and procedures;
-] oversee the development of a computer disaster recovery plan;
-] ensure that there are test runs of disaster recovery procedures at specified intervals;
-] ensure revision of the disaster recovery plan at specified intervals;
-] keep an IT assets register (hardware, software, manuals and technical support);
-] ensure that there is an access control policy in place;
-] ensure that staff is aware of maintaining password security;
-] ensure that screensavers are in place;
-] establish a routine back-up procedure;
-] ensure that restoration of data is tested at specified intervals;
-] ensure that anti-viral software is installed on all computers and the virus definitions are updated daily;
-] ensure that technical advice is sought and acted upon for the installation of appropriate firewalls;
-] ensure that computers, especially the server, are adequately maintained;
-] ensure that the computer system can deal with fluctuations in the power supply;
-] investigate the appropriate means of encrypting confidential information prior to electronic transfer;
-] coordinate the application, use and storage of digital certificates, ensure the practice understands encryption; and
-] arrange computer security training for members of the practice.

Appendix B

Computer security policies and procedures manual proforma

This manual should contain all the policies and procedures relating to the security aspects of the installation and use of computers and electronic communication by staff. Responsibilities for each component of computer security should be clearly defined, the policies should be clear, and the procedures should contain simple instructions that are easy to follow.

Some of the other appendices in this Guideline (e.g. the disaster recovery plan and the email/Internet policies) will form a part of the overall computer security manual. The manual itself is really a part of a broader IT policies and procedures manual, which is in turn part of a practice policy and procedures guide.

It goes without saying that it is more important to think through and discuss the contents of the manual within the practice and to ensure its implementation, than to allow it to sit on a shelf.

A template on computer security policies and procedures, to which you can add information and modify to suit your needs, can be downloaded from the GPCG website (www.gpcg.org).

1 Practice computer security coordinator

A practice computer security coordinator should be appointed and their role defined and acknowledged by the practice. (See Appendix A.) The responsibilities of other staff with regard to computing should also be defined. This will provide the basis of determining the level of access to each system.

The practice computer security coordinator, who might be the general IT coordinator as well, should help ensure that staff is aware of the principles of computer security and is appropriately trained.

2 Disaster recovery plan

A disaster recovery plan should firstly cover the critical functions of the practice so that it can continue without major disruption or risk to the patients and staff. Secondly, it should contain the information necessary for returning the practice to its normal state.

The plan will involve the creation of an asset register which documents the hardware and software owned by the practice, where the computer disks and manuals can be found, and who to phone for technical support. Maintaining a log of faults as they occur helps in dealing with computer problems, including 'disasters'. (See Appendix C.)

3 Back-ups

Details of back-up and recovery procedures should be documented. The back-up procedure is a key component of the disaster recovery plan. Ensure that back-up media are taken off site when the practice is closed. Record which members of staff perform the back-ups and automate as much of the procedure as possible. (See Appendix C.)

4 Internet/email

Provide a clear statement of the do's and don'ts for staff having access to email and the Internet at the practice. (See Appendix D.)

5 System access

Provide access to systems in line with responsibilities outlined in the role description above. Each staff member should create his or her own password(s) for access. Passwords should not be written down where they can be obtained by other staff or persons who have access to the premises. The system administrator's password should never be divulged to non-authorised persons.

6 Consulting room and 'front desk' security

Record the practice policy on the use of screensavers and other precautions, such as positioning of the monitors, to prevent unauthorised viewing of patient records and other confidential information.

7 Virus checking

Document virus checking software and procedures. (See Appendix D.)

8 Firewalls

Provide details of firewall hardware and software and their related procedures.

9 Maintenance

Document details of routine maintenance to be performed on the computers in the practice. This includes hard disk 'clean-ups' (e.g. by a 'defragmentation' utility program) and physical security of the network.

10 Secure electronic communication

Record the practice policy on electronic communication of patient records and other confidential information. This involves encryption and its associated procedures.

Appendix C

Disaster recovery plan

What should a disaster recovery plan cover?

A disaster recovery plan should first cover the critical functions of the practice so that it can continue without major disruption to the patients and staff, thus ensuring that no patient is put at risk and that the ongoing viability of the practice is maintained. Secondly, it should contain the information necessary for returning the practice to its normal state. This template can be downloaded from the GPCG website (www.gpcg.org).

1 Prepare a disaster recovery plan

Make a list of the critical practice functions:

-] making appointments;
-] billing patients; and
-] providing adequate clinical care.

Discuss with staff how each of these is to be handled in the case of a disaster and how the switch to a paper-based system is to occur.

Decide who is in charge of the recovery, and who is responsible for each function.

2 Create an asset register

Create an 'asset register' which will consist of:

-] hardware and software details, including documentation of their location within the practice;
-] network information; and
-] the names and contact details of technical support personnel.

3 Create a 'fault log book'

Document in a log book computer faults, errors or full-blown disasters as they occur so that the practice can learn how to combat new 'disasters'. The log might include how to deal with:

-] a virus on the system;
-] failure of the server;
-] failure of a computer to boot up;
-] failure of an individual computer or network component; and/or
-] failure to connect to the Internet.

Document the disaster recovery procedure in a step-by-step manner

Coordinating the disaster recovery

If available, the computer security coordinator will do this. The coordinator will firstly put in place the disaster recovery plan for administrative and clinical functions of the practice. The coordinator will then make a rapid and provisional investigation on what caused the crash and contact technical support.

Implementing the restoration plan

Decide on which personnel will be involved. The practice's administrative (appointment and billing) and clinical functions will be re-established before the computer restoration process commences. Locate the most recent back-up and undertake an appropriate restoration (either complete or partial software and/or hardware replacement).

Reflecting after recovery

Review the reasons for the disaster and the methods used to restore function with the aim of refining the process.

Appendix D

Internet and email policy

Policies for the use of email and Internet

-] Develop a policy on what constitutes reasonable private use of email and the Internet by staff during office hours (i.e. use which does not interfere with work efficiency);
-] Ensure that staff understand which websites are not appropriate to view at the practice (e.g. pornographic or other offensive sites);
-] Make staff aware that emails sent from the practice to anyone at all which might be construed as offensive or sexually harassing, are not permitted;
-] Explain to patients (e.g. on either the practice website - if you have one - or in the practice's information brochure) the following: that individual medical advice cannot be provided via email; that all electronic data is subjected to privacy principles; and that no confidential information can be transmitted without encryption.

Procedures for the safe use of email and the Internet

1 Protection against viruses

-] Install and use antivirus software;
-] Keep this software active at all times;
-] Keep it up-to-date using automatic updates. Periodically, check manually that it is up-to-date;
-] Apply patches to operating and application programs following technical advice;
-] Do not download or open any email attachments where the sender is not personally known to you;
-] Do not open unexpected email even from people known to you as this might have been spread by a virus;
-] Do not open *.exe or *.bat attachments;
-] Use an antivirus mail filter to screen email prior to downloading;
-] Do not use 'preview' in your email program as this automatically opens your email when you click on the header;
-] Save attachments and check for viruses before opening or executing them;
-] Do not run programs directly from websites. Download files and check them for viruses first;
-] Enable security settings in your Internet browser to medium or high;
-] Consider using Internet browsers and email programs which are more secure than some of the more frequently used versions.

2 Protection against the theft of information

-] Do not provide confidential information by email; only do so via the Internet when the site displays a security lock on the task bar;
-] Use a second, non-critical email address when registering personal details where you are not completely sure of the site's security;
-] Do not inform people of your email password.

3 Protection against hackers

-] Install hardware and/or software firewalls between computers and the Internet (following technical advice);
-] If you install a software firewall, ensure that the practice knows how to use it;
-] Ask the technical support person to test the firewall periodically and update it as required;
-] If you are using a wireless network, seek technical advice on how to prevent others with similarly equipped computers hacking into your practice's network.

4 Protection against spam

-] Do not reply to spam mail;
-] Never try to unsubscribe from spam sites;
-] Remain eternally vigilant: do not provide confidential information to an email (especially by return email) no matter how credible the sender's email seems (e.g. as if it were from your bank);
-] Consider using a spam filtering program.

5 Protection against spyware

-] Learn how to recognise (and delete) spyware;
-] Don't accept certificates or downloads from suspect sites;
-] Consider installing anti-spyware software.

6 Encryption of patient information

-] Do not send patient information or other confidential data via email unless you are using encryption;
-] Encrypted files are not automatically checked for viruses. They have to be saved, decrypted and then scanned for viruses before being opened.

7 Backing up email and Internet favourites or bookmarks

-] If you rely on information held in your email program make sure that it is backed up with the rest of your data;
-] If you have a useful list of Internet favourites or bookmarks make a back-up of the list.

Appendix E

Computer security terms

The following is a glossary (based on the original GPCG Security Guideline) of key technical terms relevant to computer security.

Boot password (also called power-on password) – a password that must be entered when a computer is started and prior to the operating system starting. If an incorrect password is entered, the computer will not continue loading. Boot passwords are used as an additional security mechanism. Another type of boot password can be used to prevent unauthorised access to the computer's BIOS settings.

Client – a client is a computer that requests services from a computer called a server. For example in a network environment, a client would be your personal computer connected to the network. The client might request print services from a print server when you want to print a document or a file server when you want to access files.

Dial-up connection – a widely used method of accessing the Internet. A dial-up connection uses ordinary phone lines to connect one computer to another via a pair of modems.

Differential back-up – a type of back-up that only includes files that have been modified or added since the previous full or incremental back-up. However, the files are not marked as having been backed up.

Digital certificate – a digital certificate is a mechanism used to verify that a user sending a message or data is who he or she claims to be.

Encryption – encryption is the process of converting plain text characters into cipher text (i.e. meaningless data) as a means of protecting the contents of the data and guaranteeing its authenticity.

Firewall – A firewall is used to provide added security by acting as a gateway or barrier between a private network and an outside or unsecured network (such as the Internet). A firewall can be used to filter the flow of data through the gateway according to specific rules.

Full back-up – a back-up of all files residing on a computer/server hard drive. The files are marked as having been backed-up.

Hard disk/drive – a hardware device used for storage of programs and data on a computer. A computer may have more than one hard drive.

Hardware – physical component of a computer, such as a monitor, hard drive, or Central Processing Unit (CPU).

Incremental back-up – a type of back-up that only includes files that have been modified or added since the previous full or incremental back-up. The files are marked as having been backed-up.

ISP (Internet Service Provider) – an ISP is a company that provides access to the Internet for companies or individuals. You typically connect to the ISP using a modem and dial-up, or a broadband connection such as ADSL.

Mail server – a server used to forward email, whether the email is sourced internally or externally and whether the destination email address is internal or external.

Mirrored hard disk – this is an additional hard disk that contains a mirror image of the original disk. If the original disk fails or becomes faulty, the mirrored disk can then be used.

Modem – acronym for Modulator/Demodulator; it's a device used to transmit computer information across the telephone network (by converting computer or digital signals into analogue signals and vice versa). It can be used to allow users to connect to the office network whilst they are away from the office (e.g. at home or travelling), or to connect computers to the Internet via a dial-up or broadband connection to an ISP.

Network – a collection of connected computers and peripheral devices, used for information sharing, electronic communication, etc.

Network Access Point – this refers to a physical socket via which a computer can be connected to the network.

Network Drive – in the simplest case, a network drive is a complete hard disk/drive on a network server that is made available to users on the network. Note that a hard drive on a network server can be logically split into multiple drives, with one physical hard drive. Each logical drive is allocated a letter of the alphabet, such as G, H, etc. Logical drives can be used as an access control mechanism, by only allowing certain users on the network to access the data on the logical drive.

Network Interface Card (NIC) – also called a Network Adapter, a NIC is a hardware device (located inside the computer) that allows the computer to connect to a network and communicate with other computers on the network.

Network Operating system – software that controls and manages how the network operates, such as authenticating users by requiring them to enter a username and password to access the network, control printing, etc.

Non-repudiation – this term means that you can't deny having performed a transaction. For example, if you send an email to your bank asking them to transfer money out of your account, non-repudiation means you cannot later deny having sent the email. Use of encryption and digital certificates provides non-repudiation capabilities.

Operating system – software that controls how a computer and its hardware and software components work. For example, Macintosh TM, Windows TM and Linux are types of operating systems.

Peripheral device – a device attached to a network or a computer, such as a modem or a printer.

Proxy/Proxy server – in the context of accessing the Internet, a proxy server typically acts as a control point by being the central point of access for users to the Internet.

RAID (Redundant Array of Independent Disks) – a second disk drive which acts as a back-up to the main hard drive by producing a mirror image copy of the original.

Reboot – when you restart your computer. You might be required to reboot your computer in some instances, for example, after you have installed new software to enable the changes to take effect.

Registry – this contains system configuration information and controls how your computer operates. It should never be tampered with unnecessarily as this can lead to your computer not functioning properly.

Router – a device that provides connectivity between networks, for example, between your internal network and the Internet. A router forwards data from one network to the other and vice versa.

Server – this is typically a computer in a network environment that provides services to users connected to a network (or 'clients'), such as printing, accessing files, running software applications. A server can be used as a central data repository for the users of the network.

Software – a program (or group of programs) which performs specific functions, such as word-processor or spreadsheet programs.

Spam – unsolicited email. Often it is simply nuisance email, but it can entice you to provide confidential personal information, e.g. banking details.

Spyware – programs which are downloaded from the Internet on to your computer (sometimes without your knowledge) to covertly send back information to the source, e.g. your personal details.

Standalone computer – this is a computer that is not connected to a network or to other computers.

Trojan Horse – Trojan Horses are unauthorised programs hidden within authorised programs.

URL (Uniform Resource Locator) – in the simplest case, it is the address for an Internet web page, such as <http://www.gpcg.org>.

Virus – a program that can create copies of itself on the same computer and on other computers. They corrupt programs.

Worm – worms are much like computer viruses, but do not attach themselves to other programs.

Author

A/Prof Peter Schattner

Department of General Practice
Monash University
867 Centre Rd
East Bentleigh Vic 3165

p: 03 8575 2222

f: 03 8575 2232

e: peter.schattner@med.monash.edu.au



MONASH University
The Department of General Practice

In affiliation with the:
Department of Rural Health,
The University of Melbourne
Monash Division of General Practice