



The Royal Australian
College of General
Practitioners

Computer security guidelines

A self assessment guide and checklist for general practice

3rd edition





The Royal Australian
College of General
Practitioners

Computer security guidelines

A self assessment guide and checklist for general practice

3rd edition

Computer security guidelines

A self assessment guide and checklist for general practice
3rd edition

Disclaimer

The information set out in this publication is current at the date of first publication and is intended for use as a guide of a general nature only. This publication is not exhaustive of the subject matter. Persons implementing any recommendations contained in this publication must exercise their own independent skill or judgement or seek appropriate professional advice relevant to their own particular circumstances when so doing. Compliance with any recommendations cannot of itself guarantee discharge of the duty of care owed to patients and others coming into contact with the health professional and the premises from which the health professional operates.

Whilst the text is directed to health professionals possessing appropriate qualifications and skills in ascertaining and discharging their professional (including legal) duties, it is not to be regarded as definitive technical advice and, in particular, is no substitute for a full investigation and consideration of a particular environment by an expert in the field in reaching a final recommendation tailored to personal needs and circumstances.

Accordingly The Royal Australian College of General Practitioners and its employees and agents shall have no liability (including without limitation liability by reason of negligence) to any users of the information contained in this publication for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of any person using or relying on the information contained in this publication and whether caused by reason of any error, negligent act, omission or misrepresentation in the information.

Published by
The Royal Australian College of General Practitioners
College House
1 Palmerston Crescent
South Melbourne VIC 3205 Australia
Tel 03 8699 0414
Fax 03 9696 0400
Email ehealth@racgp.org.au
www.racgp.org.au

ISBN: 978-0-86906-322-4

Published October 2010

Acknowledgments

The RACGP *Computer security guidelines: a self assessment guide and checklist for general practice* (3rd edition) is based on the *Computer security self-assessment guideline and checklist for general practitioners* (2nd edition), published in 2005 by the General Practice Computing Group, and on previous work by The Royal Australian College of General Practitioners and the Australian Medical Association.

The Royal Australian College of General Practitioners gratefully acknowledges the following organisations and people who were involved in the development, review, writing and funding of the 3rd edition:

The National E-Health Transition Authority

Associate Professor Peter Schattner

Associate Professor Ron Tomlins

Dr John W Bennett

Dr Nathan Pinskiar

Judy Evans

Namanita Muss

The RACGP e-health Standards and e-health Working Groups

Dr Trish Williams (PhD)

Contents

<i>Preface</i>	<i>1</i>
<i>1. Introduction</i>	<i>4</i>
<i>1.1 How should you use this guide?</i>	<i>4</i>
<i>2. Computer security checklist</i>	<i>5</i>
<i>3. The 10 item computer security guide</i>	<i>6</i>
<i>Organisational issues</i>	<i>6</i>
<i>3.1 Practice computer security coordinator</i>	<i>6</i>
<i>3.2 Practice security policies and procedures manual</i>	<i>8</i>
<i>3.3 Access control and management</i>	<i>9</i>
<i>3.4 Business continuity and disaster recovery plans</i>	<i>11</i>
<i>Technical issues</i>	<i>12</i>
<i>3.5 Backup</i>	<i>12</i>
<i>3.6 Malware and viruses</i>	<i>14</i>
<i>3.7 Network perimeter controls</i>	<i>15</i>
<i>3.8 Portable devices and remote access security</i>	<i>16</i>
<i>3.9 Computer and network maintenance</i>	<i>18</i>
<i>3.10 Secure electronic communication</i>	<i>20</i>
<i>4. Conclusion</i>	<i>23</i>
<i>Appendices</i>	<i>24</i>
<i>Appendix A – Practice computer security coordinator role description</i>	<i>20</i>
<i>Appendix B – Computer security policies and procedures manual documents</i>	<i>27</i>
<i>Appendix C – Contractual agreements with technical service providers</i>	<i>30</i>
<i>Appendix D – Business continuity plan</i>	<i>31</i>
<i>Appendix E – Internet and email policies</i>	<i>33</i>
<i>Appendix F – Computer security terms</i>	<i>35</i>

Preface

The use of clinical desktop systems and the electronic management of information has become a vital tool in the delivery of safe and high quality care for patients. Many practices utilise a combination of the skills of their staff and the engagement of external information technology (IT) consultants to install and maintain their computer systems and security. Generally it has not been easy to access appropriate training to develop IT security skills for practice staff and this has meant that staff in general practice have been working without important knowledge and skills in IT. General practice has specific requisites for computer and information security and it can be a challenge to find external security experts and technical service providers who understand the business of delivering care in the general practice environment.

Some of the issues that general practices may face

- Lack of risk analysis. Risk analysis involves reviewing the computer and information security measures and practices and then identifying gaps in security and developing strategies to mitigate security risks. Ensuring that information held on practice computer systems is secure is essential to running a general practice, to maintaining professional responsibilities to patients, and to making sure that practice information is accurate and available when it is needed
- Lack of designated authority. In this situation there is no one person with the designated authority to ensure that all computer function and security processes are documented and followed. This includes a lack of clarity about the role of the external technical service providers and when it is appropriate to engage their services. Computer security requires regular attention at a practice level and all staff need to be aware of their responsibility in protecting practice information. Unfortunately, staff position descriptions may not reflect responsibility for information security and often staff are not provided with professional development to gain the required skills in IT and security awareness
- Lack of data management processes. This is when backup procedures are poorly documented and not appropriately tested. It is important to ensure that the backup system functions correctly and that data can be recovered if there is an incident such as a server failure
- Lack of business continuity and disaster recovery planning. A lack of a properly documented business continuity plan or disaster recovery procedures means that in the event of a 'disaster' there is an inadequately planned response, which may lead to inconvenience and potential loss or corruption of information
- Lack of password security. Poor password management means it might be hard to ascertain who within a practice has entered or altered data, including clinical records. It also leaves the practice vulnerable to unauthorised system and information access
- Lack of security 'culture' and leadership. It is important that one or more people within the practice take responsibility for computer security. It is beneficial to promote a culture of security within the practice. This includes educating practice staff about the risks to the information systems and the maintenance of practical policies that direct staff in their management of the security risks.

Preface continued...

The RACGP *Computer security guidelines: a self assessment guide and checklist for general practice* (3rd edition) places greater emphasis on the roles of the personnel involved with protecting practice information. These guidelines detail the knowledge needed by practice staff, the basic security processes that are required, and indicate when it may be necessary to engage external IT and security expertise.

This 3rd edition of the security guidelines takes into account the increased use of laptops, remote access devices (eg. personal digital assistants (PDAs), USB flash drives, and removable hard drives) and wireless (Wi-Fi) connections. The practice server and network now assumes an increasingly vital role, clinical and practice management software is more complex, and there is widespread uptake of broadband internet and secure messaging.

Note: The security guidelines 3rd edition do not address patient access to medical records or the management of pathology and/or radiology results. Staff need to be aware of the RACGP Standards for general practices (4th edition) that detail the overarching professional standards related to patient access to information and the associated security and privacy issues. The principal aim of the computer security guidelines is to highlight the processes, policies and procedures that will protect your practice's information.

Healthcare Identifiers

General practice has entered the era of e-health (e-health is the use in the health sector of digital data that is transmitted, stored and retrieved electronically in support of healthcare, both at the local site and at a distance. The World Health Organization's definition is at www.who.int.) Secure transmission of data and patient identification will be underpinned by the allocation of unique healthcare identifiers, which are 16 digit numbers to be used to identify healthcare providers, healthcare organisations and individuals. Unique healthcare identifiers will better support the management of health information and the communication of health information between healthcare providers and healthcare organisations.

Three types of healthcare identifiers will be assigned by the Australian Healthcare Identifiers (HI) Service:

- Individual Healthcare Identifier (IHI) – for individuals receiving healthcare services
- Healthcare Provider Identifier – Individual (HPI-I) – for healthcare professionals and other health personnel involved in providing patient care
- Healthcare Provider Identifier – Organisation (HPI-O) – for organisations (eg. the hospital and/or general practice) where healthcare is provided.

The identifiers will be assigned and administered through the HI Service. A key aim of the healthcare identifier is to ensure individuals and providers have increased confidence that the right health information is associated with the right individual at the point-of-care.

Preface continued...

Healthcare providers who are identified with an HPI-I, or an authorised employee, can access the HI Service to obtain the LHI of a patient being treated. This means general practice staff will require training on the implications of healthcare identifier numbers and how they are assigned.

For further information

- RACGP *Standards for general practices* (4th edition) (www.racgp.org.au/standards)
- The Australian Government Practice Incentives Program (PIP) eHealth Incentive requirements (www.medicareaustralia.gov.au/provider/incentives/pip/index.jsp)
- The National Privacy Principles (www.privacy.gov.au)
- Standards Australia. HB 174-2003 Information security management – implementation guide for the health sector. Sydney: Standards Australia International, 2003. (Note: This handbook is about to be updated)
- International Organization for Standardization. ISO27799 Health Informatics – Information security management in health using ISO/IEC 27002 (2008) (www.iso.org)

It is a challenge to produce guidelines that will suit all practices. The computer systems requirements of large practices differ from those of solo practices; practices vary in their level of staff computer skills; 'paperless' practices will have different needs to those with a hybrid system; and rural practitioners may have less opportunity for obtaining technical support. It is therefore important for all practices to apply a risk analysis of their particular systems and security needs, and to document the policies and procedures to which staff will need to adhere, so that there is assurance of availability, integrity and confidentiality of data held within the practice's clinical and administrative systems.

1. Introduction

Maintaining information security is vital and requires planning and technical knowledge. These guidelines have been developed to provide a framework to enable practice staff to work through the elements of computer security and information management. It is not a technical manual, but will assist practices to understand what is needed in order to put in place a series of computer security strategies.

When reading these guidelines, bear in mind that it is about computer and information security and refers to:

- availability of information – available and accessible when needed
- integrity of information – not altered or destroyed in unauthorised ways
- confidentiality of information – only authorised people can access the information.

1.1 How should you use this guide?

There are three sections to these guidelines:

- A checklist that will determine whether you have established reasonable computer security measures in your practice to protect the information the practice uses, records and is responsible for
- A guideline for each security risk category. Each category section is divided into three subcategories to assist in understanding and implementing the correct action:
 1. What does this risk category mean? This describes the risk in some detail
 2. Why is it important? This explains why practices should spend time and money on protection from the risk and the potential consequences of ignoring the recommendations
 3. What should be done about it? This outlines the step-by-step processes which should be followed in order to manage the risk
- A series of proformas provide useful lists of information such as how to produce a business continuity and disaster recovery plan. The policies and procedures document is available as a template you can download from the RACGP website (www.racgp.org.au/ehealth/csg). By adding information relevant to your practice, you can incorporate this template directly into your practice's policies and procedures manual.

2. Computer security checklist

This is a checklist to provide an overall assessment of the basic computer security processes currently in place. The checklist should be reviewed annually. These guidelines describe each item in the checklist in more detail.

IT category	Tasks	Has this been implemented? (Tick if yes and add date)
Practice computer security coordinator	Practice computer security coordinator/s appointed (insert name) Practice computer security coordinator/s' role documented Computer security training for practice computer security coordinator/s provided Practice computer security coordinator/s' role reviewed (yearly)	_____ ☐ __/__/__ ☐ __/__/__ ☐ __/__/__
Practice computer security policies and procedures	Computer security policies and procedures documented Computer security policies and procedures documentation reviewed Staff trained in computer security policies and procedures	☐ __/__/__ ☐ __/__/__ ☐ __/__/__
Access control and management	Staff policy developed on levels of access to data and information systems Staff are assigned appropriate access level Staff have individual passwords which are kept secret and secure	☐ __/__/__ ☐ __/__/__ ☐ __/__/__
Business continuity and disaster recovery plans	Business continuity and disaster recovery plans developed Business continuity and disaster recovery plans tested Business continuity and disaster recovery plans reviewed and updated	☐ __/__/__ ☐ __/__/__ ☐ __/__/__
Backup	Backup of data performed daily, with weekly, monthly and yearly copies retained Backups encrypted Backup of data stored securely offsite Backup procedure tested by performing a restoration of data Backup procedure included in a documented business continuity and disaster recovery plan	☐ __/__/__ ☐ __/__/__ ☐ __/__/__ ☐ __/__/__ ☐ __/__/__
Malware and viruses	Antivirus and antimalware software installed on all computers Automatic updating of virus definitions is enabled on all computers/server Staff trained in antimalware procedures Automatic weekly scans of hardware enabled	☐ __/__/__ ☐ __/__/__ ☐ __/__/__ ☐ __/__/__
Network perimeter controls	Hardware and/or software network perimeter controls installed Hardware and/or software network perimeter controls tested periodically Intrusion activity logs monitored and breaches reported	☐ __/__/__ ☐ __/__/__ ☐ __/__/__
Portable devices and remote access security	Portable devices, memory devices, backup media kept secure Wireless networks and remote access systems configured securely Policy on the use of mobile devices documented	☐ __/__/__ ☐ __/__/__ ☐ __/__/__
Computer and network maintenance	Physical security of the server and network maintained Sensitive screen information kept appropriately confidential (eg. via screen positioning or 'clear screen' function keys) Computer programs maintained (eg. with automatic upgrades and patches, and performance reviewed periodically) Uninterruptible power supply and surge protectors installed	☐ __/__/__ ☐ __/__/__ ☐ __/__/__ ☐ __/__/__
Secure electronic communication	Secure messaging system (involving encryption) used for the electronic transfer of confidential information Safe and secure use of email, internet and the practice website policy developed and reviewed periodically	☐ __/__/__ ☐ __/__/__

3. The 10 item computer security guide

Computer security is more about people and their actions (or inaction) than it is about technical matters. Communication, documentation of processes and identifying appropriate training for staff and GPs is essential to maintaining good computer security. Above all, a 'computer security culture' is required. It is essential that practice staff become aware of the risks to information and the responsibility and contribution they make to maintaining the confidentiality, integrity and availability of that information. All staff need training in the fundamentals of computer security, and staff knowledge and competency in these areas need to be reviewed on a regular basis, at least once per year.

Organisational issues

3.1 Practice computer security coordinator

What does this risk category mean?

The practice computer security coordinator is the person responsible for drawing together the computer security issues that confront the practice – it is very much a leadership role. The computer security coordinator is responsible for managing the training of staff and maintaining staff knowledge of computer security principles and practice, and security policy and procedures. The practice security coordinator might be one of the doctors, a nurse, a senior receptionist or the practice manager. These tasks can be allocated to more than one person in the practice.

Specific tasks include:

- clarifying and documenting the computer security roles and responsibilities of all staff
- writing, reviewing and regularly updating the security policies and procedures manual. This will include policy and procedures on (but not limited to):
 - backup
 - access control
 - internet and email usage
 - malware (eg. virus) protection
 - wireless and mobile connections
 - perimeter controls and intrusion detection (eg. firewalls)
 - physical security (as it relates to the computer systems)
 - disaster recovery plans
 - business continuity plans
 - security management and reporting including:
 - identifying the role of the external IT consultant and when it is appropriate to seek their advice
 - monitoring and ensuring security policies and procedures are being followed
 - vulnerability management and risk assessment

- staff training – training needs identified, completed and documented including:
 - ongoing security awareness education
 - secure messaging usage
- maintenance of the asset register including:
 - hardware
 - software licences and associated installation keys
 - configuration information
 - digital certificate and signature information
 - secure storage of all operating manuals, installation media
 - ensure the practice management is aware of any outstanding security issues and regularly report on security in practice management meetings.

A generic role description for the computer security coordinator is outlined in Appendix A. While many practices now outsource aspects of computer maintenance to IT professionals, a practice computer security coordinator needs to be aware of what needs to be done, even though they may not have the technical knowledge to perform these tasks themselves.

Why is it important?

Clearly documented action plans will minimise the risk of the practice being unable to function normally. The practice security coordinator should ensure that security policies and procedures are developed systematically.

The coordinator's role is primarily to raise computer security awareness rather than to be a technical 'fix-it' person. They should help to engender interest, even enthusiasm, for an IT security 'culture' and to ensure that there is adequate and appropriate training for all staff. They also need to understand that while many aspects of computer security are rightly outsourced to IT companies, certain responsibilities and tasks need to be carried out by practice staff, eg. checks on the backup procedure. The role of the coordinator is to ensure that all practice staff have a clear view of their responsibility and role in protecting the practice's information.

What should be done about it?

- ☐ Practice computer security coordinator appointed
- ☐ Practice computer security coordinator's role description documented
- ☐ Computer security training for coordinator provided
- ☐ Security coordinator's role reviewed (eg. annually) and ongoing training provided.

Note: All practice staff should be aware of their responsibility for information security. While the role of the coordinator is well defined, it should be made explicit in the practice policies the role and responsibilities each member of the practice must assume to ensure the protection of information. Staff awareness of their role in information security is vital to enhance this protection. This includes password management, recognition of errors or abnormal software behaviour, and commitment to practice policy and procedures.

3.2 Practice security policies and procedures manual

What does this risk category mean?

Practices need to document their computer security policies and procedures. A security manual should include:

- the roles and responsibilities of the practice staff (clinical and nonclinical) in relation to protecting the practice's information, and in particular the role of the practice computer security coordinator
- a complete set of policies and procedures for:
 - backup
 - access control and password management (to define the various levels of access for clinical and nonclinical staff)
 - internet and email usage
 - malware (eg. virus) protection
 - wireless and mobile connections
 - perimeter controls and intrusion detection (eg. firewalls)
 - physical security (eg. restricted access to the practice server)
 - a disaster recovery plan
 - a business continuity plan (this is particularly important as it enables the practice to function when the computer systems are inoperable)
 - security management and reporting
 - an IT asset register of hardware, software, and support services
 - a register of digital certificates and their expiry dates where appropriate
 - timeline for review of policies
 - the communication strategy to ensure that all staff are aware of any changes to policy and their responsibilities in managing computer security.

A list of the essential computer security policies can be found in Appendix B. A generic template for these policies can be downloaded from www.racgp.org.au/ehealth/csg.

Why is it important?

A policy and procedures manual provides information and guidance to staff on the accepted practice in managing the computer systems. It also provides key information, such as a list of phone numbers of software suppliers and details about operating system configuration. It is a source of information to clarify roles and responsibilities, and to facilitate the orientation of new staff.

The manual also encourages practices to review and evaluate their computer systems and think through their requirements in both human and financial terms. The development of practice policies is informative and educative. Practices can engage in Quality Improvement and Continuing Professional Development (QI&CPD) activities as

they work through the issues. For instance, developing a 'plan, do, study, act' (PDSA) cycle will provide a framework for identifying and resolving issues.

All aspects of the manual, including the individual security policies, are important to both the protection of information and recovery from computer incidents. An essential document is the asset register. The asset register includes hardware, software and services components as it provides a reference to the set up of the computer system and network in the practice. The asset register in the manual should include:

- a detailed description of the equipment including: make, model, serial numbers, date of purchase and warranty information
- location of the equipment in the practice
- location of software installation discs (where appropriate) and installation keys and serial numbers, configuration and set up details (where appropriate)
- the contact details of external support providers.

An asset register template can be found in the policies template at www.racgp.org.au/ehealth/csg.

What should be done about it?

- ☐ Computer security policies and procedures documented
- ☐ Computer security policies and procedures documentation reviewed at specified intervals, eg. annually
- ☐ Staff trained in computer security policies and procedures.

3.3 Access control and management

What does this mean?

One of the key features of information security is information access by authorised personnel which is appropriate to their role and position in the practice. Practices should develop a policy on who can have access to specific information and systems.

Generally, there are four levels of access.

- Systems administrator – this level of access is usually the highest and often is only used by IT/security trained (external) service providers for the server, operating system and network functions
- Practice manager – this access usually includes administrative functionality on various financial, clinical and network systems used in the practice
- Receptionists – this level of access is for patient administration such as appointments and billing
- Clinical staff – this level is for use of the clinical programs. This access level may be further subdivided where delineation between the physician, nursing and allied healthcare staff access is required.

Once a policy on access has been determined (ie. the rights, roles and permissions for staff), then practice staff can be given appropriate authentication methods. These can be divided into the following types:

- something you know (eg. a password)
- something you have (eg. a smartcard)
- something you are (eg. a fingerprint).

Passwords are the most common form of access authentication.

It is important for the practice to consider the implications of staff who no longer work at the practice. The process for removal of access needs to be detailed in the access security policy and procedures manual. This will also form part of the policy relating to staff leaving the employment of the practice.

There are two other access issues that need to be considered.

1. Access to practice systems by external service providers – it is advisable to put in place a confidentiality agreement with anyone who works on or supports your computer system. This should include support for the practice computer system via modem or internet support. A suggested confidentiality agreement is given in Appendix C
2. In addition to internal policies that are concerned with access rights and other data handling processes, privacy laws require organisations that deal with personal information to make available to the public a policy about their data handling practices including collection, use and disclosure. Practices should obtain legal advice about this and other obligations under state, territory and national privacy laws, and codes of conduct and indemnity.

Why is it important?

It is essential to comply with governing privacy principles and all relevant state, territory and national privacy laws. Restricting access to only those who are authorised will protect the practice against misuse of any information that the practice retains.

Best practice principles are that staff retain the responsibility for their own passwords and do not share them with other staff members. Practices will need to develop their policy after identifying and applying a risk analysis to the needs of the practice. It is suggested that practices seek the support of suitably qualified IT professionals if needed.

What should be done about it?

- ☐ Staff policy developed on levels of access to electronic data and information systems
- ☐ Individual staff are assigned an appropriate access level
- ☐ Staff have individual passwords which are kept secret and secure.

3.4 Business continuity and disaster recovery plans

What does this risk category mean?

This is a documented plan that details what should be done when there are interruptions to the function of the computer system, so that the practice can still function effectively. A business continuity plan includes multiple scenarios from minor disruptions to the computer system, whole computer system failure, to major building and environmental disasters. While the primary plan will concentrate on internal system malfunction or failure, the broader scenario, such as the functioning of the practice in the event of an environmental disaster, should also be included. This is becoming increasingly important as e-health becomes a reality and medical practices become dependent on information transfer and not solely on internal functioning.

At the primary level, the plan must include advice on how to revert to a paper based system until the computers are functioning again. Data backup and restoration is one part of a business continuity plan; this has been called 'disaster recovery' in the past. Backups are an integral part of this recovery process.

A business continuity plan should anticipate how a practice will manage without functioning computers. Computer malfunction can be due to a number of factors including human error, hardware failure, software errors, interruptions to power supply, malicious activity, and environmental incidents. If a significant computer failure occurs, practices need to know how practice systems will be managed 'manually' and the information collected re-entered after recovery.

These practice systems include:

- appointment scheduling
- issuing patients with invoices and receipts
- enabling clinical staff to provide adequate clinical care while not having access to electronic medical records
- knowing who to telephone for technical advice
- knowing where the backup medium is and, together with technical support, ensuring that data is restored, and computer hardware and software are returned to normal working function.

A business continuity plan proforma can be found in Appendix D. It should be reviewed at specified time intervals (eg. annually) or if something changes such as the backup medium or procedure. The asset register is an integral part of the business continuity plan as it provides much of the essential information required to recover the practice computer systems quickly and efficiently.

Why is it important?

The management of a computer malfunction needs to be planned. A business continuity plan will help minimise disruption, reduce risk to the business, and reduce the potential risks and inconvenience to patients. It is therefore vital to define the critical functions for which computers are used in your practice.

What should be done about it?

- ☐ Business continuity and disaster recovery plans developed
- ☐ Business continuity and disaster recovery plans tested at specified intervals (eg. at least annually)
- ☐ Business continuity and disaster recovery plans updated at specified intervals and when technological or procedural changes occur.

Technical issues

3.5 Backup

What does this risk category mean?

Data can be lost through human error, software malfunction or failure, hardware problems and external causes. People can accidentally erase information, software can cause data loss through program flaws and data storage devices can be lost or stolen. It is critical to make regular backups of all your information and software in case any of these occur. You need to know the answers to the questions below.

- What is your backup procedure?
- Which backup medium and software will you use?
- How can your backup data be restored?
- How can you check that the backup system works every time?

The installation of a backup system requires technical skills and may best be provided by an expert IT technical consultant. Some of the issues that will require expert advice are outlined below.

- The appropriate backup software and hardware for individual practice circumstances. There are many types of backup media programs to choose from and because of the rapidly changing IT environment, practices should seek expert technical advice
- The distinction between system backups and business and clinical data backups. Business and clinical data backups need to be performed daily. Make sure that backups are taken offsite and stored securely. This includes knowing who has the most recent backup at any one time
- Data restoration is knowing how to 'rebuild' a system and server if it has become inoperable. It is not simply a matter of reloading the data; you also need documentation of which programs were on the computer and how they were configured. This needs to be done by or under the guidance of an IT expert
- Testing the backup and restoration procedures.

The practice computer security coordinator is responsible for:

- knowing what the business continuity plan is and how backups fit into this plan
- knowing where the programs are housed, eg. whether on the server or a work station, and where the software media can be found. Such information should be recorded as part of the asset register
- when to call the technical services provider
- where the backups are stored (and who took them home the previous night).

There are several other important points to note in relation to backup.

- A distinction should be made between the daily backup (stored offsite and used to restore data if necessary) and weekly, monthly and yearly archives (used for long term data retention and legal purposes). Note that both backup and archive data should be kept in secure locations. All backups and archived data should be encrypted and password protected where possible
- It is important that archive backups (weekly, monthly and yearly backups) can be read in the future. This becomes an issue when computer systems and backup methods are updated and replaced. A process for transferring archive backups to current backup media is required to ensure they can always be read by the currently available technology. The practice should be aware and meet the national and state records legislation for the retention of patient information. The archive backups now form part of this. The backup and long term record keeping policy for the practice should detail the local and national requirements. Further, these policies should ensure continuity of access to archived data and the processes for conversion of legacy system information to current readable formats
- The use of RAID (redundant array of inexpensive disks) hard drives also merits consideration as these can take over the function of the principal hard drive should it fail. However, this is a critical hardware safeguard rather than a standard backup procedure for data recovery.

Note: if practicable more than one backup method should be used.

Why is it important?

Having a reliable and tested backup procedure is essential. Being able to restore all practice information after a computer incident is vital. Storage and retrieval of information are a high priority in computer security.

What should be done about it?

- ☐ Backups of data performed daily, with weekly, monthly and yearly copies retained
- ☐ Backups encrypted
- ☐ Backups of data stored securely offsite
- ☐ Backup procedure tested (by performing a restoration of data) at specified intervals
- ☐ Restoration procedure included in a documented business continuity and disaster recovery plan.

3.6 Malware and viruses

What does this mean?

Malware, including viruses are software programs that unauthorised people seek to install on your computer. This may be for malicious reasons, such as corrupting, destroying or stealing data, or to use your computer for their own purposes, such as for seeking information about you and your practice, or to make use of your computer resources.

Malware is generally introduced into a system while communicating electronically with the outside world via email or the internet. They can also be transmitted via CDs/DVDs, USB flash drives (memory sticks) and other portable devices and media.

There are various types of malware, more formally referred to as malicious code. They include:

- viruses and worms – malicious code that attaches itself to files and spreads from one computer to another
- trojans – malware disguised as a real program
- phishing – fake emails and websites attempting to acquire usernames, passwords and credit card details
- spam – unsolicited or junk email
- spyware and adware – is advertising supported and tracking software. It is used to collect information about a person or organisation without their knowledge, usually for advertising purposes.

Certain types of software such as popular versions of internet 'browsers' or email programs allow easier downloading of viruses (and also expose computers to other security risks). Technical advice should be sought on whether changes to software would lower the risk of infection.

The risk of malware infection can be minimised by:

- having a process in place that minimises the risk of downloading malware (eg. checking email attachments for viruses)
- automatically updating antivirus and antimalware software
- monitoring staff activity and ensuring that policies on access and the use of the internet are followed.

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

Why is it important?

Malware can interfere with computer functioning, potentially resulting in minor inconvenience or in extreme cases, system inoperability. This can have a major impact on the practice through the loss or alteration of information. Certain types of malware can also capture your passwords (eg. key logging) and this is one reason why passwords should be changed regularly.

What should be done about it?

- ☐ Antivirus and antimalware software installed on all computers
- ☐ Automatic updating of virus definitions enabled on all computers/servers
- ☐ Staff trained in antimalware procedures as documented in the policies and procedures manual
- ☐ Automatic scans of hardware enabled

3.7 Network perimeter controls

What does this mean?

Network perimeter controls are the hardware and software tools used to protect your system by analysing data entering and leaving your network. It includes technical measures such as firewalls and intrusion detection systems. Today this also means gaining a balance between protections and allowing authorised remote access to practice systems. In security, using multiple techniques and tools to protect information systems within the network is called layering (or defence-in-depth). This would commonly involve multiple protection mechanisms, such as firewalls, intrusion detection systems, virtual private networks (VPNs), content filtering and antivirus protection active.

Firewalls

Firewalls are an electronic mechanism that checks messages coming in and out of a network and blocks unauthorised access into a computer system. These can be in the form of software or hardware. A firewall can be configured to allow and disallow messages from specific computers. Various programs, some of which are freely available on the internet, can be installed to protect you from 'hackers' 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 coming from specific sites.

Unless you are using a standalone computer, it is advisable to install a hardware rather than a software firewall for extra security. Firewalls need to be properly configured and periodically tested to ensure they are still working. These are matters for a technical service provider.

Intrusion detection systems

Intrusion detection systems (IDS) usually software based and specifically alert you if there has been unauthorised access to your systems – IDS do not prevent attacks on your system but they inform you that there is a potential problem so action can be taken. These are devices and programs that need technical knowledge to install and configure correctly.

An antivirus program also forms a component of network perimeter controls and is discussed in section 3.6.

Content filtering

Content filtering is when you have software programs that can restrict access and filter email and access to the internet. Filtering for spam is the most common type of email filtering. Limiting access to websites is also commonly used.

Why is it important?

Hackers can steal information and can cause mischief within your computer system and this can lead to loss of data. You should consider the need for perimeter controls in the same category as the need for antivirus protection. These are essential for the long term protection of patient information. As above, even an inadvertent breach may infringe privacy laws and doctor-patient confidentiality.

Network perimeter controls are essential for anyone using the internet. Like viruses, unwanted intruders can invade your system. Your technical service provider can inform you about logs of unauthorised activity on your system.

What should be done about it?

- ☐ Hardware and/or software network perimeter controls installed
- ☐ Hardware and/or software network perimeter controls tested periodically
- ☐ Intrusion activity logs monitored and breaches reported.

3.8 Portable devices and remote access security

What does this risk category mean?

Portable devices include laptops, USB flash drives, removable hard drives, mobile phones (especially 'smart phones'), PDAs and backup media such as tape. All of these are prone to being lost or stolen. This increases the risk of data inadvertently ending up being accessed by unauthorised people. Therefore, computer security measures need to be widened beyond the walls of the practice itself. Security on these devices can be increased using passwords and encryption.

Remote access to your practice computer system includes wireless networks and increases the convenience of access to the practice information. However, it therefore also requires additional security measures so that eavesdroppers cannot gain unauthorised entry to your databases. There is increasing usage of Wi-Fi (or Bluetooth) enabled laptops and other handheld devices, eg. for visits made outside the practice (home and aged care facilities). You should obtain technical advice on how best to keep the equipment and information secure. Wi-Fi devices must have encryption set up to ensure the confidentiality of information.

Remote access is also used by IT service providers to support your computer system. You should ensure that the methods used to access your system for IT support cannot also become security vulnerabilities. Procedures should be in place to minimise these risks. In addition, since third parties may have access to your system legitimately, an example of a confidentiality agreement for such providers is given in Appendix C.

Additionally, it is important to think about security for home computers, especially if practice staff take electronic files home to work on them after hours and then return these files to the clinic's network.

Why is it important?

It is not enough to consider computer security for fixed hardware. Portable devices are increasingly being used and remote access via Wi-Fi and web based access via internet connections make it easier to log on to the practice systems. In addition, the portability and small size of devices such as USBs mean that copying information is easier, whether for legitimate or unauthorised purposes.

Data needs to be secured (encrypted) on portable devices as they can be easily misplaced or stolen. Care should also be taken for backup media which are taken offsite on a daily basis.

What should be done about it?

- ☐ Portable computers, memory devices, including backup media need to be secured
- ☐ Wireless networks (remote access systems) must be configured securely by an expert and should include:
 - ☐ encrypting the data transfer using WPA2 (Wi-Fi Protected Access 2) or stronger encryption standards to avoid information exposure if the network is compromised
 - ☐ limiting the power of the routers' radio (Wi-Fi) signal so that it does not extend past the walls of the practice (known as the wireless footprint)
 - ☐ disabling network broadcasting to reduce the risk of devices on the network announcing themselves to other devices on the network
 - ☐ enabling MAC (media access control) address filtering to restrict unauthorised devices from connecting to your wireless network. A MAC address is unique to a specific computer or device
 - ☐ change the SSID (service set identifier) or the public name of the wireless network to something unique that does not identify the brand of device/s used or the business name
- ☐ A policy on use of mobile devices in the practice should be developed. This would include the permitted devices and in what circumstances they can be used.

3.9 Computer and network maintenance

What does this risk category mean?

Computer and network maintenance should be scheduled regularly. Maintenance includes looking after both hardware and software. More specifically, it includes:

- ☐ physical security
- ☐ computer screen confidentiality
- ☐ software maintenance
- ☐ protecting your network against fluctuations in the power supply.

Physical security

The physical location of the server is important. You can protect it against theft by locking it in a safe place or attaching it to a secured cable. Desktop computers and laptops and other portable devices should always be kept physically secured.

Environmental protection will include positioning computers and other components of the network where they are not subjected to excessive heat, eg. from direct sunlight. All computers should be kept reasonably dust free.

Physical security also includes appropriate disposal of old or decommissioned computer equipment and importantly any data storage media, especially hard disks. Password protection and/or encryption are not sufficient when disposing of old equipment. Disks and backup media should be securely erased or physically destroyed. If unsure about this aspect, it is advised to seek expert advice from your IT provider.

Computer screen confidentiality

This guideline is not about privacy principles per se, although keeping information on the computer screen private is an instance in which a 'privacy' matter overlaps with computer security.

Information security in the consulting room is more about clinical staff behaviour than technical matters. All clinical staff, including doctors, nurses and allied health providers will have to decide if there might be sensitive information on the screen which should not be seen. For example, it might not be acceptable for a parent to see a sensitive past history of their adolescent child.

More importantly, patients should not be able to view the clinical record of another person such as the patient previously consulted.

Similarly, receptionists need to be careful that patients do not have inappropriate visual access to any information on computer screens at the front desk. This includes ensuring that any medical and/or sensitive information read from the computer screen by receptionists is at an appropriate volume to maintain confidentiality.

There are various methods by which the information can be kept private. Common sense methods include remembering to exit the previous patient's electronic file before the next patient enters the consulting room. Screen positioning can also help keep information private, including computers used by reception staff at the front desk.

Two other options worth considering

- The use of 'clear screen' function keys which instantly close down an open file. For example, if you use a Windows keyboard, pressing the Windows logo key and 'D' together will take you to the desktop. Rekeying these will take you back to your previous screen. You should take technical advice on how you can quickly clear your current screen if you are unsure. This technique might be useful if you wish to leave the consulting room while the patient remains
- The use of screensavers when someone is absent from the room. These can be set so that you have to use your password to log back into your system.

Whichever method you consider most appropriate to your circumstances, the important thing is that you are aware of how you can keep sensitive screen information from being inappropriately viewed.

Software maintenance

This means performing 'maintenance' work on regular occasions.

- Patching – it is vitally important to keep your software up-to-date, especially your operating system software. Patches and other program updates are essential to rectify security 'holes' in earlier versions
- Software configuration – software also needs to be installed and maintained in accordance with the vendor's guidelines to ensure security is maintained.

Unless you have sufficient technical knowledge among the practice staff, technical advice should be sought on how to keep your computer functioning efficiently.

Installing an uninterruptible power supply

An uninterruptible power supply (UPS) is a device that contains commercial batteries that provide power to enable computers (especially servers) to shut down normally when the main electricity supply cuts out. This is important so that data that is being processed while the blackout occurs is not lost. A UPS also helps with power surges which can cause hardware damage. However, the batteries in most units only provide power for a short period of time, typically 10–30 minutes. In a prolonged blackout, the UPS should be programmed to automatically shut down the server in an orderly manner to prevent data corruption or loss. Prolonged blackouts require generators or other technical solutions which are likely to be beyond the resources of most practices.

The UPS is usually only attached to the main server and its monitor. The purpose of the UPS is not to continue running the practice systems, but to allow an orderly shutdown of the computer systems to minimise data loss.

Installing surge protectors on noncritical workstations

A UPS should be installed on the main server, but simple surge protectors will generally be sufficient on other workstations in the practice. The network itself, including other devices attached to it such as modems, also need to be protected from power fluctuations that can cause data loss and hardware failure.

Why is it important?

Preventive strategies are required to keep the computer system running properly. It is best to have an arrangement with a technical service provider that includes routine network maintenance; do not treat their role as limited to providing emergency treatment when inevitable problems arise. Power outage or fluctuations can happen at any time. A UPS is a good insurance policy to protect your practice's information on the server.

What should be done about it?

- ☐ Physical security of the server and network maintained
- ☐ Practice staff should be aware of how to maintain appropriate confidentiality of information on computer screens
- ☐ Computer hardware and software should be maintained in optimal condition (includes physical security, efficient performance of computer programs, and program upgrades and patches)
- ☐ Uninterruptible power supply and surge protectors installed.

3.10 Secure electronic communication

What does this mean?

Secure electronic communication is a broad term which includes secure messaging and the use of the internet. Messaging (ie. the transfer of sensitive clinical information) remains a difficult and controversial area for the following reasons:

- arguments exist about the degree of risk of ordinary (unsecured) email
- there is a lack of compatibility between a large number of secure messaging systems that are currently available
- the cost of some of these secure messaging systems or the difficulties associated with obtaining them and uploading their programs onto computers makes ordinary email attractive.

Nevertheless, it is universally agreed that patient information exchanged between healthcare providers, or patients themselves, should be kept private. This includes nonclinical matters such as confirming appointment times via automated short message service (SMS) mobile phone reminder methods. Explicit consent from patients should be obtained, and documented, before use of any electronic communication methods.

Sending clinical information electronically requires stringent security precautions because it is technically possible for a third party to intercept and read emails intended for someone else. It is also easy to send sensitive information astray by inadvertently clicking on the wrong person in an electronic address book.

There are two aspects to secure messaging:

- encryption
- authentication.

Encryption means that 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 electronic signatures. To prevent information being read by an unintended recipient, it is best to encrypt information including emails.

There are currently a number of ways that data can be encrypted and authenticated. One method, made available by the Commonwealth Department of Health and Ageing at no cost to the user, is called Public Key Infrastructure (PKI), but there are numerous secure messaging systems available in the medical market place.

What constitutes appropriate electronic messaging with patients is a question that every practice must address. Whether communicating via email, or via social networking sites (if your practice permits this) practices should ensure that data security remains paramount. Practices need to adopt a policy on the appropriate and safe use of email to ensure no privacy breaches – for both the practice and the patients. Given that most patients do not use encryption programs at present, emails between practices and patients need to be cautious and limited in scope, for both security and clinical safety reasons.

A suggested email and internet policy which includes security and safety considerations can be found in Appendix E.

Practice website safety and security

Practice website policies are a specific aspect of internet policies that are increasingly relevant in general practice. It is important that the information on practice websites is up-to-date and does not invite unsafe practices. For example, patients might wish to contact the practice via their website, but they need to be advised that sensitive clinical information should not be transferred in this way, and that there might be a delay in obtaining a response to their queries if they send a request in this way.

There might be additional security risks if the practice website is hosted on the same computer that holds the practice data. If there is a security breach through the practice website there is a risk of the practice data being vulnerable.

Why is it important?

Securing electronic information is important to prevent it being read by an unintended recipient. However, 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 or be delivered to the

wrong address. Why is it that electronic security sets apparently higher standards? One reason is that electronic transmission makes it easier to inadvertently broadcast information to a wider audience. Another is that electronic transmission offers the opportunity to protect information more efficiently than previous methods of transmission.

Encryption is technically easy for the end user once the system has been installed. However, until practices have access to encryption, it is advisable not to send confidential data via email or the internet.

Email and internet policies, including that of a practice website, also help to ensure that confidential information is kept secure and private. Further, these policies will help remind practices about clinical safety concerns when providing advice to patients about serious health matters using electronic means.

What should be done about it?

- ☐ Secure messaging systems considered, including the impact of new secure messaging standards as developed by Standards Australia and the National E-health Transition Authority (NEHTA)
- ☐ Secure messaging used for the electronic transfer of confidential information
- ☐ Develop and review policies in the use of email, the internet and the practice's own website
- ☐ The impact of Healthcare Identifiers (for patients, healthcare workers and organisations) – the proposed national authentication services need to be considered as these are adopted across Australia.

4. Conclusion

Remember that there are three components to computer security:

- availability of information when it is needed
- ensuring the integrity of the information
- maintaining confidentiality.

Computer security is an important issue in running a practice and for protecting your business and clinical information. The checklist and guidelines will assist the practice to maintain computer security standards, follow good practice and improve their information security processes.

These guidelines are not intended to explain all the necessary technical aspects of security. You will need expert technical advice to assist you in some areas. The computer security coordinator should be aware of the role of external IT consultants and what role they need to play in protecting your information systems. Improving computer security in your practice is about adapting to an evolving technical environment, fostering staff awareness and gradually improving your systems. 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. All of the practice staff need to be aware of computer security issues, that security protocols are followed, and that there is appropriate training.

The computer security coordinator will also take on the responsibility for reviewing computer security on a regular basis (eg. annually) and for educating all practice staff in the practice's policies and their responsibilities. All staff in the practice need to be aware of the key principles of computer security, be able to recognise incidents should they occur and adhere to the practice policy.

Computers are now a part of general practice. As e-health initiatives become core to the provision of healthcare, the practice will need to review the processes that support patient privacy and computer security. Computer security is therefore not an option: it is an integral part of using a computer system in general practice.

Appendices

Appendix A

Practice computer security coordinator role description

Appendix B

Computer security policies and procedures manual documents

Appendix C

Contractual agreements with technical service providers

Appendix D

Business continuity plan

Appendix E

Internet and email policies

Appendix F

Computer security terms

*Note: A template for a computer security policies and procedures manual can be downloaded
www.racgp.org.au/ehealth/csg.*

Appendix A

Practice computer security coordinator role description

The role of the practice computer security coordinator will vary 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, such as the practice manager. Most likely, the practice IT coordinator will also be responsible for computer security, and in many practices the roles will be shared by at least two people.

Note: Please modify this role description to suit your practice purposes.

General characteristics

This position suits someone (or two or more people who share the position) who is enthusiastic about computers. They do not need to have advanced technical knowledge, although they should be reasonably comfortable with the operating system and relevant application software. They require management skills and the ability 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. The tasks that are listed below should either be executed by the computer security coordinator, or this person should be aware which tasks the technical service provider is executing.

Tasks

The computer security coordinator will:

- oversee the development of documented computer security policies and procedures (as detailed in the list of practice policies in Appendix B)
- ensure the existence and testing of the computer business continuity and disaster recovery plans
- ensure that all policies and procedures are reviewed at least annually
- monitor and ensure that practice security policies are being followed. In particular that:
 - staff are following password security procedures
 - the routine backup procedure is in place and tested for data recovery
 - archived data remains capable of being restored
 - screensavers are in place
 - antimalware software is installed on all computers and virus definitions are automatically updated
 - the computers, especially the server, are adequately maintained and can deal with fluctuations in the power supply
- maintain an up-to-date IT asset register (hardware, software, licences, manuals and technical support).

Appendix A continued...

Practice computer security coordinator role description

- ensure technical advice is sought and acted upon for the installation of protection mechanisms such as intrusion detection and firewalls
- investigate encryption of confidential information before electronic transfer
- coordinate the application for, use and storage of digital certificates and ensure that practice staff understand the use of encryption
- arrange ongoing security awareness training for members of the practice
- ensure the practice management is aware of any outstanding security issues and regularly report on security in practice management meetings.

Appendix B

Computer security policies and procedures manual documents

This manual should contain all the policies and procedures relating to the security aspects of the installation and use of computers and electronic communication. 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 these guidelines (eg. the business continuity plan and the email/internet policies) will form a part of the overall computer security manual, which itself is a part of a broader IT policies and procedures manual, which is in turn a part of a practice policies and procedures guide.

It goes without saying that it is of utmost importance to think through and discuss the contents of the manual within the practice, and ensure its implementation – it must not be left to just sit on a shelf.

Note: A template on computer security policies and procedures, to which you can add information and modify to suit your needs, can be downloaded from www.racgp.org.au/ehealth.

1. Roles, responsibilities and important contact information

This policy contains the information on the roles and responsibilities of practice staff, and the important contact details for who to call when assistance is required. A practice computer security coordinator should be appointed and their role defined and acknowledged by the practice (Appendix A). The responsibilities of other staff with regard to computer security should also be defined. This will provide the basis for 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 are aware of the principles of computer security and are appropriately trained.

2. Business continuity and disaster recovery plans

A business continuity plan should first cover the critical functions of the practice so that in the event of a crisis the practice can continue without major disruption or risk to the patients and staff. Second, the disaster recovery plan should contain the information necessary for returning the practice to its normal state; this will include using the backup as part of the recovery process.

The business continuity plan requires the creation and maintenance of an asset register that documents the hardware and software owned by the practice, and details where the computer media 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' (Appendix D).

Appendix B continued...

Computer security policies and procedures manual documents

3. Backup

Details of backup and recovery procedures should be documented. The backup procedure is a key component of the business continuity plan. Ensure that backup media are taken offsite when the practice is closed. Record which members of staff perform the backups and automate as much of the procedure as possible. Data restoration should be tested periodically. If this is done by the technical services provider, then the computer security coordinator should be aware that it is being done on a regular basis (Appendix C).

4. Internet and email usage

Developing a practice policy that clearly states the management and use of the internet and emails by all staff within the practice will assist in mitigating security risks. This policy should also detail the practice policy on access to social networking websites such as Facebook and Twitter (Appendix E).

5. Access control and management

Access to systems should be aligned with responsibilities outlined in the role descriptions of each staff member. Each staff member should create his or her own password/s for access. Passwords should not be written where they can be obtained by other staff or people who have access to the premises. The system administrator's password should never be divulged to anyone who is not authorised.

6. Malware and virus protection

Document malware and virus software installation and monitoring procedures. This should also include guidance on what to do if malware is detected.

7. Network perimeter controls

Network perimeter controls provide details of the systems (hardware and software) that protect the network. This may include firewall and intrusion detection hardware and software, content filtering and their related procedures.

8. Portable devices and remote access security

This policy details the permitted use of portable devices within the practice. It also

Appendix B continued...

Computer security policies and procedures manual documents

provides assistance on the factors that require consideration when installing and using wireless network access. Further, it details how and who can have remote access to practice systems. This may include third party providers and access to practice systems via web based portals.

9. Physical security

Communicate to staff and record the practice policy on the use of screen savers and other precautions such as positioning of monitors, to prevent unauthorised viewing of patient records and other confidential information. This policy also details restrictions of physical access to the server for instance, and how to secure equipment from theft and damage by power interruptions. In addition, it will detail the safe disposal of hardware and practice information.

10. Computer and network maintenance

Document details of routine computer maintenance that is required. This includes hard disk 'cleanups' (eg. by a defragmentation utility program). It also addresses software maintenance procedures.

11. Security management and reporting

This policy will detail the role of external IT consultants. It also includes the monitoring processes that should be in place to ensure compliance with policies. Further, it will detail the vulnerability management, risk assessment and information security breach reporting procedures.

12. 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

Contractual agreements with technical service providers

Contractual arrangements with outsourced technical service providers should include:

- **data confidentiality** – sensitive clinical and financial data must be kept private
- **remote access** – if the technical service provider accesses the network remotely, there has to be agreement on what they can or cannot view. If they can view ‘everything’, including files saved on workstations, then all staff should be aware of this. Entities to whom information may be disclosed by a practice (or the types of entities to whom a practice would be likely to disclose information) must be stated in the practice’s published privacy policy. (Practices should obtain legal advice about this and other obligations under privacy laws)
- **backups and restoration procedures** – What is the procedure? How often are the procedures tested? When is the ability to restore data tested?
- **response times** – How long will it take the technical service provider to:
 - give phone advice?
 - provide assistance via remote access?
 - attend onsite?
 - provide after hours assistance?
- **costs** – What are the routine maintenance costs? What about additional work in case of a computer malfunction? What are the differences in costs in business hours and after hours?

Appendix D

Business continuity plan

What should a business continuity plan cover?

A business continuity plan should first cover the critical functions of the practice so that it can continue without major disruption to the patients and staff, 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.

Note: You can download a template to assist in developing a business continuity plan www.racgp.org.au/ehealth.

Prepare a business continuity plan

Make a list of the critical practice functions and critical practice information:

- making appointments
- billing patients
- providing 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 on who will oversee business continuity and who should liaise with the technical services provider.

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
- the names and contact details of technical support personnel.

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, including portable devices, or network component
- failure to connect to the internet.

Appendix D continued...

Business continuity plan

Document the step-by-step disaster recovery procedure

Coordinating the disaster recovery

This vital document will initially address the business continuity plan for administrative and clinical functions of the practice. The computer security coordinator will then make a rapid and provisional investigation on what caused the 'crash', and will then contact technical support.

Implementing the computer repair plan

Identify which personnel will be involved in implementing the computer repair plan. The practice's administrative (appointment and billing) and clinical functions will be re-established before the computer repair process commences. Locate the most recent backup and support the technical services provider to undertake a repair of the computer system and restore data as required.

Reflecting after recovery

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

Appendix E

Internet and email policies

Policies for the use of internet and email

Develop a policy on what constitutes reasonable private use of the internet and email by staff during office hours (ie. use which does not interfere with work efficiency). Ensure that staff understand that use of the internet at the practice should be for work related purposes only.

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.

If your practice is willing to communicate with patients via email or other electronic means, explain to patients and staff (eg. via the practice website if you have one or via the practice information brochure) any limitations to the timeliness and nature of the advice that can be provided. You should also explain if you charge any fees for electronic consultations. All such communication should be securely sent using encryption.

Your practice needs to communicate to patients the way in which it will meet its privacy obligations. You should inform patients that no confidential information can be transmitted without encryption or other secure means. Similarly, you should explain that you require their explicit request and permission to communicate in these ways. In addition to internal policies concerning access rights and other data handling processes, privacy law requires organisations that deal with personal information to make available to the public a policy about their data handling practices, including collection, use and disclosure. Practices should obtain legal advice about this and other obligations under privacy laws.

Procedures for the safe use of internet and email

Protection against viruses

- Install and use antivirus and antimalware software
- Keep this software active at all times
- Keep up-to-date by using automatic updates. Periodically, check manually that it is up-to-date
- Apply patches to operating systems and application programs following technical advice
- Do not download or open and 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
- Use an antivirus mail filter to screen email before downloading
- Do not use the 'preview pane' 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.

Appendix E continued...

Internet and email policies

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 and with 'https' in the web address
- Use a second, noncritical 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
- Beware of 'phishing' attacks. Phishing occurs when a website masquerades as a trustworthy entity, for example a bank, in order to lure you into passing on sensitive information such as your username, password or credit card details.

Protection against hackers

- Install hardware and/or software network perimeter controls such as firewalls and intrusion detection systems 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.

Protection against spam

- Do not reply to spam mail
- Never try to unsubscribe from spam sites
- Remain vigilant: do not provide confidential information to an email (especially by return email) no matter how credible the sender's email seems (eg. apparent emails from your bank)
- Use a spam filtering program.

Protection against spyware

- Learn how to recognise (and delete) spyware
- Do not accept certificates or downloads from suspect sites
- Install antispyware software (from a reputable supplier).

Encryption of patient information

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

Backing up internet favourites or bookmarks and emails

- If you have a useful list of internet favourites or bookmarks make a backup of the list
- If you rely on information held in your emails make sure that it is backed up with the rest of your data.

Appendix F

Computer security terms

The following is a glossary of key technical terms relevant to computer security.

Boot password (also called power-on password) – a password that is entered when the computer operating system starts. 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 basic input/output system (BIOS) settings

Client – a client is a computer that requests services from a computer called a server, eg. 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 backup – a type of backup that only includes files that have been modified or added since the previous full or incremental backup. 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 (ie. 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 (ie. the internet). A firewall can be used to filter the flow of data through the gateway according to specific rules

Full backup – a backup 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 storing programs and data on a computer. A computer may have more than one hard drive

Hardware – physical components of a computer, such as a monitor, hard drive, or central processing unit (CPU)

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

Appendix F continued...

Computer security terms

ISP (internet service provider) – an ISP is a company that provides to companies or individuals access to the internet. You typically connect to the ISP using a modem and dial-up connection, a broadband connection or ADSL (asymmetric digital subscriber line)

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 is 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 while they are away from the office (eg. 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 and electronic communication

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, eg. the 'F drive'. 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, an 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 for activities such as accessing the network and controlling printing

Nonrepudiation – this term means that you cannot deny having performed a transaction, eg. if you send an email to your bank asking them to transfer money out of your account, nonrepudiation 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 hardware and software components work. For example, Macintosh™, Windows™ and Linux are types of operating systems

Appendix F continued...

Computer security terms

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 of the internet

RAIDS – redundant array of independent disks

Reboot – when you restart your computer. You might be required to reboot your computer in some instances, eg. 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, eg. 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 and 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 spreadsheets

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

Spyware – programs that are downloaded from the internet onto your computer (sometimes without your knowledge) to covertly send back information to the source, eg. your personal details

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

Trojans – these are unauthorised programs hidden within authorised ones

URL (acronym for uniform resource locator) – in the simplest case, it is the address for an internet webpage, such as <http://www.hotmail.com>

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

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

Further definitions are available www.racgp.org/ehealth.