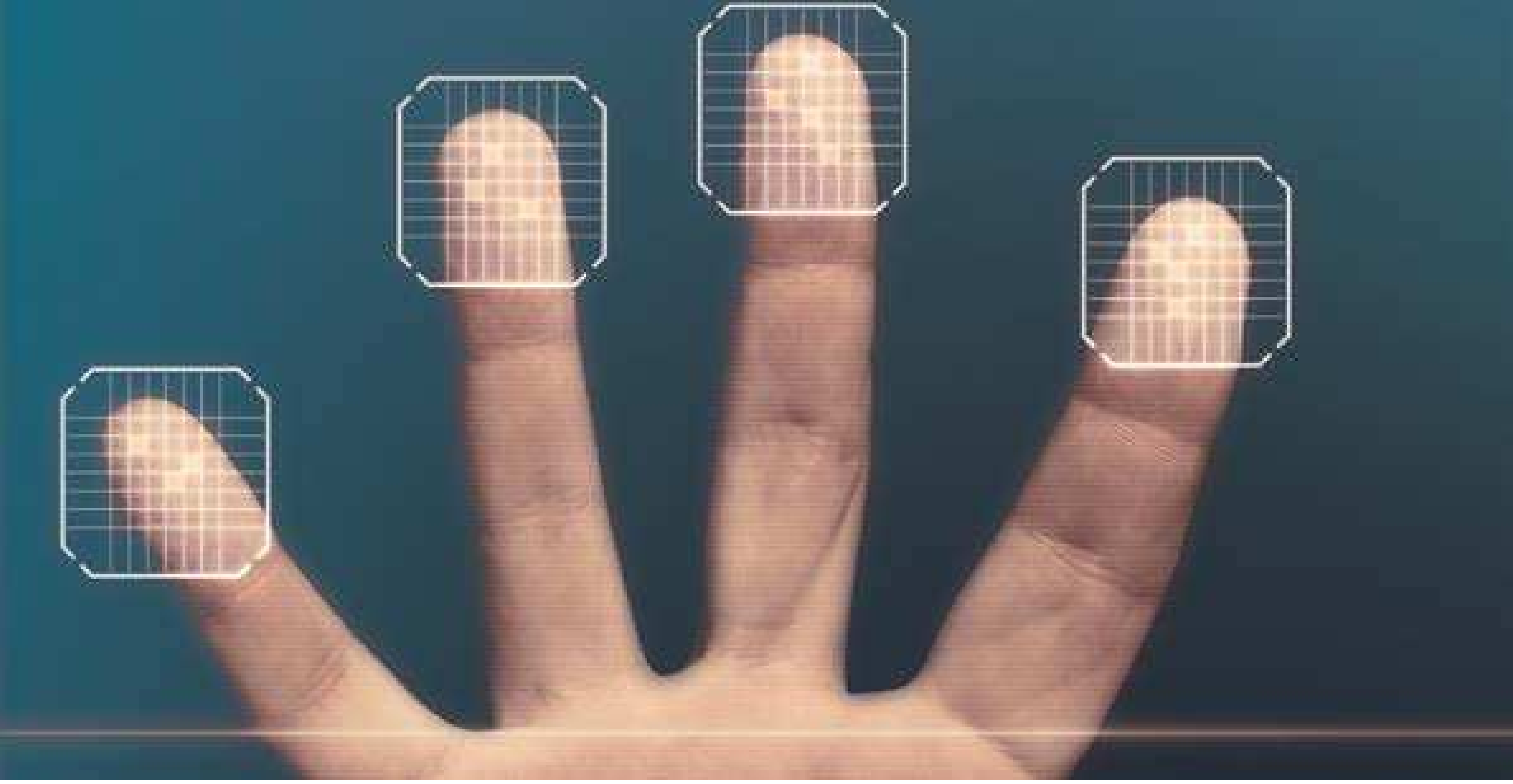
RACGP

Computer and information security standards

For general practices and other office-based practices

Second edition

©iStockphoto.com/alengo



RACGP

Computer and information security standards

For general practices and other office-based practices

Second edition

The *Computer and information security standards* provide guidance to assist general practices comply with professional and legal obligations and are designed to make compliance with best practice information security easier.

Disclaimer

The *Computer and information security standards* and accompanying *Computer and information security templates* (each a *publication*) is copyright to The Royal Australian College of General Practitioners (RACGP), ABN 34 000 223 807. The information set out in each publication has been sourced from providers believed to be reputable and reliable. The information was current as at the date of first publication, however the RACGP recognises the changing and evolving nature of medicine, and does not warrant these publications are or will remain accurate, current or complete. Nor does the RACGP make any warranties of any kind, expressed or implied, including as to fitness of purpose or otherwise. Instead, the information is intended for use as a guide of a general nature only and may or may not be relevant to particular patients, conditions or circumstances. Acting in accordance with the information in the publications cannot and does not guarantee discharge of any duty of care owed. Persons acting on information contained in the publications must at all times exercise their own independent skill and judgement, and seek appropriate professional advice where relevant and necessary.

Whilst the text is primarily directed to health professionals, it is not to be regarded as professional advice and must not be considered a substitute for seeking that professional advice relevant to a person's circumstances, nor can it be regarded as a full consideration of particular circumstances faced by the user based on then current knowledge and accepted practices.

The RACGP accepts no liability to anyone in relation to the publications, for any loss or damage (including indirect, special or consequential damages), cost or expense incurred or arising by reason of any person using or relying on the information contained in the publications, whether caused by reason of any error, any act or omission (whether negligent or not), or any inaccuracy or misrepresentation in the information in each publication.

Published by

The Royal Australian College of General Practitioners
100 Wellington Parade
East Melbourne VIC 3002 Australia

Tel 03 8699 0414
Fax 03 8699 0400
www.racgp.org.au

ISBN: 978-0-86906-349-1

First published 2011. Second edition 2013.

Acknowledgements

This edition of The Royal Australian College General Practitioners (RACGP) *Computer and information security standards* (CISS) and the accompanying *Computer and information security templates* have been developed by the RACGP.

The RACGP gratefully acknowledges the following people, who were involved in the development, review and writing of this version of CISS:

- Dr Patricia Williams PhD, eHealth Research Group, School of Computer and Security Science, Edith Cowan University, Perth, Western Australia
- Members of the RACGP Computer and Information Security Standards Taskforce.

This project has been funded by the Australian Government Department of Health and Ageing.

The information security compliance indicators for each Standard have been adapted from the work of Dr Patricia Williams: Capability Maturity Matrix for Medical Information Security (Williams PAH. A practical application of CMM to medical security capability. *Information management and computer security* 2008;16:58–73). The intellectual property relating to these capability matrices remains the property of Dr Patricia Williams.

Contents

Preamble

Background

In Australian general practice, the use of clinical desktop systems and the electronic management of information have become vital tools in the delivery of safe and high-quality healthcare and good practice management. Secure computer and information management systems are essential for the necessary protection of business and clinical information and are therefore critical to the provision of safe, high-quality healthcare and the efficient running of a general practice.

Implementing appropriate computer and information security can be challenging and general practice has specific requirements to consider. Finding the right IT support and a technical service provider with appropriate security expertise who understands the business of delivering healthcare in the general practice environment can be difficult. To help general practices meet these challenges, the RACGP developed the first edition of the *Computer and information security standards* in 2011.

This second edition of the RACGP *Computer and information security standards* (CISS) takes into account developments such as:

- increased use of laptops, remote access devices (e.g. personal digital assistants [PDA], tablet devices, USB flash drives and removable hard drives) and wireless (Wi-Fi) connections
- widespread uptake of broadband internet and secure messaging, and particularly the implementation of the national eHealth record system and the Healthcare Identifier Service, which underpin many of the e-health initiatives.

Improving computer and information security in your practice requires adapting to an evolving technical environment, fostering awareness of contemporary security issues, and monitoring and improving your security protection processes.

Computer and information security is not optional, it is essential. It should be considered a fixed cost of doing business that requires financial and human resources being allocated to ensure the protection of information assets.

The purpose of the CISS

This second edition of CISS incorporates changes to Australian legislation and the Office of the Australian Information Commissioner directives, including legislative requirements for a national eHealth record system (the personally controlled electronic health record [PCEHR] system).

The Standards are designed to assist general practices and other office-based healthcare organisations to meet their professional and legal obligations in computer and information security.

Information security obligations

Computer and information security is not optional: it is an essential professional and legal requirement for using computer systems in the delivery of healthcare.

The Standards address the legal and professional obligations in computer and information security in core areas.

Information management processes

Managing the use and ongoing availability of information requires fundamental information security processes, such as:

- backup procedures that are documented and tested: it is important to ensure that the backup system functions correctly and that data can be restored promptly if there is an incident such as a server failure
- business continuity and information recovery planning: documented business continuity plans that include information recovery procedures are essential to maintaining information availability so that in the event of an ‘information disaster’ there is an adequately planned response, and potential loss or corruption of information is minimised. These plans detail how to maintain the critical functions of the business when there is an unexpected system event
- access control and management: control of who has access to business and clinical information is essential to the protection of all practice data. Access management (password and/or biometrics) ensures accountability; without this it can be difficult to ascertain who has entered or altered data. Without these controls the practice is vulnerable to unauthorised information access.

Risk analysis

It is important to understand the security risks and threats to business and clinical information. This includes the requirement for effective information security practices by identifying gaps in security and implementing strategies to lessen security risks. Ensuring the security of information held in practice systems is essential to the running of a general practice, to maintaining professional responsibilities to patients, and to ensuring that practice information is accurate and available when it is needed.

Security governance

Governance implies accountability, responsibility, monitoring and reporting to demonstrate legal and ethical compliance to sound information security and to ensure that all computer and information security processes are documented and followed. To enable this, responsibility should be allocated to one or more staff in the practice. Staff who are allocated this responsibility should coordinate security-related activities and assist in identifying the need for external technical service providers and when it is appropriate to engage their services. Computer and information security requires regular attention at a practice level and the practice team need to be aware of their responsibility in protecting practice information.

Organisational governance

To contribute to good practice governance, practice principals/owners should be able to answer the following questions:

- What are the legal and professional requirements for the protection of the information for which the practice is custodian?
- What capabilities does the practice have in terms of security knowledge and expertise?
- Who makes the decisions about the security protections to be put in place?
- What processes are in place to assist in decision-making regarding the use of the information for purposes other than what it was collected for, for example providing health information to external organisations for research or population planning (secondary use)?

Developing a security culture

It is beneficial to promote a *security culture* within the practice. This includes educating the practice team about the risks to the practice information systems and the maintenance of practice policies that direct staff in their management of security risks.

Format of CISS

There are three components to CISS:

1. **Compliance checklist**
   This checklist is designed to help practices determine whether the practice has established and maintained reasonable computer and information security measures to protect the security of clinical and business information on an ongoing basis.
2. **Twelve computer and information security standards**
   For each Standard there is:
   - a user-friendly compliance indicator matrix
   - explanatory notes for each compliance indicator. The explanatory notes are designed to explain each Standard and the actions required to minimise potential risks to computer and information systems.
3. **Templates**
   The accompanying templates consist of sample tables and forms to assist practices to develop and record their own policies and procedures for computer and information security.

In scope

CISS describes professional and legal obligations for computer and information security and details policies and procedures designed to help general practices protect their computer and information systems.

These Standards have been developed in accordance with recognised best practice and are aligned with the requirements of international and Australian standards, current Australian legislation and legislative instruments, the National Privacy Principles and national standards in health information security (see *Appendix A*).

The computer and information security requirements that relate to the Healthcare Identifier Service and participation in the national eHealth record system have been included in this edition of CISS.

Out of scope

The Standards do not cover separate issues such as patient access to their own health information, patient identification (personal identification and validation of the Individual Healthcare Identifier), or the content of patient health records.

The Standards also do not cover all the necessary technical aspects of computer and information security. It is generally assumed practices will engage expert technical advice and support to establish and maintain computer and information security on a day-to-day basis.

The Standards are not designed to impose new professional obligations over and above recognised best practice.

Compliance with Australian legislation

The Standards are aligned with relevant legislation including the following.

Privacy Act and National Privacy Principles

The *Privacy Act 1988* (Cwlth) and National Privacy Principles stipulate that *reasonable steps* must be taken to protect and secure personal information, which includes personal health information. Reasonable steps are explained further by the Office of the Australian Information Commissioner (OAIC). When investigating compliance, the OAIC considers the *reasonable steps* that were taken to protect the information, and whether those steps were reasonable in the circumstances, including the processes followed if a privacy breach occurred.

Reasonableness is considered in relation to the organisational context and the context in which the information is collected and used. Health information is regarded as sensitive information by the OAIC and there is an expectation that such information will be given a higher level of protection than non-sensitive information. See the OAIC website (www.oaic.gov.au).

The Standards are designed to help practices meet the requirements for OAIC definition of *reasonable steps.*

Healthcare Identifiers Act and Personally Controlled Electronic Health Records Act

To participate in the Australian national eHealth record system (also known as the [PCEHR] system), practices must comply with the *Healthcare Identifiers Act 2010* (Cwlth) and the *Personally Controlled Electronic Health Records Act 2012* (Cwlth) and PCEHR Rules 2012. The PCEHR system Participation Agreement that practices must agree to prior to using the eHealth record system is derived from this legislation and consequently incorporates compliance with these Acts. There are many requirements of a participating healthcare organisation pursuant to the PCEHR system legislation and the related Participation Agreement.

The Standards are designed to help practices meet the requirements of the national eHealth record system (further detail is in *Appendix B*).

Terminology

The terminology used in CISS is designed to enhance the clarity of the text.

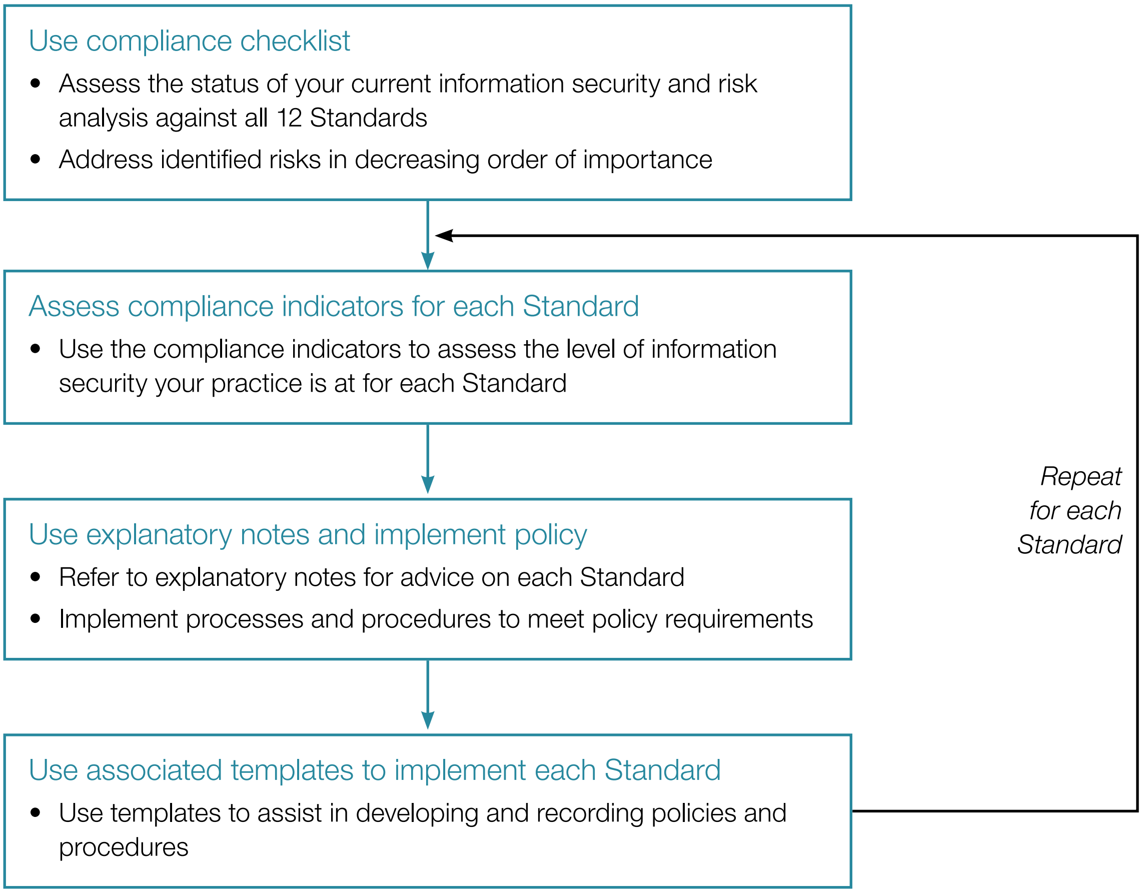
- **Availability of information:** Information is available and accessible to authorised individuals when it is needed.
- **Confidentiality:** The non-disclosure of information except to another authorised person, or the act of keeping information secure.
- **Health information:** All health information and health data about a patient that is collected during a consultation with a health professional.
- **Integrity of information:** Maintaining the accuracy and consistency of information, which requires that only authorised people can modify the information.
- **Organisation:** Any healthcare organisation operating in the Australian primary healthcare sector.
- **Practice team:** All members of a general practice, including clinicians and non-clinicians working in the Australian primary healthcare sector whether as a solo practitioner, a member of a single discipline practice team or a member of a multidisciplinary practice team.
- **Privacy:** A person's privacy is maintained by control over what and how information is disclosed.

Implementation and review

This edition of CISS was published in June 2013 and will be reviewed by the RACGP from time to time in consultation with key stakeholders.

How to use the Standards

The Standards are designed to assist practices to meet their legal and professional obligations in protecting computer and information systems. The diagram below shows the step-by-step cyclical process for using these Standards to achieve best practice in maintaining computer and information security.



Use compliance checklist

- Assess the status of your current information security and risk analysis against all 12 Standards
- Address identified risks in decreasing order of importance

Assess compliance indicators for each Standard

- Use the compliance indicators to assess the level of information security your practice is at for each Standard

Use explanatory notes and implement policy

- Refer to explanatory notes for advice on each Standard
- Implement processes and procedures to meet policy requirements

Use associated templates to implement each Standard

- Use templates to assist in developing and recording policies and procedures

Repeat for each Standard

The Standards

Standard 1: Roles and responsibilities

Our practice has designated practice team members for championing and managing computer and information security and these practice team members have such roles and responsibilities documented in their position descriptions

Standard 2: Risk assessment

Our practice undertakes periodic, structured risk assessments of computer and information security and implements improvements as required

Standard 3: Information security policies and procedures

Our practice has documented policies and procedures for managing computer and information security

Standard 4: Managing access

Our practice establishes and monitors authorised access to health information

Standard 5: Business continuity and information recovery

Our practice has documented and tested plans for business continuity and information recovery

Standard 6: Internet and email usage

Our practice has processes in place to ensure the safe and proper use of internet and email in accordance with practice policies and procedures for managing information security

Standard 7: Information backup

Our practice has a reliable information backup system to support timely access to business and clinical information

Standard 8: Malware, viruses and email threats

Our practice has reliable protection against computer malware and viruses

Standard 9: Computer network perimeter controls

Our practice has reliable computer network perimeter controls

Standard 10: Mobile electronic devices

Our practice has processes in place to ensure the safe and proper use of mobile electronic devices in accordance with practice policies and procedures for managing information security

Standard 11: Physical facilities and computer hardware, software and operating system

Our practice manages and maintains our physical facilities and computer hardware, software and operating system with a view to protecting information systems

Standard 12: Security for information sharing

Our practice has reliable systems for the secure electronic sharing of confidential information

Compliance checklist for computer and information security

This compliance checklist is designed to help general practices assess, achieve and sustain compliance with the 12 Standards that comprise good practice in computer and information security. This checklist is a guide only and does not describe the complete list of security activities that should be undertaken.

If you are unsure whether your practice complies with a particular Standard then you should tick 'no' and focus on relevant risk mitigation activity until you are sure.

Standard	Compliance indicators	Yes	No
Standard 1: Roles and responsibilities	**Do you have designated practice team members for championing and managing computer and information security and do these practice team members have such roles and responsibilities documented in their position descriptions?** This will include a written policy that is communicated to practice team members, the assignment and training of a Computer Security Coordinator, the assignment and training of the Responsible Officer and Organisation Maintenance Officer, and the national eHealth record system training where applicable.	□	□
Standard 2: Risk assessment	**Have you undertaken a structured risk assessment of information security and identified improvements as required?** This will include recording assets in the practice, a threat analysis, reporting schedule and data breach recording procedures.	□	□
Standard 3: Information security policies and procedures	**Do you have documented policies and procedures for managing computer and information security?** This will include a policy to cover each Standard. It will also include practice team and external service provider agreements, and where applicable an eHealth records system policy.	□	□
Standard 4: Managing access	**Do you have well-established and monitored authorised access to health information?** This will include a clearly defined and communicated policy that contains direction on access rights, password maintenance, password management, remote access controls, and auditing and appropriate software configuration.	□	□
Standard 5: Business continuity and information recovery	**Do you have documented and tested plans for business continuity and information recovery?** This will include tested, practical and implementable business continuity and information recovery plans to ensure business continuation and prompt restoration of clinical and business information systems.	□	□
Standard 6: Internet and email usage	**Do you have processes in place to ensure the safe and proper use of internet and email in accordance with practice policies and procedures for managing information security?** This will include details of configuration and usage of the internet and email, together with practice team education in good internet and email use practices.	□	□

Standard	Compliance indicators	Yes	No
Standard 7: Information backup	**Do you have a reliable information backup system to support timely access to business and clinical information?** This will include documented procedures for the systems to be backed up and how often (backup type and frequency, use of encryption, reliability and restoration checking, media type and rotation, where the backup is stored and who has access to it). It should also include access to data from any previous practice information (legacy) systems.	□	□
Standard 8: Malware, viruses and email threats	**Do you have reliable protection against malware and viruses?** This will include automatic updating of the virus protection software, and educating the practice team to be aware of risks of exposing the practice information systems to malware and virus attack.	□	□
Standard 9: Computer network perimeter controls	**Do you have reliable computer network perimeter controls?** This will include ensuring the firewall is correctly configured and that the log files are examined periodically; this will also apply to intrusion detection systems. Wireless networks need to be appropriately configured, and content filtering and perimeter testing should be considered.	□	□
Standard 10: Mobile electronic devices	**Do you have processes in place to ensure the safe and proper use of mobile electronic devices in accordance with practice policies and procedures for managing information security?** This will include the defined use and secure management of practice-owned and personal mobile devices that are used for business or clinical purposes.	□	□
Standard 11: Physical facilities and computer hardware, software and operating system	**Do you manage and maintain the physical facilities and computer hardware, software and operating system with a view to protecting information security?** This will include the physical protection of equipment and the use of an uninterruptible power supply (UPS). A secure disposal process should be established and appropriate system and software maintenance undertaken.	□	□
Standard 12: Security for information sharing	**Do you have reliable systems for the secure electronic sharing of confidential information?** This will include the appropriate configuration of secure messaging, digital certificate management and the practice website.	□	□

Section 1

Standard 1: Roles and responsibilities

Our practice has designated practice team members for championing and managing computer and information security and these practice team members have such roles and responsibilities documented in their position descriptions

Compliance indicators

The compliance indicators listed in the matrix identify the specific actions that comprise good security practice for Standard 1.

It is assumed the practice will provide appropriate education and training to facilitate compliance with this Standard.

The compliance indicators at level 3 reflect the minimum level of computer and information security acceptable for this Standard. The compliance indicators for higher levels provide the basis for incremental security improvement.

Helpful templates for this Standard

Templates 1.1–1.4 will assist in achieving compliance. Completion of these templates will ensure you have fully documented the requirements of this Standard.

			Minimum
Roles and responsibilities compliance indicators	**Level 1 Initial**	**Level 2 Repeatable**	**Level 3 Defined**
1.1 Policy content	No formal policy	No complete written policy	Complete written policy
1.2 Policy communication	Policy not communicated to the practice team	Policy communicated verbally to the practice team	Policy communicated in written format to relevant practice team members
1.3 Computer Security Coordinator	Role not assigned	Role assigned by default to the practice manager	Role assigned to a practice team member and training provided
1.4 Responsible Officer / Organisation Maintenance Officer	Role(s) not assigned	Role assigned by default to practice manager	Role assigned to a practice team member and training provided
1.5 Tasks and roles	Tasks and roles verbally defined only	Ad hoc allocation of roles dependent on availability and capability of practice team members Roles and responsibilities documented in a team member's position description	Tasks and roles allocated to a practice team member and defined and documented in the position description Training completed
1.6 National ehealth record system (PCEHR) training	None provided	At induction only	Ad hoc training as required

Adapted and reproduced with permission from Dr Patricia Williams

1.1 Policy content

The practice policy needs to include information about the specific roles and responsibilities of practice team members. A practice Computer Security Coordinator should be appointed and their role defined and acknowledged by the practice team. The responsibilities of all practice team members with regard to computer and information security should also be defined. This will provide the basis for determining the level of access to information systems. The practice Computer Security Coordinator, who might be the general IT coordinator as well, should help ensure that all practice team members are aware of the principles of computer security and are provided with appropriate training for their responsibilities.

1.2 Policy communication

The practice policy should be in written format and communicated to all relevant practice team members.

1.3 Computer Security Coordinator

The role of the practice Computer Security Coordinator will vary depending on the IT skills of the practice team and the availability of technical support. In most instances, the practice IT coordinator will also be responsible for computer and information security, and in many practices the roles will be shared by at least two people.

Level 4 Managed	Level 5 Optimised
Complete written policy, periodically reviewed	Complete written policy, reviewed annually
Policy communicated in written format, training provided and all practice team members have access to the policy	Policy available in written format to relevant practice team members Regular training for the practice team and communication strategy reviewed against policy All practice team aware of the content and implications of the policy
Role assigned to a practice team member and training provided, with ad hoc reporting to practice management	Role assigned to a practice team member with ongoing training provided and periodic activity reports provided to practice management Role duties and responsibilities reviewed annually
Role assigned to a practice team member and training provided with ad hoc reporting to practice management	Role assigned to a practice team member with ongoing training provided and periodic activity reports provided to practice management Role duties and responsibilities reviewed annually
Practice team members trained in specific roles and responsibilities	All practice team members aware of who is responsible for tasks Ongoing training for all roles and responsibilities assigned
All practice team provided formal and ongoing training	All practice team scheduled for regular updates and training Policy annually reviewed. Regular review of compliance by practice team

This section only specifies the role of the Computer Security Coordinator. The roles of the Responsible Officer and Organisation Maintenance Officer are outside the scope of this document

Role description

The Computer Security Coordinator will need the skills required to undertake the responsibilities listed below, or be able to liaise with appropriately skilled external providers. The role requires time dedicated to undertake the responsibilities and to ensure familiarity with the current and emerging e-health environment. The coordinator does not need to have advanced technical knowledge, although they should be reasonably comfortable with the computer operating systems (e.g. Windows) and relevant application software. They require adequate management skills to be able to develop computer security policies that are understood by the practice team, with input from technical staff when required. The role incorporates raising awareness of information security governance among the whole practice team.

The practice Computer Security Coordinator draws together the computer and information security issues that confront the practice – this is a leadership role. The coordinator manages the training and is responsible for maintaining practice team members' knowledge of computer and information security principles and practice security policy and procedures. The role also includes managing the risk assessment, creation and policy review, and the security management and reporting functions. The practice Computer 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.

The coordinator's role is primarily to raise computer security awareness rather than to be a technical 'fix-it' person. The coordinator should help foster a security culture and ensure that there is adequate and appropriate training for all of the practice team. The coordinator also needs to understand that while many aspects of computer and information security are outsourced to technical service providers, including the use of cloud services, certain responsibilities and tasks need to be carried out by the practice team (e.g. checking the backup procedure). While many practices now outsource aspects of computer maintenance to technical service providers, 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 do these tasks themselves. A generic role description for the Computer Security Coordinator is given in Section 1.5.

1.4 Responsible Officer and Organisation Maintenance Officer

In the national eHealth record system there are two roles designated in relation to computer and information security.

The Responsible Officer, as defined in the *Healthcare Identifiers Act 2010* (the HI Act), is registered under the Healthcare Identifiers (HI) Service and has authority to act on behalf of a seed organisation and relevant network organisations in its dealings with the System Operator. For large organisations, the Responsible Officer may be the chief executive officer or chief operations officer, and for small organisations the Responsible Officer may be the business owner.

The Organisation Maintenance Officer, as defined in the HI Act, is also registered under the HI Service and has authority to act on behalf of a network organisation in its dealings with the System Operator. A seed organisation maintenance officer has authority to act on behalf of the seed organisation. A healthcare organisation can have multiple Organisation Maintenance Officers. An Organisation Maintenance Officer is likely to be someone who is familiar with the IT system used by the organisation and, as such, is more likely than the Responsible Officer to be assigned tasks related to computer and information security. This role could be assigned to the practice manager.

Note: the role of the Responsible Officer and the Organisation Maintenance Officer are different and require different responsibilities. It is important to understand the specific responsibilities of each role and it is recommended that these two roles are not performed by the same person.

1.5 Tasks and roles

All of the practice team should be aware of their responsibility in regards to information security. While the role of the Computer Security Coordinator is well defined, it should be made explicit in the practice policies what role and responsibility each member of the practice must assume in the protection of information. Practice team member awareness of their role in information security is vital. This includes access management, recognition of errors or abnormal software behaviour, and susceptibility to social engineering (where someone is tricked into revealing information, e.g. a password, which can be used to attack systems or networks). A form for recording all practice team members and their allocated computer and information security tasks and responsibilities can be found in *Template 1.3*.

Examples of delegated tasks are changing backup tapes, logging all users out of the system when the practice closes, and checking that automated tasks scheduled are successful.

Computer Security Coordinator responsibilities

The role of the Computer Security Coordinator could include, but is not limited to, the following responsibilities:

- oversees the development of documented computer security policies and procedures
- ensures the existence and testing of the computer business continuity and information recovery plans
- ensures that all policies and procedures are reviewed at least annually
- monitors and ensures that practice security policies are being followed, in particular that:
  - practice team members are following password security procedures
  - the routine backup procedures are in place and tested for successful data recovery
  - archived data remain capable of being restored in a timely manner
  - anti-malware software is installed on all computers and are automatically updated
  - the computers, especially all servers, are adequately maintained and can deal with fluctuations in power
  - clear screen and clear desk policies are followed (i.e. screensavers are activated)
- maintains an up-to-date risk assessment including the IT asset register (hardware, software, licences, manuals and technical support)
- ensures technical advice is sought and acted upon for the installation of protection systems such as intrusion detection and firewalls
- ensures that information transferred electronically is secure (e.g. uses secure message delivery)
- arranges ongoing security awareness training for practice team
- ensures the practice management is aware of any outstanding security issues and regularly reports on security in practice management meetings.

1.6 National eHealth record system training

To meet the requirements of the PCEHR legislation, practice team members accessing the PCEHR system should be trained and educated in security awareness, as defined by the PCEHR system Participation Agreement.

Section 2

Standard 2: Risk assessment

Our practice undertakes periodic, structured risk assessments of computer and information security and implements improvements as required

			Minimum
Risk assessment compliance indicators	**Level 1 Initial**	**Level 2 Repeatable**	**Level 3 Defined**
2.1 Policy content	No formal policy	No complete written policy	Complete written policy
2.2 Policy communication	Policy not communicated to the practice team	Policy communicated verbally to the practice team	Policy communicated in written format to relevant practice team members
2.3 Staffing responsibility	No practice team member specifically assigned in Computer Security Coordinator, Responsible Officer, and Organisational Maintenance Officer roles Practice manager performs these roles as default	The roles of the Computer Security Coordinator, Responsible Officer and Organisational Maintenance Officer assigned	Computer Security Coordinator, Responsible Officer and Organisational Maintenance Officer assigned and appropriate training provided
2.4 Contacts	Contacts not recorded systematically	Contacts recorded in an ad hoc manner	Contacts recorded using the CISS template
2.5 Asset management	Assets not recorded	Only hardware/physical assets recorded	Hardware, software, data and electronic assets recorded
2.6 Threat analysis	Not specifically undertaken – left to installers/vendors	Installer/vendor have completed, but not provided or explained to appropriate practice team member	Practice threat, vulnerability and controls assessment done and recorded but undertaken primarily by external IT service providers
2.7 Security management monitoring and reporting	Reporting to practice management is ad hoc and only initiated when an incident occurs No ongoing monitoring	Formal incident reporting process in place but no proactive monitoring	Regular reporting and analysis undertaken Improvement/s identified
2.8 Education	No ongoing training provided for practice team	Computer Security Coordinator trained as required and other practice team members at induction only	At least annual security training updates to all practice team members
2.9 Data breach response and recording	No formal process documented Informal breach reporting only	Formal data breach process implemented and used	All data breaches reported via a formal process, fully reported and documented

Adapted and reproduced with permission from Dr Patricia Williams

Compliance indicators

The compliance indicators listed in the matrix identify the specific actions that comprise good security practice for Standard 2.

It is assumed the practice will provide appropriate education and training to facilitate compliance with this Standard.

The compliance indicators at level 3 reflect the minimum level of computer and information security acceptable for this Standard. The compliance indicators for higher levels provide the basis for incremental security improvement.

Level 4 Managed	Level 5 Optimised
Complete written policy, periodically reviewed	Complete written policy, reviewed annually
Policy communicated in written format, training provided and all practice team members have access to the policy	Policy available in written format to relevant practice team members Regular training for the practice team and communication strategy reviewed against policy All practice team aware of the content and implications of the policy
Computer Security Coordinator, Responsible Officer and Organisational Maintenance Officer assigned and appropriately trained Decision roles identified (e.g. who can make decisions on secondary use of data requests) and decision makers assigned Practice team member skills matrix completed	Computer Security Coordinator, Responsible Officer and Organisational Maintenance Officer assigned and appropriately trained Practice team member skills mapped to roles, and training identified and planned Decision making frameworks in place and documented (e.g. secondary use of data decision framework)
Contacts recorded and readily accessible to all practice team members	Contact list reviewed annually to ensure correctness and updated as required
All computer and electronic assets recorded, including hardware, software, data, and certificates Configurations partially documented	All assets and all configurations recorded, including paper assets Network diagrams created All documentation updated when changed and log of changes kept and annually checked and reviewed
Threat, vulnerability and controls assessment completed and recorded	As for level 3 plus practice team members have full understanding of the threat context and environment Plan for improvement identified Process reviewed annually
Regular reporting and analysis undertaken Improvements identified Monitoring undertaken periodically Regular item on practice meeting agenda	Established reporting schedule Established monitoring schedule Analysis to identify improvements Regular item on practice meeting agenda
Special topics presentations (at staff meetings)	Regular planned education and training, and security updates to all practice team members
All data breaches reported via a formal process, fully reported and documented, and the incident reviewed Ad hoc training to practice team members	All practice team members trained to recognise, report and document all data breaches Post-breach analysis and training for all practice team members

Helpful templates for this Standard

Templates 2.1–2.27 will assist in achieving compliance. Completion of these templates will ensure you have fully documented the requirements of this Standard.

Explanatory notes

Information security system requirements differ across practices. It is therefore important for all practices to complete a risk analysis of their particular system and security needs, and to document the policies and procedures that the practice team will need to adhere to. This will provide assurance of availability, integrity and confidentiality of all information held within the practice's clinical and business information systems. Regardless of the size of the practice, it is imperative that there is an understanding and analysis of the threats and vulnerabilities that practices are exposed to, and the possible risks to the computer and information systems. Then the most appropriate security controls can be put in place to minimise these risks. Therefore the first task in ensuring effective information security is to undertake a risk assessment.

The method suggested in this Standard has been adapted from established risk assessment and management processes and simplified to make it a practical and straightforward process for practices to undertake. The risk management process involves establishing the risk profile and appropriate risk mitigation process.

There are elements that require time to document, such as the asset register, however this information is subsequently reused in the business continuity and information recovery plans. Avoidance of this activity will mean that a practice does not have a strong foundation for its computer and information security choices and may not have effective protection of all practice information. In addition, documentation of the risk assessment provides evidence of a proper and systematic approach to security and demonstrates defensible governance. Records should be retained on physical and information assets. As an ongoing practice, each breach in security (accidental or intentional) should be recorded.

2.1 Policy content

The practice policy for assessing the risks of the practice information systems needs to be developed, and periodically reviewed. This policy will describe the roles and responsibilities of technical service providers. It will also include the monitoring processes that should be in place for compliance with practice policies. Further, it will detail the vulnerability management, risk assessment and information security breach reporting procedures.

It is a requirement of the PCEHR Rules 2012 that organisations review their PCEHR system policy at least annually and when any new or changed risks are identified. In conducting such a review, the practice must consider:

- potential unauthorised access to the PCEHR system using the healthcare provider organisation's information systems
- potential misuse or unauthorised disclosure of information from a consumer's PCEHR by persons authorised to access the PCEHR system via or on behalf of the healthcare provider organisation
- potential accidental disclosure of information contained in a consumer's PCEHR

- the increasing risks and potential impact of the changing threat landscape (e.g. newer types of security threats such as ransomware)
- the impact of any changes to the National eHealth record system that may affect the healthcare provider organisation
- any relevant legal or regulatory changes that have occurred since the last review.

2.2 Policy communication

The policy should be in written format and communicated to relevant practice team members.

2.3 Staffing responsibility

Select the person or persons in the practice team who will undertake the coordination of computer and information security in the practice – the Computer Security Coordinator. Refer to Section 1.3 for a definition of the role and responsibilities of the Computer Security Coordinator.

In addition, to comply with the legislation for participation in the National eHealth record system, the organisation must identify practice team members for two key roles – the Responsible Officer (RO) and the Organisation Maintenance Officer (OMO). Refer to Section 1.4 for a definition of the role and responsibilities of the RO and OMO.

2.4 Contacts

Systematically record all technical service provider contact details.

2.5 Asset management

Developing an asset register may require assistance from your technical service provider. The asset register documents the computer hardware, software and information systems used in the practice. The register also records the configuration of the systems that will be used when the business continuity or information recovery plan is invoked. The asset register must be updated as each new item is purchased by the practice or new service or application installed. The Computer Security Coordinator is usually responsible for maintaining the asset register.

Refer to *Templates 2.3–2.22* for examples of how to record this information. The assets are grouped as follows:

- physical assets: computer and communications equipment, mobile devices, smart phones, tablet devices, medical equipment that interfaces with the computer systems, backup media and uninterruptible power supplies. Diagrams showing the layout of the network and computers are a useful resource. It could include electronic information assets: databases, electronic files and documents, image and voice files, system and user documentation, business continuity and information recovery plans

- software assets: application programs, operating system, communications software. Include all clinical and practice management software, as well as email, firewall, backup, virus checking and other utilities. Original software media and manuals should be stored securely
- personnel assets: contact details of key members of the practice team and external service providers should be recorded as part of the human resources policy (see *Templates 2.1* and *2.2*)
- paper documents: contracts, operating and professional guidelines.

2.6 Threat analysis

By doing a threat analysis the practice will better understand and put in place planning to minimise the impact from potential threats and vulnerabilities that could adversely affect the practice. This includes financial loss, breaches in confidentiality, information integrity and availability, and patient confidence. *Template 2.24* has been formulated with the common threats and vulnerabilities that face a general practice, and suggested controls to minimise the risks and impact of these.

The threats have been categorised into three areas:

- human (unintentional and deliberate): for example, the theft of a laptop containing clinical or business information, or inadvertent viewing of a patient's information by non-practice staff or another patient
- technical: for example, a hard disk crash or data corruption from a virus
- environmental: for example, a natural disaster such as a bushfire or flood.

Once the threats and vulnerabilities have been identified, the existing mitigation strategies and security controls implemented in the practice need to be added to *Template 2.24*. Following this step, the existing controls can be compared to those suggested and any additional required controls (actions to take) added to the table. This will form the practice plan for improving the security of practice computer and information systems. This is referred to as a gap analysis.

To decide the actions to take, consideration must be given to the cost-effectiveness of controls for your practice in order to minimise the risks. Control selection will be based on cost, ease of use, integration with normal workflow, importance to practice, and objective of protection. Selection of controls is also impacted by the financial and time constraints of the practice, as well as the technical skill of the practice team.

Note: No system can ever be 100% secure and there will always be some residual risk after the implementation of security controls. This is unavoidable. Indeed, some level of risk acceptance may be necessary because of low possibility of occurrence and the high cost to protect against a risk.

2.7 Security management monitoring and reporting

Document the planned monitoring for compliance with legal obligations and establish a periodic review schedule for the risk assessment process. This is particularly important when computer equipment and software are updated, new uses of information are embarked on (such as health information exchange, the national eHealth record system [PCEHR system] and *Healthcare Identifiers Act 2010* and secondary use of information), practice team members leave or new practice team members commence, when changes occur to legislation or professional requirements, or following incidents or breaches in information security.

2.8 Education

Effective communication and education for the practice team about the risks that the practice computer and information systems are exposed to is an important aspect of risk management. Discussion at practice meetings and including these processes within the governance of the practice are essential. There is also a requirement under the PCEHR legislation and the participation agreement that the policy for interaction with the PCEHR system is written, communicated, enforced and reviewed at least annually (PCEHR Rule 25), and further, that GPs and the practice team are educated in their legal responsibilities in regard to interaction with the PCEHR system. How this is to be undertaken should be written into the practice PCEHR system policy.

2.9 Data breach response and recording

Data breaches can occur through the loss or theft of laptops, mobile devices, removable storage devices, hard disk drives and USB sticks. They also occur through unauthorised access of databases from outside the organisation through hacking, or from inside the organisation through access or disclosure by employees outside the bounds of their roles and authorisation. Not all breaches are intentional. Providing personal information to the wrong person or sending it to the wrong address (physical or electronic) can occur, and sometimes insufficient care is taken to confirm the identity of a person to whom information is disclosed. Data breaches are not limited to electronic records and the security of paper records must also be considered.

The practice policy will document the procedures on the detection, action and reporting of breaches of security. This policy will also incorporate identified ongoing training needs of the practice team, reporting procedures and consequences for noncompliance with the policy. Instructions on what action should be taken if a data breach occurs or is suspected are given in a pro forma in *Appendix C*. A copy can also be found in *Template 2.27.*

Australia has **mandatory** data breach notification requirements for the eHealth record system by the System Operator, registered repository operators and portal operators. The System Operator must notify the Office of the Australian Information Commissioner (OAIC) if a data breach to the PCEHR occurs. (Under the PCEHR Act 2012, this is termed a ‘notifiable’ data breach.) Registered healthcare organisations are not required to report breaches to the OAIC. Breaches of security that do not relate to the PCEHR system are out of scope of the mandatory data breach notification. However, the OAIC encourages voluntary data breach reporting in accordance with the *Privacy Act 1988*. Further information on voluntary data breach notifications can be found on the OAIC website.

Breach or suspected breach notification

Under the conditions of the PCEHR Participation Agreement, Healthcare Provider Organisations must notify the System Operator if a breach or suspected breach has occurred in the circumstances where:

- there is a non-clinical, PCEHR system-related error in a record that has been accessed via, or downloaded from, the PCEHR system, or
- the security of the PCEHR system has been compromised by the healthcare organisation or one of its employees or by the use of its equipment.

The Data Incident/Breach Report form (*Appendix C*) can be used to record all incidents: both accidental and intentional. The information recorded can be used to report incidents as required under the PCEHR Participation Agreement to the System Operator. In addition, the form could be used by the organisation to report any other (future) potential mandatory breach notification to the OAIC. This form can also be found in *Template 2.27*.

2.9.1 What to do if you have or suspect a data breach

All breaches or suspected breaches should be recorded and practice management notified, whether or not the breach is considered major or minor in nature.

Based on the OAIC advice, these steps should be followed:

- Containment of the breach
  - The first step is to contain the breach so that no further damage can be done. Take whatever steps are possible to immediately contain the breach. This may be to isolate the system or disconnect from the internet if this is likely where the breach occurred. If it is not practical to shut down the system (or it might result in a loss of evidence) then suspend user access to the records affected, or suspend a specific user's access.
  - Assess whether steps can be taken to mitigate the harm a consumer may suffer as a result of a breach.
- Initial assessment of the cause of the breach
  - Appoint someone to lead the initial assessment of the breach. This may require technical assistance as the person will need experience in evaluating the cause and be able to make recommendations.
  - The analysis will need to consider what personal information the breach involves, what was the cause of the breach, what the extent of the breach is, and what is the potential impact (harm) to individuals of the breach.
  - Be mindful of not destroying evidence that may be helpful in determining the cause of the breach or in rectifying the problem.
  - Ensure appropriate records of the suspected breach are maintained, including the steps taken to rectify the situation and the decisions made – use the Data Breach/ Incident Report form, which can be found in *Appendix C* and *Template 2.27*.

- Notification of the breach
  - Determine who needs to be notified, both internal and external to the practice, and where relevant:
    - notify the practice management
    - notify the police if theft or criminal activity is suspected
    - notify the PCEHR System Operator (as per the PCEHR Participation Agreement)
    - notify the OAIC.
- Investigation of the breach
  - Ascertain if the information is encrypted or de-identified.
  - Identify who is affected by the breach.
  - Evaluate what the breach information could be used for.
  - Evaluate the risk of harm from the information disclosed by the breach.
  - Determine the risk of further breaches of this type.
  - Determine if this is a systemic or isolated incident.
  - Evaluate what harm could occur to the practice as a result of the breach.

More detail and further guidance on this can be found in the OAIC documents *Data breach notification guidelines* (April 2012) and the *Mandatory data breach notification in the eHealth record system* (September 2012).

Recommendations: Detail the steps that will be put in place to prevent further breaches. For instance, should vulnerability (penetration) testing of the network be undertaken?

Section 3

Standard 3: Information security policies and procedures

Our practice has documented policies and procedures for managing computer and information security

Compliance indicators

The compliance indicators listed in the matrix identify the specific actions that comprise good security practice for Standard 3.

It is assumed the practice will provide appropriate education and training to facilitate compliance with this Standard.

			Minimum
Security policy and procedures compliance indicators	**Level 1 Initial**	**Level 2 Repeatable**	**Level 3 Defined**
3.1 Policy content	No formal policy	No complete written policy	Complete written policy
3.2 Policy communication	Policy not communicated to the practice team	Policy communicated verbally to the practice team	Policy communicated in written format to relevant practice team members
3.3 Compliance indicators	Not done and/or only verbally defined	30% completed	70% completed
3.4 Practice team agreements	Informally defined	Partially documented	Fully documented
3.5 External service provider agreements	Informal verbal	Partial set of standard policies used	Partial set of standard policies adapted for practice
3.6 PCEHR policy	Template used, with practice-specific policy documented	Policy documented and version controlled Ad hoc training on legal responsibilities	Reviewed annually Communicated and accessible to practice team members Education in legal obligations of interaction with the PCEHR regularly reiterated (required to be eligible to register for the PCEHR under PCEHR Rule 25(4))

Adapted and reproduced with permission from Dr Patricia Williams

The compliance indicators at level 3 reflect the minimum level of computer and information security acceptable for this Standard. The compliance indicators for higher levels provide the basis for incremental security improvement.

Helpful templates for this Standard

Templates 1.1–12.1 will assist in achieving compliance. Completion of these templates will ensure you have fully documented the requirements of this Standard.

3.1 Policy content

Practices should document in the policy and procedure manual all of the policies and procedures relating to the security, installation and use of computers, and electronic communication. Responsibilities for each component of computer and information security should be clearly defined, the policies should be clear, and the procedures should contain simple instructions that are easy to follow. It is of utmost importance to think through and discuss the contents of the manual with the practice team to ensure compliance and implementation.

Level 4 Managed	Level 5 Optimised
Complete written policy, periodically reviewed	Complete written policy, reviewed annually
Policy communicated in written format, training provided and all practice team members have access to the policy	Policy available in written format to relevant practice team members Regular training for the practice team and communication strategy reviewed against policy All practice team aware of the content and implications of the policy
90% completed	100% completed
Documented and updated as required Accessible on request	Documented, annually reviewed and updated Accessible to all practice team members
Full set of policies contextualised for practice	Contractual and confidentiality policies written, communicated and annually reviewed
Reviewed annually Communicated and accessible to practice team members Education in legal obligations of interaction with the PCEHR regularly reiterated (required to be eligible to register for the PCEHR under PCEHR Rule 25(4))	Reviewed annually Communicated and accessible to practice team members Education in legal obligations of interaction with the PCEHR regularly reiterated (required to be eligible to register for the PCEHR under PCEHR Rule 25(4))

All policies should have the following general structure:

- purpose and objectives of the policy
- scope of the policy (i.e. to whom and what it applies, and under what circumstances)
- definition of computer and information security incidents and their consequences
- organisational structure and defined roles, responsibilities and levels of authority
- reporting requirements and contact forms.

Additional information on what should be in each section is provided in the relevant section of this document. The templates will provide guidance as to what information should be recorded in the policies.

3.2 Policy communication

The policy should be in written format and communicated to relevant practice team members.

3.3 Compliance indicators

Assessing the practice's current status in relation to the compliance indictors (at the beginning of each Standard section) is important. This provides a simple method to implement improvements in this security status.

3.4 Practice team agreements

A policy and procedures manual provides information and guidance to the practice team on the protocols in managing the computer and information systems. It is a source of information to clarify roles and responsibilities, and to facilitate the orientation of new practice team members. Confidentiality and privacy agreements for practice team members to sign, together with an appropriate computer use agreement (e.g. on internet and email usage), should be included in this manual. All practice team members and others, as identified in the risk assessment, should sign these agreements. These act to protect the owners of the practice in the event of legal action against the practice arising out of a security breach.

A generic confidentiality agreement can be found in *Template 1.4*. This agreement can be used to ensure that practice team members and other people working in a practice who may have access to confidential patient or business information comply with privacy and security of information as required under legislation, including the *Privacy Act 1988* (amended) and the National Privacy Principles.

While there are significant levels of trust inherent in the healthcare environment, caution should be exercised in automatically extending this to external service providers.

3.5 External service provider agreements

There is an onus on the practice to ensure that anyone who has legitimate access to practice clinical and/or business information is aware of their obligations to comply with practice policies related to that information. Since technical service providers and those providing software and system support are usually granted unrestricted access to practice data, the following gives guidelines on what contractual agreements should contain.

Contractual agreements with technical service providers

The practice should have a contract in place for the external service providers they use. Contractual arrangements with outsourced technical service providers should include:

- data confidentiality: sensitive clinical and business information 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 practice team members 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
- 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?
- regular maintenance: does the IT service provider undertake monthly server checks? Does the software provider perform software and drug updates and how often?
- audit log: what audit log checking will be undertaken of the network and how will this be reported to the practice?
- secure disposal of information assets: how are information assets (e.g. backups) disposed of or returned to the practice? (see Section 11)
- cloud services: where is the data stored? What security assurances are provided?

3.6 National eHealth record system (PCEHR) policy

In addition to the computer and information security policy, a policy to cover the specific requirements of the PCEHR Act and Rules is required, as specified in the PCEHR Participation Agreement. Parts of this policy may refer to other practice policies and therefore it is important to ensure that all policies are dated and have version numbers in order to meet the requirements of the legislation.

Templates 1.1, 1.2, 2.26 and *4.1* will make it easier for you to achieve compliance.

Section 4

Standard 4: Managing access

Our practice establishes and monitors authorised access to health information

Compliance indicators

The compliance indicators listed in the matrix identify the specific actions that comprise good security practice for Standard 4.

It is assumed the practice will provide appropriate education and training to facilitate compliance with this Standard.

Managing access compliance indicators		Level 1 Initial	Level 2 Repeatable
4.1 Policy content		No formal policy	No complete written policy
4.2 Policy communication		Policy not communicated to the practice team	Policy communicated verbally to the practice team
4.3 Access rights	**Identification (usernames)**	None	Users share single username
	Authentication for system administrator	No special username or login	Same as for normal username and password
	Authentication of users	None	All users share one password
	Functionality of role	Has access to all systems and functions when logged on	Has access to all systems except administration functions
	Public access	Unknown	Not considered
	Review of accesses	Unknown	Never performed
4.4 Password maintenance	**Change frequency**	None	Ad hoc change
	Type (strong/weak) minimum length and format	None	Short password and words allowed
	Reusability	Not checked (i.e. unrestricted reuse allowed)	Cannot reuse existing password
	Default passwords	Unknown	Account can be created with default or no password

Adapted and reproduced with permission from Dr Patricia Williams

The compliance indicators at level 4 reflect the minimum level of computer and information security acceptable for this Standard. The compliance indicators for higher levels provide the basis for incremental security improvement.

The compliance indicators for managing access are extensive because this is a fundamental and important area of information security and in the protection of both your practice clinical and business information. The processes involved in managing access are numerous and complex, and therefore in this matrix have been deconstructed to be as simple as possible.

Helpful templates for this Standard

Template 4.1 will assist in achieving compliance. Completion of this template will ensure you have fully documented the requirements of this Standard.

	Minimum	
Level 3 Defined	**Level 4 Managed**	**Level 5 Optimised**
Complete written policy	Complete written policy, periodically reviewed	Complete written policy, reviewed annually
Policy communicated in written format to relevant practice team members	Policy communicated in written format, training provided and all practice team members have access to the policy	Policy available in written format to relevant practice team members Regular training for the practice team and communication strategy reviewed against policy All practice team aware of the content and implications of the policy
Single role username used	Unique identification for all systems	Multiple unique identifications for different systems
Single username for all systems administration	Different identification for system administration	Multiple authentication methods for system administration
Group password for group user identification	Individual password	Two-factor authentication for health records
Group-role-based functionality, with no minimum set of accessible functions defined	Group-role-based functionality with minimum set of accessible functions defined	Individual restricted functions to minimum required for role
Ad hoc access allowed	No access	Access with strong authentication and ease of use
Ad hoc	When required	Periodic review for access and review for completeness and accuracy of user information
Policy-suggested frequency change	Periodic change of password and immediately if it has been compromised	Regular password change forced ≤-90 days and immediately if it has been compromised
Allows dictionary words	>6 characters but not enforced	>8 characters with alpha, numeric and special characters enforced
Reuse allowed but not last one used	Reuse allowed after 3 changes	Reuse not allowed
Forced change at first login	Password change enforced at creation	Password change enforced after unsuccessful login attempt

Managing access compliance indicators		Level 1 Initial	Level 2 Repeatable
4.5 Password management	**Who can create/remove users (identifications)**	Unknown or all users	Some users
	Reset passwords	Unknown or all users	Cannot be reset
	Process for removing IDs	Unknown or all users remain active indefinitely	User's password changed only
	Invalid access attempts	Unknown or unlimited	Notify after 3 invalid attempts
4.6 Remote access	**Remote access by vendor**	Unknown	Information systems or software vendor has uncontrolled access to whole system **without** confidentiality agreement in place
	Remote access for normal users	Unknown	All normal users have remote access using normal logins
	Virtual private network (VPN)	Unknown or not used	Group user authentication
	Remote access to server/files systems	Unknown	Open access to servers
	Guest accounts	Unknown	Guest accounts active with default passwords
4.7 Default user accounts		Unknown	Default accounts active with default passwords
Network access controls is dealt with in Standard 9: Computer network perimeter controls		This includes renaming administrator accounts on devices,	
4.8 Auditing	**Recording**	Unknown or access not logged	Access logged
	Review	Unknown or not performed	Audit not reviewed
	Retention period	Not retained	Retained on rolling cycle or can be deleted by users
4.9 Initial definition and permissions management	**Detailed role-based access (job, title, responsibility, role)**	None, unknown	Ad hoc (known but not documented)
	Workgroup-based (clinical team) as to what records are accessible	None, unknown	Ad hoc (known but not documented)
	Discretionary access: who can grant access to other health providers (e.g. specialist) to a patient's record (practice data not PCEHR)?	Unknown	No one allocated
	Secondary use of data access	Requests assessed informally or unknown	Formal assessment on individual basis No practice policy
	Website access	Undefined or informal policy on website access	Written policy

Adapted and reproduced with permission from Dr Patricia Williams

	Minimum	
Level 3 Defined	**Level 4 Managed**	**Level 5 Optimised**
Only external IT support can create or remove users	Multiple system administrators in practice	Practice system administrator only
Only external IT support can reset passwords	Practice manager or system administrator only can reset passwords	Automated system for password reset using user identification
Users removed ad hoc	Users removed at periodic review	In accordance with policy, user IDs archived or removed upon leaving
Reject access after 3 invalid attempts and wait period for exclusion	Reject access after 3 invalid attempts and reset required by user notification	Reject access after 3 invalid attempts and reset required by system administration
Information systems or software vendor has uncontrolled access to whole system **with** confidentiality agreement in place	Limited access to patient data Confidentiality agreement in place	Information systems or software vendor access controlled by practice Vendor default access removed at installation Confidentiality agreement in place
Users have remote access using different logins	Remote access restricted to specific users with different usernames	Disabled or one-time-only remote access sessions for a individual username
Individual user authentication	Individual user authentication	Client authentication (computer used is always authenticated to system in addition to user) and enforced usage for remote access
Limited to servers	Remote server access limited	Administrator remote access to servers only
Guest accounts enabled with passwords changed regularly	Guest accounts disabled	All guest accounts removed
Default accounts active with passwords changed regularly	Default accounts disabled	All default accounts removed except for system administrator
deciding on type of access control to network		
Access and type of change logged for clinical information systems	All logged with minimum details	All access attempts to individual software logged (including date, time, ID, IP, event, action)
Reviewed only for checking	Reviewed as needed	Reviewed, analysed and reported on to meet practice policy
Retained in rolling cycle and read only	Retained but can be deleted by software providers Read only	Retained indefinitely (as per policy/legislation) and restricted access to read only
Detailed for main application only	Detailed once at system installation for applications and operating system	Determined, documented and reviewed annually for all applications and operating system (as defined in risk assessment register)
Detailed for main application only	Detailed once at system installation for applications and operating system	Determined, documented and reviewed annually for all applications and operating system
Decision made ad hoc by person not directly responsible for that patient's care	Decision made ad hoc by patient's treating healthcare professional	Determined, documented and reviewed periodically
Practice policy established and followed No formal documentation of decisions	Written practice policy followed, decisions documented	Secondary use of data policy and decision framework followed All requests and decisions documented as per General Practice Data Governance Council resources
Written policy	Written policy Protected SSL connection	Written policy Protected SSL connection

Explanatory notes

Practice team members should only have access to the systems and information required to enable them to perform their role in the practice. All practice team members require a position description that clearly outlines their roles and responsibilities and the required access to clinical and/or business information. Restricting access reduces the opportunity for accidents and errors. The practice team requires appropriate training in the relevant computer software and the potential risks before access and passwords are provided. Additionally, healthcare identifiers (healthcare provider identifier – individual (HPI-I) and healthcare provider identifier – organisation (HPI-O)) should be recorded in a secure place (for further explanation of these refer to Section 12).

The software will have the capability to provide the appropriate level of access to match the individual user role. In older systems there will be a small number of choices – such as Clinician, Nurse, or Administration. In more advanced systems there will be a permissions matrix that allows access levels to be set to suit a much larger number of practice roles. Individuals can have these further tailored to their particular roles.

Third party access (e.g. external IT consultants) for support and problem solving is an issue that requires careful consideration. This is often undertaken remotely and a great deal of trust is placed in software and support service staff. While technical support personnel will be knowledgeable in IT, they may not fully understand the sensitivity and confidentiality requirements of health information. Hence, technical support provisions should be underpinned by confidentiality agreements and the practice should ensure that the levels of confidentiality required are in alignment and enforced by the third party organisation.

Generally, there are different levels of role and responsibility-based access, such as:

- systems administrator: this level of access is usually the highest and often is only used by IT/security trained and external service providers for the server, operating system and network maintenance functions, and software support
- practice manager: this access usually includes administrative functionality on the financial, clinical and network systems used in the practice
- receptionist: this level of access is for patient administration such as appointments and billing; there may be some limited access to clinical programs
- clinical practice team members (including locums): this level of access is for use of the clinical programs. This access level may be further subdivided where delineation between the doctor, nursing and allied healthcare staff access is required
- other staff, such as researchers, students, software vendors and other healthcare provider organisations: this level of access will vary depending on the activities the person is undertaking.

A table for recording all practice team members, their access levels and permitted software access is provided in *Template 4.1*. Once a policy on access has been determined (i.e. the rights, roles and permissions), then practice team members can be given appropriate authentication methods. These can be divided into the following types:

- something you know (e.g. a password, currently the most common means of authentication)
- something you have (e.g. a token or smartcard)
- something you are (e.g. a biometric profile – fingerprint).

Passwords are the most common form of access authentication. All non-clinical practice staff should have their own passwords and not use a shared common password. Best practice principles are that all of the members of the practice team retain the responsibility for their own passwords and security tokens and do not share them with other members of the team; passwords should not be written down and placed near monitors Two-part authentication methods (a combination of two types of authentication) offer greater security.

A common problem in information security is the failure to remove the access rights of practice team members who leave the practice. It is important for the practice to consider the implications of practice team members 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 practice team members leaving the employment of the practice. A regular review of user access rights is important to help detect where omissions have occurred or when practice team members have changed roles.

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 advice about this and other obligations under state, territory and national privacy laws, and codes of conduct and indemnity or legal advisors.

4.1 Policy content

One of the key features of information security is information can only be accesed by authorised personnel, appropriate to their role in the practice. Practices should develop a policy for who can have access to specific information and systems. This will be driven by the identification of potential system users in the risk assessment activity (*Standard 2*).

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

Practices will need to develop their policy, after identifying and applying a risk analysis, according to the needs of the practice. It is suggested that practices seek the support of suitably qualified technical service providers if needed.

Practice policy should be developed on levels of access to electronic data and information systems. The practice will need to establish an access and password policy that defines the user access level, password structure (number and type of characters) and the frequency with which passwords are required to be changed. All practice team members should create their own login passwords and be responsible for keeping them secure.

It is also important for the practice to consider the implications of practice team members who terminate their employment, to ensure the decommissioning of passwords, remote access logins, and the return of computer equipment, backups and entry devices (keys) to the practice.

The access control policy should include guidance on:

- access rights
- passwords
- management of guest account and remote access accounts
- suspension of access where known or suspected data breach has occurred
- termination of practice team member's access.

4.2 Policy communication

The policy should be in written format and communicated to relevant practice team members.

4.3 Access rights

Access to systems should be consistent with the responsibilities outlined in the role description of each member of the practice team. Each practice team member should create his or her own strong password(s) for access. Passwords should not be written where they can be obtained by other practice team members or people who have access to the premises. The system administrator's password should never be divulged to anyone who is not authorised.

4.4 Password maintenance

Password maintenance is a challenging process. Passwords should be changed immediately if they have been or are suspected of having been compromised. The objective of this section is to raise awareness of the need to have and implement good password policy. The password policy should include the following aspects of password maintenance.

- Practice team members have individual passwords (not generic), which are kept secret and secure. 'Strong' passwords are used and the practice team are trained in the importance of this.
- Individual practice team members are assigned an appropriate access level specific to their role.
- Default user account passwords are changed.
- Passwords are changed periodically (using regular intervals, e.g. every 3 months, is the best practice security recommendation; however, this is difficult to manage for practices and therefore is acknowledged as a goal practices can be working towards). The longer the same password is used, the greater the risk that it will become known and then used, possibly without the user knowing.

- A minimum length is set (i.e. number of characters).
- A mixture of alphabetic and numeric characters and lower and upper case is used.
- Passwords do not use familiar and family names or words that can be found in a dictionary.
- Dates of birth are not used.
- Passwords are not reused.
- Passwords are not disclosed to anyone and others are not allowed to use your login.
- Passwords are not written down and attached to screens.
- Logins are not shared (i.e. people in the same role do not use the same username and password).

4.5 Password management

The password policy and practice should include the following aspects of password management:

- specification of who can create and remove users on each practice information system
- specification of who has authority to reset user passwords
- specification that a practice team member's access will be removed when they are no longer working at the practice
- specification of the temporary disabling or removal of access passwords where a data breach is known or suspected.

4.6 Remote access

Management of guest accounts and remote access accounts may include:

- the process to establish guest accounts
- the process to remove unused or unnecessary guest accounts.

Where access to practice systems by external service providers is required, 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 *Template 1.4*.

4.7 Default user accounts

All operating systems and some software applications have default user accounts at installation. These should be removed where possible or the default passwords changed.

4.8 Auditing

Auditing of access to applications and information, as well as downloading information, should be enabled. This should include actions performed (access, modification and deletion) and be identifiable by individual user. The audit logs should be reviewed periodically.

4.9 Initial definition and permissions management

The following definitions and permissions management decisions should be documented. This task only needs to be done once or when changes in practice occur.

- Detailed role-based access (job, title, responsibility, role).
- Workgroup-based (clinical team) as to what records are accessible.
- Discretionary access: who can grant access to others (e.g. other healthcare provider) to a patient's record.
- Secondary use of data access: refer to the General Practice Data Governance Council website (www.gpdgc.org.au) for further information and a decision-making tool on who can access your data for secondary use purposes.
- Website content and access for website maintenance and content changes.

Section 5

Standard 5: Business continuity and information recovery

Our practice has documented and tested plans for business continuity and information recovery

Compliance indicators

The compliance indicators listed in the matrix identify the specific actions that comprise good security practice for Standard 5.

It is assumed the practice will provide appropriate education and training to facilitate compliance with this Standard.

The compliance indicators at level 4 reflect the minimum level of computer and information security acceptable for this Standard. The compliance indicators for higher levels provide the basis for incremental security improvement.

Helpful templates for this Standard

Templates 5.1–5.10 will assist in achieving compliance*.* Completion of these templates will ensure you have fully documented the requirements of this Standard.

Explanatory notes

Practical and implementable business continuity and information recovery plans are critical elements of computer and information security.

With the increasing dependence on electronic information systems and access to information, these plans contribute to good governance processes within a practice. Management and recovery from a computer malfunction or security incident needs to be planned for. A business continuity plan will help ensure business continuation, ensure less inconvenience to patients, and assist prompt recovery of systems. The objective of clear and simple plans is that practice team members fully understand the plan and what they need to do to action it when there is a disruptive event, a crisis or disaster situation. It is important that the whole practice team know their individual roles and responsibilities in such events.

The process for developing and implementing business continuity and information recovery described here is based on current established standards and has been simplified to be implementable by the practice with minimal technical assistance.

Business continuity and information recovery compliance indicators		Level 1 Initial	Level 2 Repeatable	Level 3 Defined
5.1 Policy content		No formal policy	No complete written policy	Complete written policy
5.2 Policy communication		Policy not communicated to the practice team	Policy communicated verbally to the practice team	Policy communicated in written format to relevant practice team members
5.3 Business continuity and information recovery plans	**Plans**	No formally documented plan	Plans are informal but not documented	Plans are partially developed and documented
	Critical business functions	Identified but not documented	Informally developed but undocumented	Partially developed and documented
	Processes defined	Identified but not documented	Informally defined, undocumented	Partially developed and documented
	Additional resources	Not identified	Informally identified	Partially identified and documented
	Alternative procedures (preparedness)	Not assessed	Alternative procedures developed ad hoc	Alternative procedures identified but not documented
5.4 Education		None provided	Ad hoc training	Training prompted by incidents
5.5 Plan testing		No business continuity plan testing	Business continuity plan testing ad hoc	Business continuity plan testing driven by incidents only
5.6 Fault recording (fault log)		Faults not recorded	Ad hoc recording of faults	Major faults recorded

Adapted and reproduced with permission from Dr Patricia Williams

5.1 Policy content

Business continuity

A business continuity plan ensures continued practice operations when computer system failure occurs. The plan should concentrate on internal system malfunction or failure; however, the broader scenario should also be included, such as the functioning of the practice in the event of an environmental or natural disaster. This includes consideration of the transfer of information to and from the practice to other healthcare providers (pathology laboratories, radiology providers, specialists and hospitals), new e-health services (electronic transfer of prescriptions) and government bodies (Medicare).

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. This will have been documented as part of the risk assessment process (*Standard 2*).

Minimum	
Level 4 Managed	Level 5 Optimised
Complete written policy, periodically reviewed	Complete written policy, reviewed annually
Policy communicated in written format, training provided and all practice team members have access to the policy	Policy available in written format to relevant practice team members Regular training for the practice team and communication strategy reviewed against policy All practice team aware of the content and implications of the policy
Plans are fully developed	Plans are fully developed and tested
Fully documented	Fully documented and tested Contacts listed and responsibilities assigned
Fully documented	Process fully documented and tested
Identified but not budgeted	Additional requirements for practice staff resources and equipment identified and allocated Budget allocated
Alternative procedures formally documented	Alternative procedures formally documented and reviewed periodically for currency
Ongoing education at practice team meetings	Ongoing education at practice team meetings Planned training (bi yearly) practical exercises
Business continuity plan testing intervals established	Business continuity plan testing intervals established and specific dates diarised
All faults recorded	All faults recorded and fault log periodically reviewed and analysed

Information (disaster) recovery

An effective disaster recovery plan will bring the computer system back to working order, including the restoration of data. This is an increasingly technical and difficult area, and practices are well advised to consult a technical service provider. Some failures in the computer system can be very simple. However, a disaster implies a major computer failure such as the server being inoperable. It is very important to know quickly when a computer problem can be fixed inhouse and when it requires assistance from a technical service provider.

Data backup and restoration is one part of a business continuity plan and is referred to in this document as information recovery. Backups are an integral part of the information recovery process. Information recovery corrective procedure examples are provided in *Templates 5.2–5.10.*

5.2 Policy communication

The policy should be in written form and communicated to relevant practice team members.

5.3 Business continuity and information recovery plans

This section leads you through the steps required to create a business continuity plan, and details the functions, resources and procedures that are common to most general practices. The plan should be reviewed at specified time intervals (e.g. annually or if something changes such as the backup medium or procedure). Forms for recording the relevant information in a plan, together with examples, are provided in *Templates 5.1–5.10*.

When developing a business continuity plan, the first step is to identify the critical business functions and the resources required to operate the practice at a minimum acceptable level without functional computers. If a significant computer failure occurs, practices need to know how practice systems will be managed 'manually' and the information to be collected for re-entering after recovery. Therefore, the plan must include advice on how to revert to a paper-based system until the computers are functional again (e.g. prescriptions can be written on the electronic script paper) and should cover basic practice systems such as:

- enabling clinical team members to provide adequate clinical care while not having access to electronic health records
- appointment scheduling
- billing
- business financial operations (payroll, Medicare claims).

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 patients and practice team members. Second, the information (disaster) recovery plan should contain the information necessary for returning the practice to its normal state and to minimise downtime. 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'. The development of an information recovery plan is usually in consultation with the GPs, practice team and technical service provider. The Computer Security Coordinator is responsible for managing this task.

A fundamental principle in developing plans is that they are simple to understand and follow. In general there are three levels of response:

- emergency (first) response: this involves protection of people and property from immediate harm
- continuity phase: the processes and procedures to ensure the practice continues to meet its critical functions at a minimum acceptable level
- recovery phase: the processes and procedures to re-establish normal operation.

Identify critical practice functions

These functions should include:

- clinical and business functions
- identifying the system normally used to undertake a task and the resources required to complete the task if the system is not available.

A further consideration is noting any critical times of the month that activities usually have to take place. This may include payroll or end-of-month processes.

Identify additional resources that will be required for continuity and recovery

A practice needs to consider what organisational capacity and knowledge it already has in order to manage and implement the strategies detailed in the plans. What additional resources may be needed? To assist in identifying possible resource requirements, these have been categorised in the tables in *Template 5.2*.

Document continuity and recovery processes, including alternative work procedures

This section has been structured to reflect the emergency, continuity and recovery phases, as follows.

Emergency response

The emergency and evacuation procedures will already be defined for the practice in the case of emergencies and natural disasters. First and foremost, these are in place to protect and preserve life.

Continuity phase

This phase concerns how to convert to manual procedures for critical practice functions. Each critical function in the practice requires a contingency plan so that when things go wrong the practice can continue to operate, and this includes the computer systems. Critical functions can be divided into either business or clinical. The practice needs to identify the major functions that are required to run the practice and how these will continue should the computer system be inoperable. Consider the following:

- access to a laptop computer with copy of database on it
- access to the contact details of the key practice staff
- access to patient contact details
- work-around processes (for all critical functions identified). Some procedures and examples are provided in *Template 5.4.*

Recovery phase

The recovery phase involves assessing the problem, taking corrective action, restoring the system, entering the backlog of information, communicating with those affected, and undertaking a post-incident review. These tasks are discussed below.

Assess the computer problem

An assessment of the computer problem should be documented and include the following items:

- writing down or capturing ('print screen') any error messages
- noting anything that changed prior to the system failing
- checking that all power and network connections and cables are plugged in and that the devices are turned on (check that lights are on).

Perform corrective action (with or without technical support)

Complete the tables given in *Template 5.5* and add any further items from past practice experience. Discuss them with your technical service provider. While these are listed as separate incidents it should be remembered that sometimes attacks have multiple components, such as malware (e.g. trojan), on your computer that leads to unauthorised access.

It is important that the practice Computer Security Coordinator knows the realistic capability of the practice to correct and recover from incidents to ensure that time is not wasted if technical assistance is required.

Restore system and reconfigure

The restore procedure is detailed in Section 7 (Information backup). The information recorded in the risk assessment (e.g. assets and their settings, users and their access levels) will be used for this. This task involves establishing procedures to test that the systems are functional. Systems checks will vary depending on the identified malfunction.

Enter backlog of information

This may need to be undertaken prior to resuming normal operations depending on the systems used in the practice and if information is required to be entered chronologically. You may need to consult with your software provider to ascertain this.

Template 5.6 lists common tasks to assist you in planning what information will need to be entered or re-entered into the computer system, how this will be done and who will undertake this task. There should be plans for both entering data that was processed manually, including re-entering data if the system had to be restored from a previous backup.

Note: In the event of short and medium term events, follow-up with external information transfer and exchange healthcare organisations may be necessary to ensure that any data that was transmitted during the time of non-operation is transmitted again.

Communicate with those affected

Practice team members, patients, other healthcare providers, technical support providers and relevant authorities may need to be informed following an incident. Use the contact list in *Template 2.2*.

Review following recovery

Review the reason for the problem and ascertain how the recovery was executed, update the computer set-up, document any important lessons, and update the policy and procedures manual. This step might involve modifying the software, backup process or acquiring new components. Further, consideration of insurance claims and policies may be necessary.

Assess current preparedness and actions to be taken

Assess and document (in an action plan) what needs to be put in place to support the alternative procedures and access to additional resources. This will include the following:

- computer equipment redundancy
- human resources
- facilities
- communications
- data
- paper records
- technical assistance.

5.4 Education

Education and training of the whole practice team in business continuity procedures is vital, so that when a disaster occurs all practice team members know what to do and what role and responsibility they have, so they are confident they can safely and efficiently handle these adverse events. This training activity can be undertaken using practical exercises in the same way fire drills are practised. Alternatively, such plans could be points of discussion at monthly practice meetings.

Consider planning for bi-yearly practical exercises and the scheduling of regular discussion on business continuity and information recovery at regular practice team meetings.

5.5 Plan testing

Business continuity and information recovery plans should be tested at specified intervals. Determine the interval or specific dates the plans are to be tested and schedule them into the practice diary.

Business continuity and information recovery plans should be updated at specified intervals and when technological or procedural changes occur. It is important to keep the business continuity and information recovery plans current. This means updating them when new equipment is installed or when the practice procedures change.

5.6 Fault recording (fault log)

Any fault or incident should be recorded. A form is provided in *Template 5.10*.

Section 6

Standard 6: Internet and email usage

Our practice has processes in place to ensure the safe and proper use of internet and email in accordance with practice policies and procedures for managing information security

Compliance indicators

The compliance indicators listed in the matrix identify the specific actions that comprise good security practice for Standard 6.

It is assumed the practice will provide appropriate education and training to facilitate compliance with this Standard.

The compliance indicators at level 3 reflect the minimum level of computer and information security acceptable for this Standard. The compliance indicators for higher levels provide the basis for incremental security improvement.

			Minimum
Internet and email usage compliance indicators	Level 1 Initial	Level 2 Repeatable	Level 3 Defined
6.1 Policy content	No formal policy	No complete written policy	Complete written policy
6.2 Policy communication	Policy not communicated to the practice team	Policy communicated verbally to the practice team	Policy communicated in written format to relevant practice team members
6.3 Internet configuration	No usage monitoring Open access to all sites or usage configuration unknown	Monitoring after incidents only Open access to all sites Reactive monitoring only	Monitoring and access control to certain sites and incidents
6.4 Internet use education	Training at induction only or no training	Ad hoc training following incidents or policy breaches and at induction	All practice team members trained in good practice and policy
6.5 Email configuration	No monitoring of email usage Open use of all email accounts (e.g. Hotmail) No limitations on email use or configuration unknown	Monitoring after incidents only Open use of all email accounts (e.g. Hotmail)	Ad hoc monitoring Reasonable use of email permitted No confidential information sent via insecure email
6.6 Email use education	Training at induction only or no training	Ad hoc training following incidents or policy breaches	All practice team members trained in good practice and policy

Adapted and reproduced with permission from Dr Patricia Williams

Helpful templates for this Standard

There are no additional templates for this section.

Explanatory notes

There are many applications (programs) that can be installed that can be harmful to practice information and computer systems. While a significant amount of trust is placed in practice team members, it is remiss to disregard essential security measures that minimise potential risks in relation to usage of computer resources. Uses of external applications, software, websites and programs that can transmit information outside the practice pose a considerable security risk. This encompasses the use of both internet and email programs.

As social networking applications such as Facebook and Twitter have risen in popularity, the practice needs to be mindful of the desire of staff to be 'constantly connected'. Therefore a reasonable use of internet and email policy should be provided. This will guide practice team members as to what is acceptable in the use of the practice internet and email. Limiting use of internet applications will also assist in defending against software attacks and the subsequent necessity for support services to fix these.

Level 4 Managed	Level 5 Optimised
Complete written policy, periodically reviewed	Complete written policy, reviewed annually
Policy communicated in written format, training provided and all practice team members have access to the policy	Policy available in written format to relevant practice team members Regular training for the practice team and communication strategy reviewed against policy All practice team aware of the content and implications of the policy
Manual monitoring of usage Regular reporting	Automatic usage monitoring and scheduled reporting and analysis, informing change in policy or prompting reinforcement of policy, whitelisting used
All practice team members trained in policy requirements and good practice Training in recognition of spyware	All practice team members receive ongoing education on recognition of insecure practices Record of education time and content Practice team members have signed a conditions of employment document about internet use
Manual monitoring of usage Email restricted to practice email only No confidential information sent via insecure email	Automatic usage monitoring and scheduled reporting and analysis, informing change in policy or prompting reinforcement of policy Sender policy framework and domain key identified mail used
All practice team members trained in policy requirements and good practice Practice team members can recognise spam and respond appropriately	All practice team members receive ongoing education in policy /processes in practice Practice team members able to detect unsafe email Practice team members have signed a conditions of employment document about email use

6.1 Policy content

Developing a practice policy that clearly defines and describes the management and use of internet and email by all practice team members within the practice will assist in mitigating security risks. This policy may also detail the practice policy on access to social networking websites such as Facebook and Twitter. The practice may develop a policy on what constitutes reasonable private use of internet and email by practice team members during office hours.

The practice policy will inform and guide the practice team on how to manage and use the internet and email. For example, is occasional personal use of the internet during lunch breaks allowed? The policy must provide guidance to all practice team members on the responsible use of these resources.

Make practice team members aware that it is not permitted to send emails that might be construed as offensive or sexually harassing to anyone.

If the practice chooses to communicate with patients via email or other electronic means, explain to patients and the practice team (e.g. 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. Refer to the RACGP *Standards for general practices* (4th edition) for further information.

The practice needs to communicate to patients the way in which it will meet its privacy obligations. You can inform patients that no confidential information should be transmitted without encryption or other secure means. 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.

6.2 Policy communication

The policy should be in written format and communicated to relevant practice team members.

6.3 Internet configuration

Suggested considerations for appropriate internet use and configuration include:

- internet use for business, clinical and research purposes only
- all downloads accessed from the internet must be scanned for viruses
- all sites accessed must comply with legal and ethical standards and practice policy
- web browser security settings are not to be changed without authorisation.

Methods for limiting internet use could include the blocking of specific sites and applications; this can be set up by technical service providers. This is called whitelisting (permissible) and blacklisting (impermissible) website listing.

Configuring a sender policy framework is an advanced method to mitigate spoofed emails. Email spoofing is where an email appears to have originated from one source when it was sent from a fake email address. It is used to trick the user, much like phishing emails. Common examples of spoofed email that could affect the security of your system include emails alleging to be from the system administrator requesting password changes to specific characters, which often threaten suspension of an account if this is not done, or email requesting users to send copies of sensitive information or passwords. A sender policy framework has to be set up in conjunction with your email system and will require technical assistance. You can also use domain keys identified email using cryptographic authentication for recognised domain names.

Specific actions must include:

- installing and using antivirus and anti-malware software, centrally installed and managed and locally deployed: keep this software active at all times
- installing anti-spyware software (from a reputable supplier): ensure currency by setting up automatic updates and periodically check manually that the anti-spyware is current
- applying patches to operating systems and application programs following advice from technical support providers.

Protection against hackers

- Install hardware and/or software network perimeter controls such as firewalls and intrusion detection systems between computers and the internet (following advice from technical support providers).
- If you install a software firewall, ensure that the practice knows how to use it (centrally installed, centrally managed).
- Ask the technical support providers 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 the practice network.

6.4 Internet use education

Practice team members should be educated and trained in best practice processes when using the internet. This includes learning about protection measures against viruses and spyware.

Protection against viruses

- 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 (note this does not relate to the clinical secure messaging but to attachments received through email and websites).
- Do not run programs directly from websites. If files are downloaded, check for viruses first.
- Enable security settings in your internet browser to medium or high.
- Consider using internet browsers and email programs that are more secure.

Protection against spyware

- Learn how to recognise (and delete) spyware.
- Do not accept certificates or downloads from suspect sites.

General protection

- If you have a useful list of internet favourites or bookmarks make a backup of the list.

6.5 Email configuration

Communication of clinical information to and from healthcare providers should be done from within the practice’s clinical software using a secure clinical messaging system. The use of a practice’s clinical software means that a record of communication is automatically retained in the patient’s medical record.

Protection against spam

- Use a spam filtering program.

Encryption of patient information

- Use server to server encryption such as SSL or TLS.

6.6 Email use education

General protection

- If you rely on information held in your emails make sure that it is backed up with the rest of your data.
- Do not download or open any email attachments where the sender is not known to you.
- Email use that breaches ethical behaviours and/or violates copyright is prohibited.
- Do not send or forward unsolicited email messages, including the sending of ‘junk mail’ or other advertising material (email spam).
- Do not use email for broadcast messages on personal, political or non-business matters.

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 (e.g. apparent emails from your bank).
- Use a spam filtering program.

Encryption of patient information

- All email communications should be treated as confidential.
- When sending patient information or other confidential data by email, it is best practice to use 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.

Protection against the theft of information

- There are significant risks if providing confidential information by email: only do so via the internet when the site displays a security lock on the task bar and with an https in the web address.
- Do not inform people of your email password.
- Be aware of phishing scams requesting logon or personal information (these may be via email or telephone).

Section 7

Standard 7: Information backup

Our practice has a reliable information backup system to support timely access to business and clinical information

Compliance indicators

The compliance indicators listed in the matrix identify the specific actions that comprise good security practice for Standard 7.

It is assumed the practice will provide appropriate education and training to facilitate compliance with this Standard.

Information backup compliance indicators	Level 1 Initial	Level 2 Repeatable	Level 3 Defined
7.1 Policy content	No formal policy	No complete written policy	Complete written policy
7.2 Policy communication	Policy not communicated to the practice team	Policy communicated verbally to the practice team	Policy communicated in written format to relevant practice team members
7.3 Backup frequency	None or manual initiation of backup on ad hoc basis, or frequency unknown	Manual initiation of backup weekly or every few days	Manual initiation of backup daily
7.4 Backup type	Unknown or partial (data only) or incremental	Partial (data and setup files)	Full: all data
7.5 Backup encryption	Unknown	Not used	Encrypted
7.6 Backup reliability	Backup not checked or reliability unknown	Backup checked for completion	Backup periodically checked for reliability
7.7 Backup restoration	Never restored or restore status unknown	Ad hoc restoration	Manually restored
7.8 Backup media	Unknown or obsolete media (e.g. floppy)	Jaz/ZIP or tape (e.g. DAT/QIC) media	CD/DVD
7.9 Media rotation	No rotation or rotation unknown	Daily	Daily and weekly
7.10 Backup storage	Unsecured in practice (e.g. next to computer)	Secure onsite (e.g. in a safe) or offsite	Secure onsite and secure offsite
7.11 Backup access	Uncontrolled or access not known	Open access	Appropriate practice team members
7.12 Legacy systems data storage	Unknown access to previous backup technology or previous technology unknown	Unknown access to previous backup technology	Access to previous backup technology

Adapted and reproduced with permission from Dr Patricia Williams

The compliance indicators at level 4 reflect the minimum level of computer and information security acceptable for this Standard. The compliance indicators for higher levels provide the basis for incremental security improvement.

Helpful templates for this Standard

Templates 7.1–7.3 will assist in achieving compliance. Completion of these templates will ensure you have fully documented the requirements of this Standard.

Explanatory notes

Data can be lost through human error, software malfunction or failure, hardware problems and external causes such as theft or natural disasters. 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 clinical and business information and software in case any of these occur. Also, the longer term preservation and access to health records needs to be maintained.

Minimum	
Level 4 Managed	**Level 5 Optimised**
Complete written policy, periodically reviewed	Complete written policy, reviewed annually
Policy communicated in written format, training provided and all practice team members have access to the policy	Policy available in written format to relevant practice team members Regular training for the practice team and communication strategy reviewed against policy All practice team aware of the content and implications of the policy
Automatic initiation of backup daily	Automatic initiation of backup Continuous or real time with checks in place
Full: all data and programs	Full systems back up or imaging, including operating system
Encrypted with password	All backups encrypted and password protected
Backup periodically checked for reliability and outcome tracked	Backup reliability tested with automatic notification Every backup has outcome tracked
Regularly manually restored	Fully automated restoration
Second hard disk, raid configuration, solid state or to other computer/laptop	Removable hard disk or networked storage that is not generally accessible across the network or on a separate network or offsite (cloud)
Daily, weekly and monthly	Daily, weekly, monthly and annual
Current backup securely stored onsite and current backup stored security stored offsite	Multiple copies of current backup securely stored onsite and current backup stored securely offsite
Authorised practice team members	Authorised practice team members, fully trained
Access to previous backup technology and readability of previous media tested	Data transferred from previous backup technology media to current one and verified Encrypted

Storage and retrieval of information are a high priority in information security. A reliable and tested backup procedure is vital, as is the ability to restore all practice information after a computer incident. Knowing when to seek technical assistance is essential, and timely access to the latest backup (knowing where it can be located) is important.

The backup procedures are an integral part of the practice's business continuity and information recovery plans (see Section 5).

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 long will it take?
- How can you check that the backup system works every time?
- If you store any health information offsite, does this information reside on Australian soil?

The installation of a backup system requires technical skills and is best provided by a technical service provider. There are several important points regarding backup and the backup procedures.

Backup and data restoration procedures are a vital component of the business continuity plan. However, as the optimal method of backup and restoration is quite technical, practices are advised to consult with a technical expert on these matters. Document the backup process using the forms provided in *Templates 7.1–7.3*.

7.1 Policy content

Details of the backup and recovery procedures should be documented. The backup procedure is a key component of the business continuity and information recovery plans. Ensure that backup media are taken offsite when the practice is closed. Record which members of the practice team perform the backup 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 ensure that it is being done regularly.

7.2 Policy communication

The policy should be in written format and communicated to relevant practice team members.

7.3 Backup frequency

A distinction should be made between the daily backup (stored offsite and used to restore data when necessary) and weekly, monthly and yearly archives (used for long-term data retention and legal purposes). A distinction should be made between system backups versus business and clinical data backups: business and clinical data backups must be performed daily, while system backups can be performed less frequently as the operating system and software change less frequently.

7.4 Backup type

Any changes to data and files should be backed up. This includes practice management and clinical systems data as well as other relevant documents, email files, user profiles including desktop settings and internet favourites and bookmarks. You may require different backup and recovery procedures to manage these requirements. While you do not need to back up your operating system or programs daily as these can be restored from the original media, it is a good idea to periodically back up the entire server. This can be done using disk imaging software as it takes an identical copy, or 'image' of your computer hard drive. Continuous backup should be considered as an option where you have two onsite servers.

Note: It is important to keep a correct and current copy of the computer practice and policy procedure manual offsite so that if there is a systems failure, there is ready access to the restoration and business continuity procedures.

7.5 Backup encryption

All backups and archived data should be encrypted and password protected where possible and kept in secure locations.

7.6 Backup reliability

A common problem is that the verification step of the backup process (did it work) is overlooked or not undertaken. Unfortunately, backup failures are often only detected when it is necessary to use the backup for restoration purposes. It is vital that a process is established for determining that the backup has successfully completed.

7.7 Backup restoration

Data restoration is the knowledge of 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 that defines which programs were on the computer and how they were configured. This needs to be done by or under the guidance of a technical service provider. Appropriate documentation of the process in your risk assessment and asset register is therefore important.

In addition, the restoration process needs to be periodically tested and validated. More frequent restoration reduces the risk of data loss and practice downtime. In most instances the restoration process should be automated. If it is not set up to be automated, the restoration process will need to be actioned by, or under the guidance of, your technical service provider. It is recommended that an authorised person in the practice visually checks the restored data. One method is to ensure the last patient entry from the previous day is present on the restored system.

The process for backup restoration needs to be documented, so that if required the backup can be used to restore all or part of your practice data and programs. There are important issues to be considered regarding testing the backup and restoration procedures.

7.8 Backup media

Choosing the appropriate backup software and hardware for individual practice circumstances is important. There are many types of backup media and programs to choose from and because of the rapid changing IT environment, practices should seek technical advice. Common backup media include read/writeable DVD/CD-ROM and portable hard drives. Also, in a networked environment the backup method can include transfer of data to another computer over the network or to an online backup service via the internet. If the backup is performed across the network, practices should ensure that this backup is not accessible across the normal network from the internet. Unauthorised access into a network that has the backup also fully accessible to the whole network is an added vulnerability. At least one current backup should be kept offsite or segregated from the network.

It is important to be observant for potential problems within the systems that manage data, including backups. It is useful to have a series of backups so that you can restore a file from a point before the problem occurred. Having a system of daily, weekly, monthly and annual backups enables you to do this.

For daily backups, use a different tape, CD, DVD or hard drive. Label them by the day of the week, and use the appropriately named tape or hard drive (e.g. Monday data is always backed up (overwritten) on the media marked Monday).

7.9 Media rotation

Backup media must be cycled so that at any point in time there are multiple backup copies of the practice data. If practicable, more than one backup method should be used. A suggested backup rotation strategy for portable media and associated recording sheet can be found in *Template 7.2*. A backup rotation is not applicable to networked or online backup.

- Weekly backups: have backup media labelled 'Week #1', 'Week #2'. This should be used once every week of each month (e.g. every Friday). Therefore 'Week #1' would be used on the first Friday of each month, 'Week #2' on the second Friday of each month, and so on.
- Monthly backups: have one backup media labelled 'Monthly'. This should be used once every month (e.g. on the first working day of each month).
- Annual backup: this should be done at the end of the financial year.

Note: While this section gives details for physical media, network and online backup is also an option. This should not, however, be the only form of backup used. Consult your technical service provider for setup of network and online backup.

The backup rotation procedure will be dependent on the type of backup media and the process and software used. An example backup rotation schedule is provided in the *Templates* for Standard 7. This can be printed each month as a reminder of which media to use and record that the backup has been executed and checked.

7.10 Backup storage

The physical protection of backup media is important. It should be securely stored and access to it controlled. Leaving backups next to the computer or in publicly accessible areas creates a security risk. Ensure that backups are taken offsite daily and stored in a secure environment (e.g. not left in cars or subject to heat). This includes awareness of who has the most recent backup at any one time.

Continuous backup (real-time) is best practice as it protects against business downtime. Practices should consider the costs associated with a server failure versus the initial capital cost of installing a second server.

7.11 Backup access

There should be restrictions on who can access the backup.

7.12 Legacy systems data storage

The practice policy on backup process should also include the procedures for keeping archived data (e.g. yearly backups) to ensure that they are able to be read by current hardware.

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 of and adhere to the national and state records legislation in regards to the retention of patient information. The archive backups form part of this requirement. 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.

Section 8

Standard 8: Malware, viruses and email threats

Our practice has reliable protection against computer malware and viruses

Compliance indicators

The compliance indicators listed in the matrix identify the specific actions that comprise good security practice for Standard 8.

It is assumed the practice will provide appropriate education and training to facilitate compliance with this Standard.

The compliance indicators at level 4 reflect the minimum level of computer and information security acceptable for this Standard. The compliance indicators for higher levels provide the basis for incremental security improvement.

Malware, viruses and email threats compliance indicators	Level 1 Initial	Level 2 Repeatable	Level 3 Defined
8.1 Policy content	No formal policy	No complete written policy	Complete written policy
8.2 Policy communication	Policy not communicated to the practice team	Policy communicated verbally to the practice team	Policy communicated in written format to relevant practice team members
8.3 Software (antivirus/anti-malware)	Software installed at internet service provider (ISP)	Installed on practice server only	Installed on practice server and main computer
8.4 Updates	Anti-virus not updated, update status unknown	Manual updates ad hoc	Manual daily updates on all computers
8.5 Scanning	Manual scanning when prompted by incident	Periodic (regular) manual scanning	Automatic scanning every 3 months
8.6 Education	None provided or unknown	Ad hoc training	Training prompted by incidents
Adapted and reproduced with permission from Dr Patricia Williams			

Helpful templates for this Standard

Template 8.1 will assist in achieving compliance. Completion of this template will ensure you have fully documented the requirements of this Standard.

Explanatory notes

Malicious code (malware) includes viruses, worms and trojans. Malware can have many purposes and intentionally seeks to corrupt, destroy or steal data, or to use your computer for unauthorised purposes. Malware can interfere with computer functioning, resulting in minor inconvenience or in extreme cases system inoperability. Certain types of malware can also capture your passwords (e.g. key logging) and this is one reason why passwords should be changed regularly.

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

There are also various email threats such as phishing and spam. Other threats associated with internet use include spyware, adware and cookies. These types of threats are described in the glossary.

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 security and privacy settings would lower the risk of infection.

Minimum	
Level 4 Managed	**Level 5 Optimised**
Complete written policy, periodically reviewed	Complete written policy, reviewed annually
Policy communicated in written format, training provided and all practice team members have access to the policy	Policy available in written format to relevant practice team members Regular training for the practice team and communication strategy reviewed against policy All practice team aware of the content and implications of the policy
Installed on all practice computers	Installed on all computers and mobile devices (practice and personal) that connect to the practice system
Automatic data/signature file updates on server Weekly updates on other computers	Automatic daily updates on all computers and devices
Automatic scanning monthly	Automatic weekly, full scans of all computers
Ongoing education at practice meetings	Ongoing education at practice meetings Planned additional training (bi-yearly)

8.1 Policy content

Malware and virus software installation and monitoring procedures should be documented. This should also include advice on what to do if malware is detected.

This policy provides a guide to protection from malware. It should include:

- all computers attached to the practice network must have installed and fully enabled virus and malware checking software
- malware protection software that is not disabled or bypassed, nor the settings adjusted to reduce their effectiveness. This means that general users of the system are not authorised to alter these settings
- automatically updating malware protection software and its data files should be enabled for daily updating. This can be done overnight, so as not to impact on system response time. Technical advice may be required
- automatically scanning all email attachments
- automatically scanning all documents imported into the computer system
- nightly scanning of all computers
- training to detect and report all malware incidents
- practice team members trained in malware prevention procedures
- practice team members trained in malware detection and to report all incidents
- turn off the cookies feature in web browsers, although some legitimate software may need this to function properly.

8.2 Policy communication

The policy should be in written format and communicated to relevant practice team members.

8.3 Software (antivirus/anti-malware)

Antivirus and anti-malware software should be installed on all computers and servers. It should be centrally installed and controlled.

The risk of malware infection can be minimised by having a process in place that minimises the risk of downloading malware (e.g. checking email attachments for viruses, segregating downloading files until established they are safe, and turning off cookies).

8.4 Updates

Automatic updating of virus and malware definitions should be enabled on all computers and servers.

8.5 Scanning

Automatic scans of computers should be enabled and occur regularly.

8.6 Education

Practice team members should be educated and trained:

- not to respond or click on links in emails from unknown sources
- to only open attachments where the source of the file is known
- to ensure all files downloaded from the internet are scanned for viruses
- how to respond to pop-up messages from antivirus software
- to report unusual activity on the system, as no malware software is 100% effective.

Section 9

Standard 9: Computer network perimeter controls

Our practice has reliable network perimeter controls

Compliance indicators

The compliance indicators listed in the matrix identify the specific actions that comprise good security practice for Standard 9.

				Minimum
Computer network perimeter controls compliance indicators		**Level 1 Initial**	**Level 2 Repeatable**	**Level 3 Defined**
9.1 Policy content		No formal policy	No complete written policy	Complete written policy
9.2 Policy communication		Policy not communicated to the practice team	Policy communicated verbally to the practice team	Policy communicated in written format to relevant practice team members
9.3 Firewall	**Firewall configuration**	Internet service provider gateway- based firewall used	Local LAN firewall, default installation setup	Local LAN firewall set up to meet practice policy
	Firewall monitoring	No activity monitoring	Manual monitoring of some systems activities	System-prompted exception monitoring
	Firewall auditing	No auditing/log file examination	Manually basic security log files examined	Log files examined periodically
9.4 Intrusion detection system (IDS)	**IDS configuration**	Default configuration	Installation setup (no practice policy link)	Periodic automated check of some system and network vulnerabilities
	IDS activity monitoring	No activity monitoring	Manual monitoring of some system activities	System-prompted exception monitoring
	IDS auditing	No auditing or log file examination	Security log files examined manually	Log files examined periodically
9.5 Demilitarised zone (DMZ)		Not installed or status unknown	Pseudo DMZ using router	Installed for web services
9.6 Secure remote access: virtual private network (VPN) and remote desktop protocol (RDP) (also see Access control)		Not installed for remote connections	RDP used without additional security	RDP with additional SSL TLS security

Adapted and reproduced with permission from Dr Patricia Williams

It is assumed the practice will provide appropriate education and training to facilitate compliance with this Standard.

The compliance indicators at level 3 reflect the minimum level of computer and information security acceptable for this Standard. The compliance indicators for higher levels provide the basis for incremental security improvement.

Helpful templates for this Standard

Templates 9.1–9.2 will assist in achieving compliance. Completion of these templates will ensure you have fully documented the requirements of this Standard.

Explanatory notes

Network perimeter controls are the hardware and software tools used to protect the practice system by analysing data entering and leaving your network. It includes technical measures such

Level 4 Managed	Level 5 Optimised
Complete written policy, periodically reviewed	Complete written policy, reviewed annually
Policy communicated in written format, training provided and all practice team members have access to the policy	Policy available in written format to relevant practice team members Regular training for the practice team and communication strategy reviewed against policy All practice team aware of the content and implications of the policy
Local LAN and personal firewalls issued Practice policy used for configuration	Conformance to practice policy Antivirus (anti-malware) software active on firewall Packet filtering, application proxy and stateful inspection (authorised connections)
Automated monitoring for user, system and policy violations	Automated monitoring and attack pattern recognition
All log files routinely examined	All log files routinely examined by trained practice team members (either inhouse or external)
Periodic automated check of all systems and networks	Automated configuration checking of each system and networks daily using port scanning tools
Automated monitoring for user, system and policy violations	Automated monitoring of abnormal attack patterns on the system and all user activities and policies
Log files automatically examined for router and server periodically	All log files for router, server, process and other security logs examined automatically each day
Installed for web services and email server	Configured to conform to practice policy including for web services email server and VOIP server Proxy server used
VPN installed	VPN installed

				Minimum
Computer network perimeter controls compliance indicators		**Level 1 Initial**	**Level 2 Repeatable**	**Level 3 Defined**
9.7 Content filtering		No content filtering in place	Software application filtering only for email	Software filtering via specific applications: email, antivirus
9.8 Perimeter vulnerability testing		No testing	Scanning performed ad hoc	Scanning performed regularly inhouse
9.9 External technical support		Not used	Technical support engaged ad hoc after critical incidents	External technical support engaged used for initial configuration and ad hoc as required
9.10 Wireless networks	**Wireless network encryption**	No encryption or unknown	WEP (wireless encryption protocol)	WPA2 (Wi-Fi protected access 2)
	Wireless network configuration	Default configuration or configuration unknown	Disable network broadcasting	Disable network broadcasting Change SSID (service set identifier/public name) to not identify practice or equipment brand

Adapted and reproduced with permission from Dr Patricia Williams

as firewalls and intrusion detection systems. It is recommended that qualified technical support be sourced for installation and configuration. This will help achieve a balance between protections and allowing authorised remote access to practice systems. In network perimeter security, it is necessary to use multiple techniques and tools to protect the information systems: this is known as layering or defence-in-depth. This involves multiple protection mechanisms, such as firewalls, intrusion detection systems, virtual private networks (VPNs), content filtering and antivirus protection.

Hackers can steal information and can cause harm to your computer system through loss or corruption of data. Network perimeter controls are essential for the long-term protection of patient information; even an inadvertent breach may infringe privacy laws and doctor–patient confidentiality.

9.1 Policy content

Network perimeter controls provide details of the systems (hardware and software) that protect the network and necessarily extend to include remote and wireless access networks. This may include firewall and intrusion detection hardware and software, content filtering and their related procedures. The network perimeter control policy and associated procedure will include access to network perimeter control hardware and software, its configuration and appropriate settings for the practice. This will need to be developed with assistance from your technical service provider or experts in this area.

Level 4 Managed	Level 5 Optimised
Files scanned by user prompt	Access to trusted websites only All files scanned automatically
Professional testing, including scanning, and network violation analysis	Annual professional testing
External technical support engaged for regular maintenance	External technical support engaged for regular maintenance and monitoring
WPA2-PSK (Wi-Fi protected access 2-pre-shared key) specifically using random letter or random word passphrase	WPA2-ENT (Wi-Fi protected access 2 enterprise) or higher used, specifically using random letter or random word passphrase
Disable network broadcasting Change SSID (service set identifier/public name) to not identify practice or equipment brand MAC address filtering used All wireless connections to network such as wireless printers and mobile devices also use password authentication to connect	Wireless network footprint mapped and adjusted to limit power MAC address filtering used Disable network broadcasting Change SSID (service set identifier/public name) to not identify practice or equipment brand All wireless connections to network such as wireless printers and mobile devices also use password authentication to connect Use of smart card, USB token or software token Use of wireless intrusion prevention systems (WIPS) or wireless intrusion detection systems (WIDS)

All hardware and software perimeter controls used and their configuration should be documented. Some of this information may already be recorded as part of the asset register in the risk assessment process.

An antivirus program also forms a component of network perimeter controls (discussed in *Standard 8*).

The practice policy on remote access and use of wireless systems should be documented. Technical assistance may be required with this. Aspects that should be considered include:

- allowable access channels (e.g. guest accounts, wireless, modem access)
- allow resources and system access when using remote access
- disallow downloading or installing additional programs and utilities
- establish third party and vendor access rights and confidentiality agreements (see Sections 3.4 and 3.5)
- use a VPN for all remote access
- avoid public or open, unsecured networks.

9.2 Policy communication

The policy should be in written format and communicated to relevant practice team members.

9.3 Firewall

Firewalls check messages coming *in* to and *out* of a network and block unauthorised access to a practice network. These can be either software or hardware. A firewall is configured to a set of rules to allow and disallow messages to flow in and out of the practice network. It adds a layer of protection between the practice computers and the internet. Unless you are using a standalone computer, it is advisable to install a hardware firewall for extra security rather than a software one. Firewalls need to be properly configured and periodically tested to ensure that they are still working. These are usually matters for a technical service provider.

Record the hardware and software configuration of firewall devices. These should be consistent with the network protection policies.

Hardware and/or software network perimeter controls need to be correctly installed and configured.

9.4 Intrusion detection systems (IDS)

Intrusion detection systems (IDS) monitor network and system activity to detect malicious and unauthorised actions and policy violations. They are usually software based and raise alerts if there has been unauthorised access to your systems. Intrusion detection systems do not prevent attacks on your system but they inform you that there is a potential problem so action can be taken. These systems are devices and programs that need technical knowledge to install and configure correctly. Record the hardware and software setup of IDS devices. These should be consistent with the network protection policies.

9.5 Demilitarised zone (DMZ)

A demilitarised zone (DMZ) acts as a neutral zone or protected space between the internal practice networks and the external facing connections, such as the internet, web services and email. It prevents access by outside users to the internal servers holding practice and patient data. It adds an additional layer of security to the local network for outside security attacks. For instance, if the practice website were hacked, while there may be corruption of the web pages, other practice information would not be placed at risk. Additionally, a proxy server is often placed in the DMZ where an intermediate server controls access to and from the internet.

9.6 Secure remote access

Secure remote access means communicating from your remote computer to the practice server securely. There are two commonly used methods to do this: virtual private networks and remote desktop protocol.

Virtual private networks (VPN) provide a secure and reliable connection over the internet – sometimes referred to as a ‘VPN tunnel’. A VPN uses encryption to prevent unauthorised reading of messages (confidentiality), authentication to ensure only authorised users have access to the system being connected to (authentication) and also uses authentication to ensure messages are not altered (integrity). It is most often used for remote access (access from outside the practice) to practice systems (e.g. accessing a practice system while visiting a nursing home). Establishing this service requires technical assistance.

Remote desktop protocol (RDP) is less secure than VPN. RDP is a Microsoft proprietary facility incorporated into the Microsoft operating system. It allows connection remotely from one computer to another over a network connection. One end of the connection runs the client software and the other the RDP server software. It uses a remote desktop service (the terminal server) and a remote desktop connection (the terminal service client).

The communication through RDP is encrypted at the transmission level, which protects it from the risks associated with interception of information; however, it lacks the authentication component to verify the identity of the server that is inherent in using a VPN. Note the encryption level is dependent on the version of the remote desktop connection client application as older versions do not support the higher levels of encryption.

You can increase the level of security by combining the use of RDP with secure socket layer (SSL) transport layer security (TLS) for authentication of the server and to encrypt the session connection information. This requires expert technical knowledge to set up correctly.

9.7 Content filtering

Content filtering is the use of software programs that can filter email and restrict access to the internet. Filtering for spam is the most common type of email filtering. Limiting access to known and trusted websites is commonly used.

9.8 Perimeter vulnerability testing

Testing the vulnerability of your network is called penetration testing. This uses methods such as scanning networks to discover security weaknesses, and network violation analysis, which examines logs for unauthorised access and unusual or inappropriate activity. If this is required it should be undertaken by a specialist in this field.

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. A form for recording the types and configuration of the network perimeter controls installed on your system can be found in *Templates 9.1* and *9.2*.

9.9 External technical support

Remote access is also used by technical 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, such as the use of a VPN (see Section 9.6). In addition, since third parties may have access to your system legitimately, a list of suggested guidelines to include in a contractual agreement, as well as a sample confidentiality agreement for such providers, is given in *Template 1.4*.

Technical IT service provider support should be used to install and configure appropriate network perimeter controls. Other, more complex controls may include technical solutions such as the use of hidden network addressing. Further, external technical support should be used for regular system and network maintenance and monitoring.

9.10 Wireless networks

Remote access to your practice computer system includes wireless networks and increases the convenience of access to practice information. However, it also requires additional security measures so that *eavesdroppers* cannot gain unauthorised entry to your computer system. There is increasing use of Wi-Fi (or Bluetooth) enabled laptops and other handheld devices (e.g. for home and aged care visits), and you should obtain technical advice on how best to keep the equipment and information they hold secure. Wi-Fi devices must have encryption set up to ensure the confidentiality of information. Care should be taken when using devices in public places to avoid information being sighted, as well as when connecting via open or unsecured public networks.

Wireless networks (remote access systems) must be configured securely by a technical service provider expert and should include:

- encrypting the data transfer using WPA2 (Wi-Fi protected access 2) or stronger encryption standards to avoid information exposure
- limiting the power of the router's 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 media access control (MAC) address filtering to restrict unauthorised devices from connecting to the wireless network. A MAC address is unique to a specific computer or device
- changing the service set identifier (SSID) or the public name of the wireless network to something unique that does not identify the brand of device used or the business name
- using password authentication for all wireless connections to the network, such as wireless printers and mobile devices
- considering using a smart card, USB token or software token authentication
- implementing a wireless intrusion prevention system (WIPS) or a wireless intrusion detection system (WIDS) for maximum protection. A WIPS and WIDS monitors for the presence of unauthorised wireless access points. A WIPS can take action to prevent intrusion using any detected unauthorised access points, while a WIDS notifies the computer system administrator.

Section 10

Standard 10: Mobile electronic devices

Our practice has processes in place to ensure the safe and proper use of mobile electronic devices in accordance with practice policies and procedures for managing information security

Compliance indicators

The compliance indicators listed in the matrix identify the specific actions that comprise good security practice for Standard 10.

It is assumed the practice will provide appropriate education and training to facilitate compliance with this Standard.

The compliance indicators at level 4 reflect the minimum level of computer and information security acceptable for this Standard. The compliance indicators for higher levels provide the basis for incremental security improvement.

Helpful templates for this Standard

Template 10.1 will assist in achieving compliance. Completion of this template will ensure you have fully documented the requirements of this Standard.

Explanatory notes

It is not enough to consider computer and information security only for the fixed hardware. Mobile devices are increasingly being used inside and outside practices for the provision of healthcare and the running of the business. Remote access via wireless (Wi-Fi) connections 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. All portable devices should be password protected, encrypted and stored securely where possible.

Mobile devices include any device used to contain information or enable access to sensitive information. Examples may include but are not limited to laptop computers, tablet devices, notebook PCs, USB flash drives, removable hard drives, mobile phones (particularly ‘smart phones’), personal digital assistants (PDA), and backup media such as drives, tapes and discs. Examples may also include portable electronic clinical equipment such as ABI (arterial brachial index monitor), spirometer, 24-hour BP and ECG monitoring devices. All of these devices present a higher risk of being lost, stolen or left unsecure, which increases the risk of data inadvertently ending up with unauthorised people. Computer and information security measures need to be broadened to include all mobile devices.

Mobile electronic devices compliance indicators	Level 1 Initial	Level 2 Repeatable	Level 3 Defined
10.1 Policy content	No formal policy	No complete written policy	Complete written policy
10.2 Policy communication	Policy not communicated to the practice team	Policy communicated verbally to the practice team	Policy communicated in written format to relevant practice team members
10.3 Data transfer only devices	Unsecured or security unknown	Password protected but not encrypted	Ad hoc encryption
10.4 Practice and personally owned mobile devices	Unsecured or security unknown	Password protected but not encrypted	Ad hoc encryption

Adapted and reproduced with permission from Dr Patricia Williams

10.1 Policy content

This policy details the permitted use of portable devices. It also provides guidance on the many considerations in installing and using wireless network access. Further, it should detail how and who can have remote access to practice systems (e.g. accessing practice information systems from home). This may include third party providers and access to practice systems via web-based portals.

The practice policy should include what devices are authorised to be used in the practice and how these devices are managed. The policy must direct the practice team on the use of privately owned mobile devices.

10.2 Policy communication

The policy should be in written format and communicated to relevant practice team members.

10.3 Data transfer only devices

This includes devices such as USB devices. The security around memory sticks and USBs is typically lax, due to the ease of use and small size of the devices. However, they can store a large amount of information and are often not used with security in mind. Therefore, their use should be strictly controlled within the healthcare setting. Even the ad hoc transfer of information poses security risks as USBs tend to be left around unsecured and usually are not used in conjunction with protection mechanisms such as encryption.

Minimum	
Level 4 Managed	**Level 5 Optimised**
Complete written policy, periodically reviewed	Complete written policy, reviewed annually
Policy communicated in written format, training provided and all practice team members have access to the policy	Policy available in written format to relevant practice team members Regular training for the practice team and communication strategy reviewed against policy All practice team aware of the content and implications of the policy
Where possible health data encrypted, password protected and stored securely	All USB and transfer data media encrypted Devices tracked and use monitored
Where possible health data encrypted, password protected and stored securely	All health data encrypted on device Devices password protected, tracked and monitored

10.4 Practice and personally owned devices

The devices may be owned by the practice or owned by members of the practice team.

- Security for all mobile devices can be increased using passwords and encryption.
- When not in use, these devices should be placed in secure locations.
- Additionally, it is important to review the security for practice team members' home computers where GPs and the practice team take electronic files home to work on them after hours and then return them to the clinic's network. 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 that are taken offsite on a daily basis.
- Seek technical advice on how the devices can be secured using mobile device management (MDM) or mobile application management (MAM) for personal devices used for clinical purposes.
- Bulk downloading or transfer of information using portable devices should be strictly controlled and audited. This also incorporates the 'store and forward' methods used in telehealth (refer to RACGP *Standards for general practices offering video consultations. An addendum* to the RACGP *Standards for general practices* (4th edition).

Section 11

Standard 11: Physical facilities and computer hardware, software and operating system

Our practice manages and maintains our physical facilities and computer hardware, software and operating system with a view to protecting information security

Compliance indicators

The compliance indicators listed in the matrix identify the specific actions that comprise good security practice for Standard 11.

Physical facilities, hardware, software and operating system compliance indicators	Level 1 Initial	Level 2 Repeatable	Level 3 Defined
11.1 Policy content	No formal policy	No complete written policy	Complete written policy
11.2 Policy communication	Policy not communicated to the practice team	Policy communicated verbally to the practice team	Policy communicated in written format to relevant practice team members
11.3 Physical protection	No access control to physical location of equipment	Access to practice team members only	Physical restriction to servers
11.4 Uninterruptible power supply (UPS)	Not used	Surge protector (power line conditioner) on server	UPS on server and monitor
11.5 Secure disposal	Unknown	Ad hoc and no formal process	Ad hoc but hard drives reformatted
11.6 Confidentiality	No screen savers	Clear desk policy followed	Clear desk policy followed Screen savers used
11.7 System maintenance	No maintenance undertaken	Maintenance activities undertaken invoked by incident	Ad hoc: temporary files deleted, hard disk capacity checked, status of anti-virus software checked
11.8 Software maintenance	No maintenance undertaken	Maintenance activities undertaken invoked by incident	Operating system patches applied to all computers manually Software upgrades applied when enforced by software provider

Adapted and reproduced with permission from Dr Patricia Williams

It is assumed the practice will provide appropriate education and training to facilitate compliance with this Standard.

The compliance indicators at level 4 reflect the minimum level of computer and information security acceptable for this Standard. The compliance indicators for higher levels provide the basis for incremental security improvement.

Helpful templates for this Standard

Templates 11.1–11.6 will assist in achieving compliance. Completion of these templates will ensure you have fully documented the requirements of this Standard.

Explanatory notes

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 proactive routine network

Minimum	
Level 4 Managed	**Level 5 Optimised**
Complete written policy, periodically reviewed	Complete written policy, reviewed annually
Policy communicated in written format, training provided and all practice team members have access to the policy	Policy available in written format to relevant practice team members Regular training for the practice team and communication strategy reviewed against policy All practice team aware of the content and implications of the policy
Physical restriction to servers Environmental conditions controlled	Physical restriction to servers Environmental conditions controlled Anti-theft cables fitted Removal of assets lists kept up to date
UPS on server and monitor Surge protectors on all computers and network equipment	Automatic server shutdown initiated by UPS UPS tested monthly UPS on server and monitor Surge protectors on all computers and network equipment
Secure disposal process established	Secure disposal process monitored
Clear desk policy followed Screen savers used with reactivation using password	Clear desk policy followed Screen savers used with reactivation using password System auto logoff activated
Periodic maintenance activities undertaken including temporary files deleted, hard disk capacity checked, status of anti-virus software checked	Scheduled regular maintenance undertaken including temporary files deleted, hard disk capacity checked, status of anti-virus software checked and disk defragmentation, checking of error logs, system maintenance log kept
Operating system patches applied to all computers automatically Software upgrades applied when convenient	Operating system patches applied to all computers automatically Software upgrades applied as soon as available Checking for installation of unauthorised programs Software maintenance log kept

maintenance; do not treat their role as limited to providing reactive emergency treatment when problems arise. There are certain maintenance procedures which, if performed regularly, will ensure that computers and other equipment run smoothly. The practice policy and procedures for these can be addressed as three separate areas:

- physical protection and maintenance
- system maintenance (e.g. the amount of free space on a hard disk)
- software maintenance (e.g. updates and patching).

In addition to protecting information you must also protect the computer systems physically. There are several components to this policy and associated procedures:

- label 'server' so that all practice team members are aware which computer is the server
- clean around the back of computers and other equipment so that dust does not accumulate near the fans and power supplies
- restrict physical access to the server
- secure all equipment from theft
- control the environmental conditions (e.g. extreme heat)
- limit damage from power interruptions and/or fluctuations
- ensure the secure disposal of hardware, in particular where it may contain clinical and/or business information.

11.1 Policy content

This policy will communicate to all practice team members the practice policy on the use of screensavers and other precautions such as the positioning of monitors to prevent unauthorised viewing of patient medical records and other confidential information. This policy will also detail restrictions of physical access, for instance to the server, 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. Document details of routine computer maintenance that is required. This includes hard disc 'clean-ups' (e.g. by a defragmentation utility program). It also addresses software maintenance procedures.

The policy should also include how to minimise and prevent unauthorised and accidental viewing of patient and practice information. This policy can include:

- the physical positioning of monitors in open access areas, consulting rooms and reception
- appropriate use of screensavers
- clear screen policy
- clear desk policy
- the requirement to remove documents from printers and faxes immediately.

The practice policy and procedures should document the disposal of old, decommissioned and replaced hardware, particularly devices with any data on them. This could include:

- securely deleting all data on a device or media. Reformatting the media is not sufficient as forensic techniques can still access data on the device and media
- disposing of equipment through appropriate destruction.

11.2 Policy communication

The policy should be in written format and communicated to relevant practice team members.

11.3 Physical protection

Location

Physical security is the first level of defence. It provides protection from theft and unauthorised access. The physical location of the server is important, for instance locking it in a safe place or using antitheft steel cables. Password access to the server should be limited to key members of the practice team. Desktop and laptop computers and other portable devices should always be kept physically secured. Locking away software, disks and backup media limits physical access.

The practice computers and network are valuable and therefore limiting unauthorised personnel access to this equipment is recommended. The practice policy will document which personnel have authorisation to access such equipment.

Heat, dust and humidity

Environmental protection includes positioning computers, backup media and other components of the network where they are not subjected to excessive heat (e.g. away from direct sunlight). All computers should be kept reasonably dust free, particularly over intakes for the cooling fans. To minimise the possibility of equipment failure, the server room temperature should be regularly monitored with consideration given to installing dedicated air conditioning if required.

Some buildings switch air-conditioning off at night to save power; however, if the server is still running it might overheat.

Securing equipment from theft

All removable computer equipment should be secured from theft or damage.

This is particularly important where equipment is in areas that are frequented by patients and visitors to the practice. This policy should include items such as:

- use cable device locks for notebook and desktop computers and monitors and other mobile devices when in use in the practice
- lock laptops and similar equipment away at night if left on the premises
- do not leave USBs and software media in an unsecured environment.

11.4 Uninterruptible power supply (UPS)

Power outages and fluctuations can happen at any time. 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 is lost. This is important so data being processed is not lost or corrupted while the blackout occurs.

A UPS also helps with power surges that can cause hardware damage. The batteries in most units only provide power for an average of 10–30 minutes. In a prolonged blackout, the UPS should automatically shut the server down in an orderly manner to prevent data corruption or loss – it is not designed to run practice systems. This requires installation of the dedicated UPS monitoring software and a connection from the UPS to the server (ethernet or USB).

The management of prolonged blackouts requires the installation of a generator; however, this purchase will require careful consideration.

A UPS should be installed on the main server and other essential devices, such as routers, switches and IP phones. Simple surge protectors may 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.

The controlled shutdown procedure should be documented. Refer to the *Templates*, Standard 11 to record this procedure and details of the power protections installed in the practice. To ensure that the batteries in the UPS are checked appropriately, apply a sticker to acknowledge battery life, and when to replace them, or preferably record this in the templates register.

11.5 Secure disposal

Appropriate and secure disposal of old or decommissioned computer equipment, and importantly any data storage media especially hard disks, is vital. Password protection and/or encryption are not sufficient when disposing of old equipment. Disks and backup media should be securely erased (overwritten), disposed of using a secure document collection company or physically destroyed. There are many commercially available products capable of secure erasure. Seek advice from your technical service provider.

Recording removal of assets from the practice premises

To reduce the potential loss or theft of equipment and assets, all removal from the practice premises should be formally recorded to minimise loss and theft. This will include recording the date out, date in and location when offsite. *Template 11.3* provides a form for this.

11.6 Confidentiality

Clear screen – computer screen confidentiality

This Standard is not specifically about privacy principles, although keeping information on the computer screen confidential is an instance in which a 'privacy' matter overlaps with information security. Information security in the consulting room is more about clinical practice team member behaviour than technical matters. For example, some healthcare professionals like their computer screens to be clearly visible to their patients during consultations. However, it is important to be vigilant about inappropriately exposing information to a third party, for example it might not be acceptable for a parent to see the past history of their adolescent child. More importantly, patients should not be able to view the clinical record of another person (e.g. 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.

There are various methods by which the information can be kept private. For example, remember 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. Other options worth considering are:

- the use of 'clear screen' function keys, which instantly close down an open file or switch off the monitor
- the use of password protected screensavers. These can be set so that you have to use your password to log back into your system (suggested default of 15 minutes)
- log off when leaving terminals or use automatic session time-outs.

Whichever method you consider most appropriate to your circumstances, the important thing is that all practice team members are aware of how they can keep sensitive information from being inadvertently viewed.

Clear desk policy

To avoid accidental and unauthorised viewing of documents, it is recommended to use a clear desk policy. This means at the end of each day each practice team member clears their desks of all documents, notes and media. In addition, all documents should be removed from printers and fax machines immediately after being copied, sent or received.

11.7 System maintenance

While some preventive system maintenance can be carried out by authorised and trained practice team members, most is usually undertaken by a technical service provider. This will include checking disk capacity (hard disk space), defragmenting the hard disk when necessary, deleting and tidying up system and temporary files, checking error logs, checking that antivirus and other protective software is up to date, checking battery life on the UPS and documenting all maintenance performed and completed on the system. An example of a system maintenance log can be found in *Template 11.4.* Simple system maintenance can be carried out by authorised and trained practice team members, such as ensuring that areas near and around computer equipment are clean and dust free.

11.8 Software maintenance

Software maintenance means the 'maintenance' work on the computer system software on an ongoing and regular basis. This can also include monitoring for signs of potential incidents using file integrity checking programs or using an external monitoring service.

- Patching is vitally important to keep the software up to date, especially your operating system software (e.g. Windows). Patches are program updates essential to rectifying security 'holes' in earlier versions.
- Restrict user access to avoid full administrative access. This will limit vulnerabilities to malware as this limits the ability of users to install additional applications and programs. This also protects against modification of software configuration settings (such as security settings in web browsers).
- Limit access to system utilities to full administrative access only. Seek advice from a technical service provider in this matter.
- Check for installation of unauthorised programs.
- Software configuration: install and maintain software in accordance with the vendor's guidelines to ensure security is maintained. This may also include ensuring that auditing is turned on to log operating system and application activity as this information can be very useful when an incident occurs.
- Run file integrity software periodically. This software is sometimes provided by your software vendor to check the integrity of the database and files.
- Consider the use of an external network and system monitoring service.
- Keep a software maintenance log.

Unless you have sufficient technical knowledge and skills among the practice team, seek technical advice on how to keep your computer software functioning efficiently.

Section 12

Standard 12: Security for information sharing

Our practice has reliable systems for the secure electronic sharing of confidential information

Compliance indicators

The compliance indicators listed in the matrix identify the specific actions that comprise good security practice for Standard 12.

It is assumed the practice will provide appropriate education and training to facilitate compliance with this Standard.

The compliance indicators at level 4 reflect the minimum level of computer and information security acceptable for this Standard. The compliance indicators for higher levels provide the basis for incremental security improvement.

Helpful templates for this Standard

Template 12.1 will assist in achieving compliance. Completion of this template will ensure you have fully documented the requirements of this Standard.

Explanatory notes

Securing electronic information is essential and requires higher security standards because:

- it can prevent information being intercepted or changed during transmission
- it can prevent information being received by unintended recipients
- it is easier to disseminate electronic information and therefore lose control of the information
- there are better security measures available to protect electronic health information than other methods of communication
- it may be difficult to detect accidental or malicious changes to a record.

Security for information sharing compliance indicators	Level 1 Initial	Level 2 Repeatable	Level 3 Defined
12.1 Policy content	No formal policy	No complete written policy	Complete written policy
12.2 Policy communication	Policy not communicated to the practice team	Policy communicated verbally to the practice team	Policy communicated in written format to relevant practice team members
12.3 Secure messaging	Status of certificates unknown	Certificates expiry recorded	Medicare and NASH certificates stored securely and the expiry of each recorded
12.4 Healthcare identifiers	No training provided	Induction training only provided to practice staff members	Training on the use of healthcare identifiers undertaken ad hoc
12.5 Practice website safety and security	Website installed but not updated.	Website shares server with other practice data	Website on a separate server to other practice data

Adapted and reproduced with permission from Dr Patricia Williams

12.1 Policy content

Establish written policy and procedures for secure communication. All patient-related information sent electronically between healthcare providers should be sent by secure message delivery (unless there is an overwhelming reason not to, such as putting a patient or healthcare professional at risk). The policy will include the practice policy for electronic communication of patient records and other confidential information with healthcare professionals and patients. This may involve encryption and associated procedures. The policy should also include the processes required when a healthcare professional terminates their contract or employment with a practice.

12.2 Policy communication

The policy should be in written format and communicated to relevant practice team members.

12.3 Secure messaging

There are broadly two types of electronic information transfer that are relevant to general practice: secure message delivery and communication via standard or unencrypted email.

Secure message delivery

Secure message delivery (SMD) involves two processes: encryption and authentication. Encryption means that data is electronically ‘scrambled’ so that it cannot be read unless the information is decrypted. Authentication means that the sender can be verified; this is done using electronic signatures. E-health information exchange in the Australian health system relies on and incorporates encrypted, secure messaging techniques. The software programs used will handle this function and are required to meet Australian standards.

Minimum	
Level 4 Managed	**Level 5 Optimised**
Complete written policy, periodically reviewed	Complete written policy, reviewed annually
Policy communicated in written format, training provided and all practice team members have access to the policy	Policy available in written format to relevant practice team members Regular training for the practice team and communication strategy reviewed against policy All practice team aware of the content and implications of the policy
All certificates stored securely and the expiry of each recorded	All certificates (Medicare, NASH and commercial) stored securely and the expiry of each recorded Record kept of which certificate is installed on which computer and device
Training on the use of health identifiers undertaken as required when first used or when changes occur in the service	Regularly updated training for practice team members on the use of healthcare identifiers
Website hosted externally or on a separate server to practice data, not accessible directly through the practice network	Website hosted externally or on a separate server to practice data and using a DMZ

To use SMD both the sending and receiving parties must use compatible encryption processes. SMD is technically complex and does not need to be understood by practices as SMD vendors must conform to Australian standards.

SMD can be either P2P (point-to-point), where information is sent from a specific sender to a specific recipient or recipients, or P2shared (point-to-shared), where information is sent from a specific sender to a shared record such as with the national eHealth record system.

The storage of the digital certificates and recording of expiry dates needs consideration. Store certificates securely – this means the original disk and serial numbers. Further, keep documentation on which computers the certificates are installed.

Communication via standard or unencrypted email – email can be intercepted, retrieved and read by unintended receivers without authorisation

Emails can legally be read by an internet service as messages pass through the provider system. This is in contrast to messages directly transmitted such as telephone calls and faxes, which are subject to interception legislation.

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 the 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, emails between practices and patients need to be cautious and limited in scope, for both security and clinical safety reasons.

Providers/practices should not send confidential data via email or the internet. A suggested email and internet policy, which includes security and safety considerations, can be found in Section 6. In addition, a template for recording secure electronic communication systems and purposes is included in *Template 12.1*.

12.4 Healthcare identifiers

Healthcare identifiers underpin secure transmission of data and patient and healthcare provider identification. Healthcare identifiers are unique 16 digit numbers that comply with international identification standards. They are non-sequential, randomly allocated and not searchable. The identifiers are administered through the national Healthcare Identifiers Service (HI Service). The use of healthcare identifiers ensures better identification of individuals and healthcare providers and means individuals and healthcare providers have increased confidence that the right health information is associated with the right individual at the right place and time. The use of and access to healthcare identifiers are governed by the *Healthcare Identifiers Act 2010* (Cwlth).

Four types of healthcare identifiers are assigned by the HI Service:

1. individual healthcare identifier (IHI): every Australian has an IHI whether are receiving healthcare or not. An IHI is to electronically link healthcare information about the individual.
2. healthcare provider identifier – individual (HPI–I): for healthcare providers registered under the Australian Health Practitioner Regulation Agency
3. healthcare provider identifier – organisation (HPI–O): healthcare provider organisations (e.g. a hospital or general practice)
4. contracted service provider.

Healthcare providers who are identified with an HPI–I or HPI–O or an authorised employee can access the HI Service to obtain the IHI of a patient receiving healthcare. This means practice team members will require education and training on the implications and use of healthcare identifiers.

The *Healthcare Identifiers Act* (Division 5, 27 Protection of healthcare identifiers) stipulates that reasonable steps must be taken to protect the identifiers from misuse, loss and unauthorised access, modification or disclosure. Further, the healthcare identifier for an individual is taken to be personal information and therefore is also subject to the *Australian Privacy Act 1988* Para 28(1) (h).

Digital certificates

To participate in the Australian national eHealth record system, healthcare organisations and healthcare providers need to obtain nationally trusted digital credentials (public key infrastructure [PKI] certificates). These certificates authenticate, encrypt and seal the message and can also be used to connect to national repositories.

Healthcare organisations will need to install two PKI certificates: a Medicare claims and payments certificate (location or site certificate) for HI Service access and a National Authentications Services for Health (NASH) PKI certificate to access the national eHealth record system and for secure message delivery.

Healthcare providers and other authorised staff may also require digital certificates issued on tokens (smart cards or USB) for individual access to national repositories.

In addition, a range of commercial certificates are used for a variety of purposes, such as laboratory results.

Message system record

If more than one electronic communication method is used (for communication with different health organisations), each one should be documented separately. Template 12.1 provides a form for recording the messaging systems used in the practice.

12.5 Practice website safety and security

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. The practice must abide by the Guidelines for Advertising of Regulated Health Services set by the Medical Board of Australia (www.medicalboard.gov.au/Codes-Guidelines-Policies.aspx).

There are additional security risks if the practice website is hosted on the same computer that holds the practice data. It is strongly advised not to have patient data on the same computer as your web server. If there is a security breach through the practice website there is a potential risk that the practice data will be vulnerable. In addition, if your practice allows appointments to be made through the website, then no patient names should be stored in the web server database. Your technical service provider will be able to advise on the best methods to secure your website as this may require the use of a demilitarised zone (DMZ), which separates the website and services that patients may access from the main practice systems.

The general practice website is a communication method that requires maintenance to ensure that the information held within the site is current and correct. The documentation includes identifying the timeframe for regular review of the website. If using the website for information transactions of any sort, for example online appointment bookings, these transactions should be encrypted. The practice will need to identify which practice team member is responsible for the practice website and document this in the practice team member's position description.

Email and internet policies including practice websites help to ensure that confidential information is kept secure and private.

Glossary of computer and information security terms

The following is a glossary of key technical terms used in this document relevant to computer and information security.

Adware: Free software that is supported by advertisements.

Anti-malware: A general term for antivirus, antispyware and intrusion detection systems; it covers any type of software that detects and blocks unwanted data and programs.

Antivirus program: Software that searches for known computer viruses.

Availability: Ensuring that authorised users have access to information when required.

Backup: A copy of the files (system, software and data) in case the original is lost or corrupted.

Blacklisting: An access control mechanism used to deny access to certain websites and URLs.

Cache: Stores recently used information for quicker access. The term is most commonly associated with the retrieval of web pages. A disk cache is an area of the computer's memory that stores the most recently read information from the hard disk.

Client: A computer that requests services from a computer called a server (e.g. 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.

Clinical information system: A computer-based system designed for the collection, storage, retrieval and manipulation of clinical and patient information to assist in healthcare delivery processes.

Computer and information security standards (CISS): A document that provides guidance on the essential information needed to put in place effective computer and information security.

Confidentiality: Ensuring that information is only accessible to those who have authorised access.

Contracted service provider (CSP): A third-party organisation that can act on behalf of a healthcare provider organisation to deliver health software as a service and facilitate access to the National eHealth record system on behalf of the healthcare provider organisation.

Cookies: Data sent to a computer by a web server that records browsing behaviour of the user. Cookies are small text files stored on your computer that keep your login and other information, so that a web application or server can keep track of your activity. Cookies are not a security risk in that they are not malicious code or programs and cannot access the data on the computer. However, they can compromise the user's privacy.

Demilitarised zone (DMZ): A separation of an internal trusted network from a connection to untrusted external networks such as the internet. It provides an extra layer of security (using firewalls) where public or external access to services such as a website is required. It is also referred to as a perimeter network.

Denial of service (DoS): A computer network attack that prevents or impairs the authorised use of networks, systems or applications by exhausting resources.

Digital certificate: A mechanism used to establish identity and authenticity of the message sender and/or receiver. It may also be used to encrypt the message.

Domain key identified mail: A security method for associating a domain name (organisational identification) to an email allowing a person or organisation to assert responsibility for the message. The association is set up by means of a digital signature that can be validated by the email recipient.

Encryption: The process of converting plain text characters into cipher text (i.e. meaningless data) as a means of protecting the contents of the data.

File integrity software: Software that generates, stores and compares message integrity checks for files to detect changes to the files.

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

Hard drive (hard disk drive): A hardware device used for storing programs and data on a computer.

Hardware: Physical components of a computer, such as a monitor, hard drive or central processing unit (CPU).

Healthcare provider identifier – individual (HPI–I): A unique identification number for healthcare professionals and other health personnel involved in providing patient care.

Healthcare provider identifier – organisation (HPI–O): A unique identification number for organisations (e.g. a hospital or general practice) where healthcare is provided.

Inappropriate usage: When a person violates acceptable use of any network or computer policies.

Incident: A violation or imminent threat of violation of computer and information security policies, acceptable use of policies or standard security practices.

Individual healthcare identifier (IHI): A unique identification number for individuals who seek healthcare.

Information security: The protection of confidentiality, integrity and availability of information.

Integrity: Maintaining and safeguarding the accuracy and completeness of information and data.

Internet service provider (ISP): A company that provides access to the internet.

Local area network (LAN): A group of connected (networked) computers in the same location such as an office building or company.

Log file: Contains records of events that have occurred, automatically generated by the software or hardware.

Malware: Short for malicious software or code: the term used to describe software programs that are designed to damage data or perform unwanted actions. It is used as the collective term for viruses, worms, trojans and spyware.

Man-in-the-middle: A form of attack where an attacker intercepts the message exchange and makes independent connections with the correspondents, then relays messages between them. The correspondents believe they are communicating directly when in fact they are being sent messages via the attacker.

Mirrored hard disk: 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 be used.

Modem: Acronym for modulator – demodulator: 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 (e.g. at home or travelling), or to connect computers to the internet via a dial-up or broadband connection to an internet service provider.

National Authentication Service for Health (**NASH):** Australia's nationwide secure and authenticated service for healthcare delivery organisations and personnel to exchange sensitive eHealth information.

Network: A collection of connected computers and peripheral devices used for information sharing and electronic communication.

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.

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.

Non-repudiation: Means that you cannot deny having performed a transaction (e.g. 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 communicates with the computer hardware at a basic level, allowing application software to function. For example, Macintosh, Windows and Linux are types of operating systems.

Organisation Maintenance Officer (OMO): The OMO is registered with the Healthcare Identifiers Service (HI Service) and acts on behalf of the organisation in its dealings with the national e-health record System Operator. The OMO's primary role is to undertake the day-to-day administrative tasks in relation to the HI Service and the eHealth record system. A healthcare organisation can have multiple OMOs. An OMO needs to be someone who is familiar with the IT system used by their organisation.

Patching: A piece of software applied to fix or update software programs or the operating system.

Peripheral device: A device attached to a network or a computer that provides input and output such as a keyboard or a printer.

Phishing: Fake emails and websites attempting to acquire usernames, passwords and credit card details without authorisation or permission.

Proxy/proxy server: A server that all requests from computers on a local network have to pass through to access the internet. It can improve internet access speeds as it uses caching to save recently viewed web pages, images and files. It also acts as a filter for what is allowed into the local network.

Ransomware: Also known as crypto-viruses, crypto-trojans, crypto-worms: refers to a type of malware that prevents access to the computer system or the data, and demands a 'ransom' is paid. Ransomware works in one of two ways: by encrypting files with a password, which prevents access to them, or a 'lock screen' message, which displays an image or webpage that prevents access to anything else on the computer.

Reboot: When you restart your computer. You might be required to reboot your computer in some instances (e.g. after installing new software) to enable the changes to take effect.

Redundant array of independent disks (RAID): A method for storing data on multiple hard disks in a computer. This can improve performance and fault tolerance.

Registry: A database used by Microsoft Windows to store system configuration information about the software installed on a computer. It should never be tampered with unnecessarily as this can lead to your computer not functioning properly.

Remote access: The ability to gain access to a network or system that is not in the same physical location.

Remote desktop protocol (RDP): A Microsoft program to connect remotely from one computer to another over a network connection.

Responsible Officer (RO): An RO is registered with the Healthcare Identifiers Service (HI Service) and has authority to act on behalf of the seed organisation in its dealings with the eHealth record 'System Operator' and the HI Service Operator. The RO has primary responsibility for their organisation's compliance with participation requirements in the eHealth record system. For large organisations the RO is usually the CEO; however, for smaller business organisations the RO could be the practice manager or business owner.

Rootkit: A group of programs and files designed to gain unauthorised access to a computer using full administrative privileges.

Router: A device that provides connectivity between networks (e.g. between your internal network and the internet). A router forwards data from one network to the other and vice-versa. Many routers also have built-in firewall capabilities.

Secure socket layer (SSL): SSL is a protocol to securely transfer files and messages over the internet using encryption.

Sender policy framework: An email validation system designed to detect and block spoofed (forged) emails by verifying the sender's email server before delivering email to a recipient's inbox.

Server: 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.

Social engineering: An attempt to trick someone into revealing information (e.g. a password) that can be used to attack systems or networks.

Software: A program (or group of programs) that performs specific functions, such as word processor or spreadsheet programs.

Spam: Unsolicited or junk email. Often it is simply nuisance email, but it can entice you to provide confidential personal information (e.g. banking passwords).

Spoofing: Spoofing is where a person or program pretends to be another by faking information or data. Email spoofing is where an email appears to have originated from one source when it actually was sent from a fake email address.

Spyware: Programs that are downloaded from the internet onto your computer (sometimes without your knowledge) to covertly send back information (e.g. your personal details) to the source.

Standalone computer: A computer that is not connected to a network or to other computers.

Threat: A potential event that could cause harm to information or an information system.

Transport layer security (TLS): A protocol for providing security over the internet using encryption. It can be enabled on email servers to allow secure transmission of messages, and it is transparent to the email user.

Trojan: Malware disguised as a real program.

Unauthorised access: Attempting to gain access or gaining access without permission to a network, system, application or data.

Uniform resource locator (URL): The address for an internet website, page or file, such as http://www.racgp.org.au.

Uninterruptible power supply (UPS): Battery backup to maintain power for a specified time period during power outages.

USB flash drive: A memory data storage device integrated with a USB (universal serial bus) interface.

Virtual private network (VPN): Creates a secure connection (using encryption) between specific locations or networks across the internet or a wide area network.

Virus: A malicious software program that can create copies of itself on the same computer and on others, and attach these copies to files and emails to spread itself.

Vulnerability: Weakness in an information system that could be exploited by a threat or action.

Whitelisting: An access control mechanism to allow access only to websites and URLs listed.

Wide area network (WAN): A network that is not restricted to a local area. Using telephone lines, fibre-optic cable and satellite links, it can span long distances.

Wi-Fi: Wireless networking standard that enables transmission of data over wireless networks.

Wi-Fi protected access (WPA): A security protection method using encryption to create secure wireless (Wi-Fi) networks.

Wi-Fi protected access 2 (WPA2): A more advanced and security protection method than WPA using encryption to create secure wireless (Wi-Fi) networks.

Worm: A self-replicating computer program (similar to a computer virus) that uses the network to send copies to other computers.

Zero day exploits: A malicious computer attack that takes advantage of security vulnerability before it is known or patched.

Appendix A – List of related standards, principles and legislation

These Standards have been developed in accordance with recognised best practice and are aligned with the requirements of international and Australian standards, current Australian legislation and legislative instruments, the National Privacy Principles and national standards in health information security as listed below.

- *AZ/NZS ISO 31000:2009 Risk management – principles and guidelines.* Sydney: Standards Australia International, 2009.
- *HB 292 – 2006 A practitioners guide to business continuity management*. Sydney: Standards Australia International, 2006.
- *HB 174 – 2003 Information security management – implementation guide for the health sector*. Sydney: Standards Australia International, 2003.
- *HB 231 – 2004 Information security risk management guidelines*. Sydney: Standards Australia International, 2004.
- *HB 292 – 2006 A practitioners guide to business continuity management*. Sydney: Standards Australia International, 2006.
- *HB 293 – 2006 Executive guide to business continuity management*. Sydney: Standards Australia International, 2006.
- Information Privacy Principles under the *Privacy Act 1988* (www.privacy.gov.au/materials/types/infosheets/view/6541).
- *ISO/IEC 27002:2006 Information technology – security techniques – Code of practice for information security management.*
- *ISO 27799:2008 Health informatics – information security management in health using ISO/IEC 27002*.
- *Healthcare Identifiers Act 2010* (Cwlth) (incorporating amendments). www.comlaw.gov.au/Details/C2012C00590
- *Personally Controlled Electronic Health Records Act 2012* (Cwlth). www.comlaw.gov.au/Details/C2012A00063
- *Computer security incident handling guide*. Special publication 800-61. National Institute of Standards and Technology, 2008. http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
- *National Privacy Principles*. Office of the Australian Information Commissioner, 2006. www.privacy.gov.au/materials/types/infosheets/view/6583
- *Data breach notification – a guide to handling personal information security breaches.* Office of the Australian Information Commissioner, April 2012. www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html.
- *Guide to information security: 'reasonable' steps to protect personal information*. Consultation draft. Office of the Australian Information Commissioner, 2012.
- *National Ehealth Security and Access Framework v3.1*. NEHTA, 2012.

National Privacy Principles

Principle 4 – Data security

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.

Australian Information Privacy Principles

Principle 4 – Storage and security of personal information

A record-keeper who has possession or control of a record that contains personal information shall ensure:

(a) that the record is protected by, such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse; and

(b) that if it is necessary for the record to be given to a person in connection with the provision of a service to the record-keeper, everything reasonably within the power of the record-keeper is done to prevent unauthorised use or disclosure of information contained in the record.

Appendix B – National eHealth system security requirements

Conforming to the Standards demonstrates sound information security governance and compliance with the following security requirements.

- Allocation of a person to the role of Responsible Officer (as defined by the *Healthcare Identifiers Act*) and an Organisation Maintenance Officer (as defined by the *Healthcare Identifiers Act*) to be the contact person for the Healthcare Identifiers Service and the PCEHR System Operator.
- Participation Agreement: Notification of known and suspected data breaches that may affect the PCEHR to the System Operator. This is covered in the data breach response and notification section.
- *Healthcare Identifiers Act*: Protection of healthcare identifiers (Division 5, 27). Reasonable steps to protect healthcare identifiers against misuse and loss, and from unauthorised access, modification or disclosure.
- *Personally Controlled Electronic Health Records Act* and Rules (Division 2 Security Requirements):
  - provision of a practice policy specifying the access control in relation to the PCEHR; how staff accessing the PCEHR will be trained and educated in security awareness; process for identification of access requesters; the security measures in place (or to be put in place)
  - dissemination and enforcement of the PCEHR practice policy
  - the policy must be version controlled, up to date and auditable with at least annual reviews
  - regular (annual) risk assessment in relation to the policy is undertaken
  - practices must have a policy or other documentation that details the computer and information security measures in place
  - practices must have a policy or other documented procedure for data breach and security incident management
  - a copy of the relevant policies must be available when requested (within 7 days) by the System Operator
  - effective and appropriate user account management.

Note: to meet PCEHR Rule 28, Retention of record codes and document codes (as below), practices should ensure that the practice team are aware that they should not be recording record and document codes, such as a patient's individual health identifier, from the PCEHR in any format (paper or electronic).

Healthcare provider organisations must ensure that people using their information technology systems to access the PCEHR system via or on behalf of the organisation do not record, store or retain a copy of a consumer's record code or document code for the purposes of accessing the consumer's PCEHR, or a record in the consumer's PCEHR, in the future.

Appendix C – Data incident/breach report

Practice name

Data incident / breach report

Report date/time

Author

Description of the incident/breach

When the breach occurred (date and time)

What happened?

What information specifically was or may have been compromised?

Type of personal information involved

What caused the breach?

What steps were already in place to prevent the breach?

Was the breach accidental or deliberate?

Were any other people or organisations involved?

Steps taken

Who contacted

Corrective action taken

Prevention of recurrence action taken

Outcome

PCEHR System Operator notified (if applicable)

Date/time

Office of the Australian Information Commissioner notified (if applicable)

Date/time

Police notified (if applicable)

Date/time

Report no.

Future actions required (e.g. ensure malware protection up to date)

Consideration should be given to how the breach may impact the individual and what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves. This may include information to assist the individual to protect themselves against identity theft or further interferences with their privacy.

RACGP

Healthy Profession.
Healthy Australia.