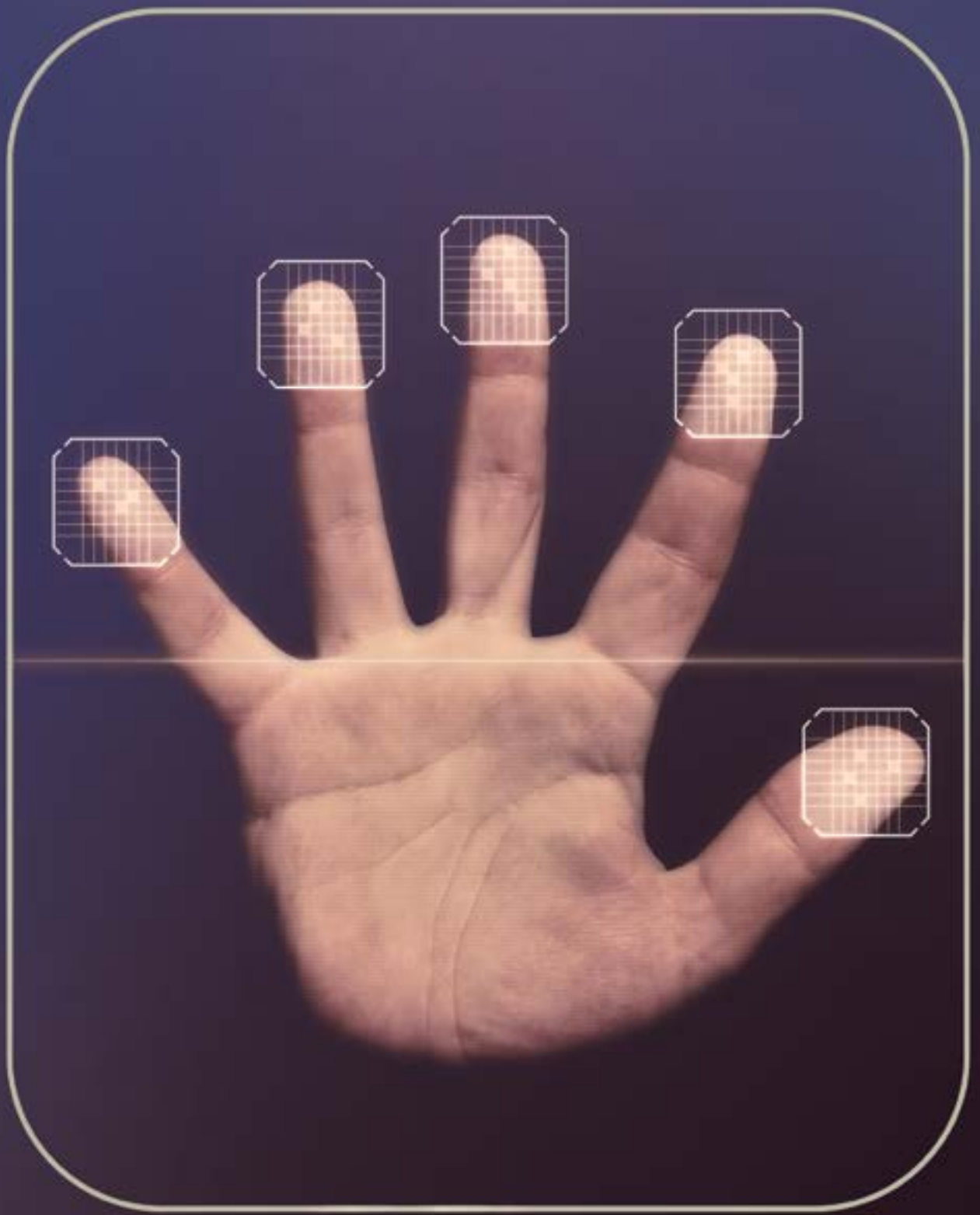
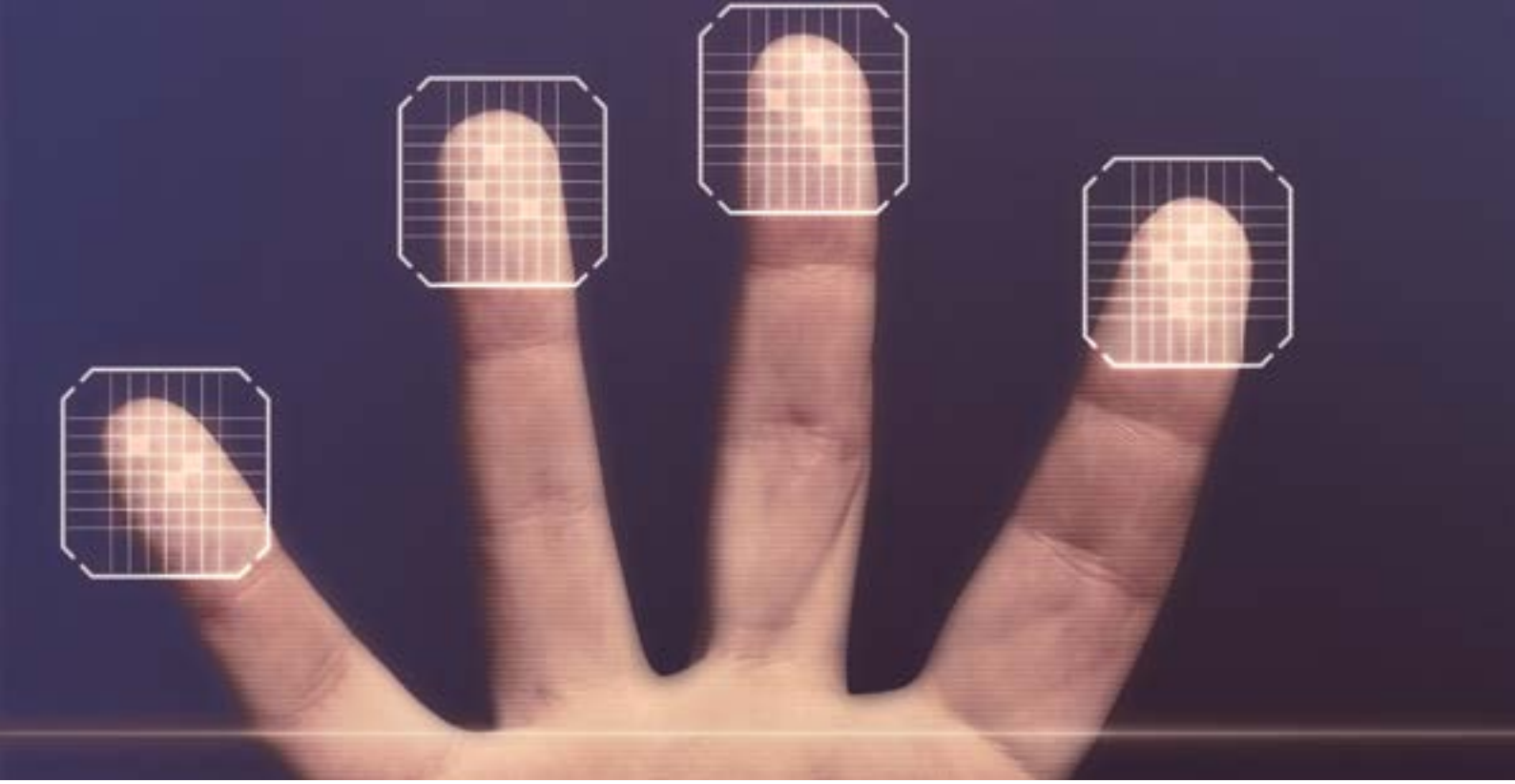
RACGP

Computer and information security templates

To support the RACGP *Computer and information security standards*





RACGP

Computer and information security templates

To support the RACGP *Computer and information security standards*

Disclaimer

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: 978-0-86906-350-7
Published June 2013

Practice name

Date completed	Version number	Next review date

	Document owner(s)	Project/organisation role
1.		
2.		
3.		
4.		
5.		

Document version control

	Version	Date completed	Author	Change description
1.				
2.				
3.				
4.				
5.				

Acknowledgements

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

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

- 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

How to use this document

The *Templates* are to assist both general practice and office-based clinical practices to record the essential information needed to put in place effective computer and information security. It should be completed by the designated practice Computer Security Coordinator with assistance from other practice team members and where appropriate an external IT/security technical support consultant. The computer and information security templates, when completed, will form part of the general practice's policies and procedures manual. Refer to the RACGP *Computer and information security standards* (CISS) for explanations of each section to be completed in the templates.

This document is designed to be completed electronically.

- Save this document on your hard drive. Make a copy of the document and rename it to include the name of your practice.
- There may be some elements that are not relevant to your particular general practice. These items should be marked 'not applicable'.
- Examples have been provided to help clarify what information is needed to complete certain sections of the document.
- Completing this workbook may require specific technical information that is only available from an external technical service provider.
- On page iii of this document record the date of completion, the current version of the document and note the review date so as to ensure that a review of the CISS is scheduled. Also fill in the document person responsible for creating/editing the document and version control history table.
- Remember to update the documentation when there are changes that affect the content of your policies in relation to staff responsibilities or the computer setup at the practice. Change the date on the manual to reflect the revision and update the time for review.
- Keep multiple copies of the completed document and a printed copy that can be located easily in the event of an incident or disaster, or on mobile storage devices (e.g. USB) or other mobile devices.

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 also includes 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.		

Standard 1: Roles and responsibilities

For explanatory notes refer to Section 1 of the RACGP *Computer and information security standards*.

Template 1.1: Security coordinator

Person or persons responsible

	Name(s)
1.	
2.	
3.	
4.	
5.	

Template 1.2: Coordinator role review and training dates

	Coordinator role review dates	Coordinator training provided dates
1.		
2.		
3.		
4.		
5.		

Staff roles and responsibilities

Template 1.3: Staff roles and responsibilities

	Task	Person or persons responsible
1.		
2.		
3.		
4.		
5.		

Template 1.4: Sample confidentiality agreement

I (name) _____ understand that as a condition of employment

by (name and address of practice) _____

I shall, neither during nor after the period of employment/engagement with the practice, except in the proper course of my duties or as permitted by the practice or as required by law, divulge to any person any confidential information concerning:

- patient personal, health and financial information
- the business or financial arrangements or position of this practice or any related company
- any of the dealings, transactions or affairs of the practice or any related company.

The contractual arrangement between this practice and its employees/contractors is founded on trust. I undertake not to knowingly access any confidential information about the business of the practice, patients or patient medical information, unless such information is essential for me to properly and efficiently perform my duties. I am aware that these conditions extend to unnecessary discussion of confidential information within the practice. I understand that any breach of this trust will render me liable to disciplinary action, termination and/or civil proceedings.

I further undertake to inform my supervisor immediately if I become aware of any breach of privacy or security relating to the information I access in the course of my duties.

This restriction ceases to apply to any information or knowledge, which subsequently comes into the public domain by way of authorised disclosure.

All confidential records, documents and other papers together with any copies or extracts thereof in my possession will be returned to the practice on the termination of my employment.

Signature	Signature of witness
Name (print)	Name (print)
Date	Position

Standard 2: Risk assessment

For explanatory notes refer to Section 2 of the RACGP *Computer and information security standards*.

Template 2.1: Security coordinator(s) and associated roles

Security coordinator name(s)

1.
2.
3.
4.
5.

Responsible Officer name

Organisation Maintenance Officer name

Template 2.2: Staff and technical support contact details

	Name and company	Support provided for	Contact details
1.			
2.			
3.			
4.			
5.			

Asset register

Physical assets – computer and communications equipment, backup media, power supplies, printers

Network diagrams should also be included.

Template 2.3: Asset register – computer server 1

Make

Model

Serial number

Location

Supplier

Cost

Purchase date

Warranty

Support

Support supplier

Configuration

System name

Used for (e.g. server, billing, clinical records)

Internet protocol (IP) address

Central processing unit (CPU) speed

CD/DVD

Hard disk drive (HDD) size/make

Random access memory (RAM) size

Internal devices (e.g. modem, network card)

External devices attached (e.g. printer, scanner)

Operating system (OS) and version

OS serial number/licence key

Template 2.4: Asset register – computers

Duplicate this page as needed.

	Computer no.	Computer no.
Make		
Model		
Serial number		
Location		
Supplier		
Cost		
Purchase date		
Warranty		
Support		
Support supplier		

Configuration

System name		
Used for		
IP address		
CPU speed		
Memory RAM size		
HDD size/make		
CD/DVD		
Internal devices		
External devices attached		
Operating system (OS) and version		
OS serial no. /licence key		
Network patch panel no.		
Network wall socket no.		

Template 2.5: Asset register – portable computers (e.g. laptops)

	Portable computer 1	Portable computer 2	Mobile devices
Make			
Model			
Serial number			
Location			
Supplier			
Cost			
Purchase date			
Warranty			
Support			
Support supplier			
Configuration			
System name			
Used for			
IP address			
CPU speed			
Memory RAM size			
HDD size/make			
CD/DVD			
Internal devices			
External devices attached			
Operating system (OS) and version			
OS serial no./ licence key			

Template 2.6: Asset register – printers

	Printer 1	Printer 2	Printer 3
Location			
Make			
Model			
Serial number			
Supplier			
Cost			
Purchase date			
Warranty			
Support			

Configuration

System name			
Used for			
IP address			
Network patch panel no.			
Network wall socket no.			

Template 2.7: Asset register – other peripheral devices (1)

	Scanner	Modem	Uninterruptible power supply (UPS)
Location			
Make			
Model			
Serial number			
Supplier			
Cost			
Purchase date			
Warranty			
Support			

Configuration

System name		
Used for		
IP address		
Network patch panel no.		
Network wall socket no.		

Template 2.8: Asset register – other peripheral devices (2)

	External hard drive	Monitors	Keyboard/mouse
Location			
Make			
Model			
Serial number			
Supplier			
Cost			
Purchase date			
Warranty			
Support			
Configuration			
System name			
Used for			

Template 2.9: Asset register – network equipment

	Router/hub	Firewall (if hardware-based)	Intrusion detection system (IDS) (if hardware-based)
Location			
Make			
Model			
Serial number			
Supplier			
Cost			
Purchase date			
Warranty			
Support			
Configuration			
System name			
Used for			
IP address			
Network patch panel no.			
Network wall socket no.			

Template 2.10: Asset register – network configuration

Type (e.g. client server, peer-to-peer)

IP address range

Subnet mask

Domain/workgroup

Windows internet name service (WINS) server IP

Domain name system (DNS) server IP

Dynamic host configuration protocol (DHCP) server IP

Gateway

Number of data connections

Locations of data connections (and identification)

Could be cross-referenced to network diagram

1.

2.

3.

Maintenance details

Electronic information assets – databases, electronic files and documents, image and voice files, system and user documentation, business continuity and information recovery plans

Template 2.11: Asset register – shared databases

	Used by (which program)	Located on (which computer)	Path and database name (e.g. \\Server\C\program\...)
1.			
2.			
3.			
4.			
5.			

Template 2.12: Asset register – other databases, document and file locations

	Used by (which program)	Located on (which computer)	Path and database name (e.g. \\Reception1\C\programname\...)
1.			
2.			
3.			
4.			
5.			

Software assets – application programs, operating system, communications software

Template 2.13: Asset register – operating system

Name/version

Description

Serial numbers/licence codes

Which computers

Location of media

Location of manuals

Location of licence codes and agreements

Date purchased/upgraded

Supplier

Support details

Template 2.14: Asset register – practice management software program

Name/version

Description

Serial numbers/licence codes

Which computers

Location of media

Location of manuals

Location of licence codes and agreements

Date purchased/upgraded

Supplier

Support details

Template 2.15: Asset register – clinical software program

Name/version

Description

Serial numbers/licence codes

Which computers

Location of media

Location of manuals

Location of licence codes and agreements

Date purchased/upgraded

Supplier

Support details

Template 2.16: Asset register – financial management software program

Name/version

Description

Serial numbers/licence codes

Which computers

Location of media

Location of manuals

Location of licence codes and agreements

Date purchased/upgraded

Supplier

Support details

Template 2.17: Asset register – antivirus/anti-malware software program

Name/version

Description

Serial numbers/licence codes

Which computers

Location of media

Location of manuals

Location of licence codes and agreements

Date purchased/upgraded

Supplier

Support details

Template 2.18: Asset register – secure messaging/ communications software and PKI certificates

Name/version

Description

Serial numbers/licence codes

Which computers

Location of media

Location of manuals

Location of licence codes and agreements

Date purchased/upgraded

Supplier

Support details

Encryption keys

PKI certificates

Practitioner

Details (dongle/smart card, expiry, location)

Medicare certificate PKI-O

HPI-O NASH certificate

PKI-I

NASH-I

Electronic transfer of prescriptions – certificates

eTP supplier

Support details

Encryption keys

Template 2.19: Asset register – other software programs (e.g. pathology, diagnostics download)

Name/version

Description

Serial numbers/licence codes

Which computers

Location of media

Location of manuals

Location of licence codes and agreements

Date purchased/upgraded

Supplier

Support details

Template 2.20: Asset register – email configuration

Practice email address

Incoming mail server (e.g. POP3)

Outgoing mail server (e.g. simple mail transfer protocol [SMTP])

Other details

Template 2.21: Asset register – internet service and configuration

Provider (ISP)

Dial-up number (if still used)

Access plan

Proxy server

Transmission control protocol (TCP)/IP address

DNS

Secondary DNS

Modem type

Support details

Template 2.22: Asset register – documents (location of contracts, operating and professional guidelines, important paper documents)

	Document description (practice to complete)	Location
1.		
2.		
3.		
4.		
5.		

Template 2.23: Network diagrams

Attach network diagrams here.

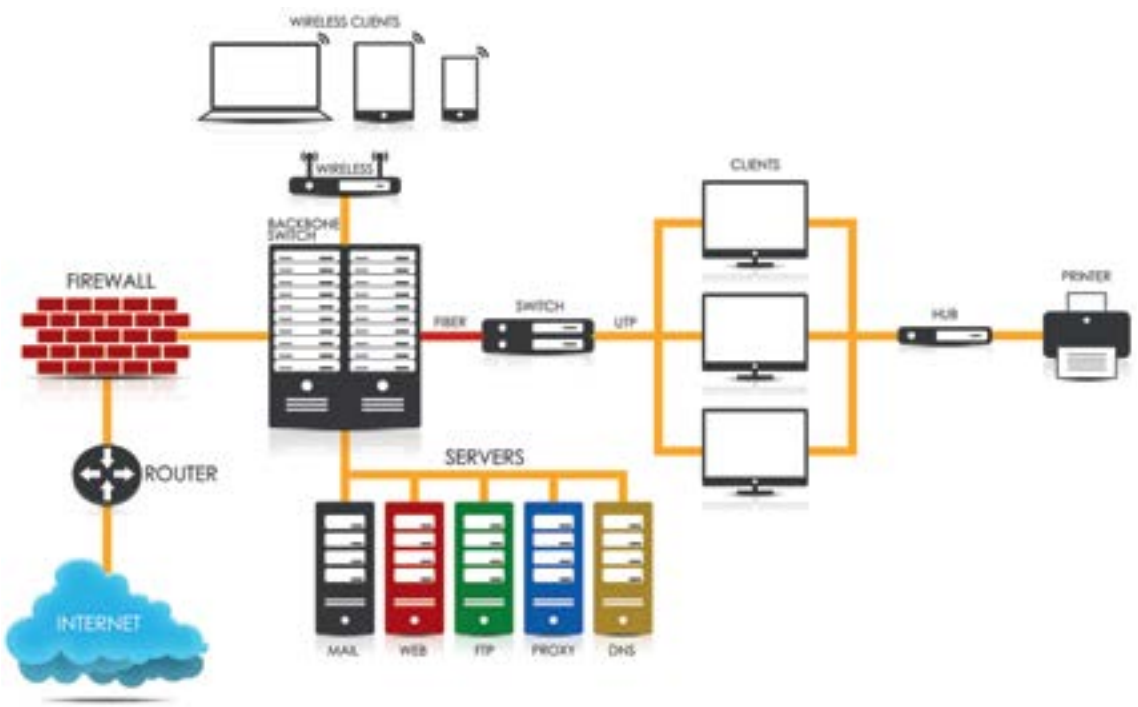


Figure1. Example network diagram.

Identify appropriate controls

Use *Template 2.24* to identify the appropriate controls and existing controls implemented in the practice.

Template 2.24: Risk assessment – threat, vulnerability and controls

Threat/risk source	Disruption/impact	Vulnerability
Human – unintentional – internal (insider threats/staff/authorised third parties)		
Error/omissions (e.g. deletion of files, failure to check backup)	Financial loss Disruption of operational activities Breach of integrity (inadvertent information modification or destruction)	Legitimate access to systems Lack of training
Inadvertent access by staff	Violation of legislation or regulation Breach of confidentiality (potential information disclosure)	Legitimate access to systems by staff Lack of formal implemented policy and procedures, particularly password controls
Inadvertent viewing of information by non-staff	Violation of legislation or regulation Breach of confidentiality	Lack of appropriate access control Staff not following policy
Non-compliance with PCEHR and Healthcare Identifiers legislation	Penalisation of practice or individuals	Staff not following policy or lack of appropriate training
Human – deliberate – internal (insider threats/staff/authorised third parties)		
Theft or damage of equipment	Financial loss Disruption of operational activities	Legitimate access to premises and equipment
Leakage or theft of information	Violation of legislation or regulation Adverse effect on reputation Breach of confidentiality (potential information disclosure)	Legitimate access to systems
Employee sabotage	Disruption of operational activities Breach of integrity (potential information modification or destruction)	Legitimate access to systems Lack of policy and procedure monitoring

Suggested appropriate solutions and mitigation strategies	Solutions		Person responsible
	Existing	Required (to action)	
	Practice to complete		
Staff trained in policy and procedures (see CISS Section 7.2) Information backup and recovery procedures in place (see CISS Section 7.1)			
Access control policy and procedure implemented and monitored (see CISS Section 4.1, 4.2) Breach reporting in place (see CISS Section 2.9) Confidentiality and non-disclosure agreements signed (see CISS Section 3.4) Agreements with third parties signed (see CISS Section 3.5) Password protected screen savers in place (see CISS Section 11.6) Access to system utilities limited (see CISS Section 11.8)			
Staff trained in policy and procedures (see CISS Section 4.1, 4.2) Clear desk and clear screen policy in place (see CISS Section 11.6)			
Staff trained in practice and PCEHR policies (see CISS Section 1) PCEHR and practice policies annually reviewed (see CISS Section 1, 3.6)			
Asset register up to date (see CISS Section 2.5) Removal of all equipment and assets formally recorded (see CISS Section 11.3) Assets (keys and equipment) returned on termination of employment (see CISS Section 4.1) Equipment located to minimise unnecessary access (see CISS Section 11.3) Network connections and cabling protected, including segregation of power and communications cables, electromagnetic shielding, and documented setup of patching (seek technical advice for confirmation of these) Portable devices policy and procedures enforced and monitored (see CISS Section 10)			
Confidentiality and non-disclosure agreements signed (see CISS Section 3.4) Agreements with third parties including compliance with practice policies signed (see CISS Section 3.5) Access rights removed on termination of employment (see CISS Section 4.5) Information securely deleted when equipment and assets disposed of (see CISS Section 11.5) Use of external and personal devices such as USBs controlled or prohibited (see CISS Section 10)			
Access control policy and procedure implemented and monitored (see CISS Section 4) Breach reporting in place (see CISS Section 2.9) Access rights removed on termination of employment (see CISS Section 4.5) Access to system utilities limited (see CISS Section 11.8)			

Threat/risk source	Disruption/impact	Vulnerability
Fraud	Financial loss	Access to systems No monitoring of access or business functions business functions
Email-based social engineering (e.g. phishing)	Breach of confidentiality and unauthorised access	Lack of staff awareness
Misuse of information systems	Financial loss Breach of confidentiality	Lack of usage monitoring
Additional items		
Human – deliberate – external		
Theft or damage of equipment	Financial loss Disruption of operational activities	Inadequate physical controls of system and network
Theft of information	Violation of legislation or regulation Adverse effect on reputation Breach of confidentiality	Lack of appropriate access control Limited network controls

Suggested appropriate solutions and mitigation strategies	Solutions		Person responsible
	Existing	Required (to action)	
Access control policy and procedure implemented and monitored (see CISS Section 4) Breach reporting in place (see CISS Section 2.9) Agreements with third parties signed (see CISS Section 3.5) Access rights removed on termination of employment (see CISS Section 4.5) Information securely deleted when equipment and assets disposed of (see CISS Section 11.5)			
Staff awareness training in place (see CISS Section 6.4)			
Internet and email policy monitored (see CISS Section 6.1) Breaches of policy attract suitable consequences (see CISS Section 2.9) Agreements with third parties signed (see CISS Section 3.5) Auditing and audit review in place (see CISS Section 3.4)			
Asset register up to date (see CISS Section 2.5) Equipment effectively physically protected, including limited access to critical resources such as server (see CISS Section 11.3) Removal of all equipment and assets formally recorded (see CISS Section 11.3) Assets (keys and equipment) returned on termination of employment (see CISS Section 4.1) Equipment located to minimise unnecessary access (see CISS Section 11.3) Network connections and cabling protected, including segregation of power and communications cables, electromagnetic shielding, and documented set up of patching (seek technical advice confirmation of these) Portable devices policy and procedures enforced and monitored (see CISS Section 10)			
Access control policy and procedures in place (see CISS Section 4) Use of external and personal devices such as USBs controlled or prohibited (see CISS Section 10) Breach reporting to authorities in place (see CISS Section 2.9) Perimeter controls including firewalls and IDS security effective (see CISS Section 9) Secure messaging and transfer of information using encryption and authentication in place (see CISS Section 12.2) Removal of all equipment and assets formally recorded (see CISS Section 11.3) Equipment securely disposed of or re-used (see CISS Section 11.5) Logical segregation of networks into clinical, administrative and external access and installation of secure gateway between them to filter traffic (seek advice from technical service provider) Wireless networks segregated as perimeters are ill-defined (seek advice from technical service provider) Other network routing control mechanisms based on source and destination addresses (see technical service provider for advice) Portable devices policy and procedures enforced and monitored (see CISS Section 10)			

Threat/risk source	Disruption/impact	Vulnerability
Fraud	Financial loss	Lack of appropriate access control
Malicious hacking and unauthorised access	Disruption of operational activities Breach of integrity (potential information disclosure, modification or destruction)	Inadequate network and internet protection
Unauthorised access	Financial loss Breach of confidentiality and integrity	

Suggested appropriate solutions and mitigation strategies	Solutions		Person responsible
	Existing	Required (to action)	
Access control policy and procedures in place (see CISS Section 4) Breach reporting to authorities in place (see CISS Section 2.9) Perimeter controls including firewalls and IDS security including incoming and outgoing filtering effective (see CISS Section 9) Network configured to identify unauthorised access attempts and alert (see CISS Section 9.4) Clinical and business information systems separated (seek advice from technical service provider)			
Network configured to identify and record unauthorised access attempts and provide alerts on this (see CISS Section 9.4) Network services configured to deny all incoming traffic not expressly permitted (see CISS Section 9) Remote access methods such as modems secured and use VPNs (see CISS Section 4.6, 9.9) Connection time of users restricted and log-on attempts limited (seek advice from technical service provider) Private IP addresses used on internal networks and unused services disabled on servers accessible to internet (seek advice from technical service provider) Good password policy in place (see CISS Section 4) Physical access to critical equipment restricted (see CISS Section 11) Users required to change passwords regularly (see CISS Section 4) All publicly accessible services put on secured demilitarised zone (DMZ) network segments (see CISS Section 9.5, 12.3) Use of equipment and information off-site includes education and suitable home-office or tele-working security measures (see CISS Section 4, 9.9) Access to system utilities limited (see CISS Section 11.8)			
Network-based IDS and firewalls, email content filtering software, and/or other security controls to identify the use of unauthorised services (such as peer-to-peer file and music sharing), spam and spoofing configured (see CISS Section 6) Log file activity monitored (e.g. email attachments, FTP transfers, web requests) with suspicious words in the filename (e.g. 'confidential', sexually explicit terms) (see CISS Section 6) URL (web browser) filtering implemented for inappropriate sites – whitelisting and blacklisting (see CISS Section 6.3) Portable devices policy and procedures enforced and monitored (see CISS Section 10) Care taken when using wireless networks and using portable devices in public places (see CISS Section 9.10)			

Threat/risk source	Disruption/impact	Vulnerability
Technical – unintentional		
Equipment or hardware failure (e.g. hard disk crashes and telecommunications failures)	Disruption of operational activities	Poor or no backup procedures Lack of system maintenance
Software failure (e.g. bugs, patches)	Disruption of operational activities	Irregular software updates or patching
Information loss	Disruption of operational activities Adverse effect on reputation Breach of confidentiality Financial loss (e.g. loss of billing data)	Poor or no backup procedures Encryption not used appropriately
Power outage or spikes	Disruption of operational activities	Lack of power backup and conditioners Ageing infrastructure
Technical – deliberate		
Malicious code (e.g. virus)	Disruption of operational activities Denial or degradation of service Data loss Breach of integrity	Inadequate network and internet protection Lack of staff training Not keeping anti-virus updates current Inadequate spam filtering
Information loss	Violation of legislation or regulation Adverse effect on reputation Breach of confidentiality	Poor or no backup procedures Lack of appropriate access control
Denial of service (DoS – attempt to make computer resources unavailable)	Loss or degradation of network capacity Loss of internet connectivity	

Suggested appropriate solutions and mitigation strategies	Solutions		Person responsible
	Existing	Required (to action)	
Environmental conditions such as temperature and humidity controlled (see CISS Section 11.3) Two methods of telecommunications routes available for emergency situations (e.g. landline and mobile service available)			
System utilities segregated from application software (seek advice from technical service provider) Security features and limitation of these in application software known (see CISS Section 11.8) Software updates loaded as soon as they become available (see CISS Section 11.8)			
Use of external and personal devices such as USBs controlled or prohibited (see CISS Section 10) Backup policy and procedures in place, and monitored for compliance (see CISS Section 7) Portable devices policy and procedures enforced and monitored including backup of portable device (see CISS Section 10) Encryption used for backups, portable and mobile devices and message transfer (see CISS Sections 6.5, 6.6, 7.5 and 9.10)			
UPS and power line conditioners installed (see CISS Section 11.4) If power supply unreliable alternative power source installed UPS batteries periodically tested (see CISS Section 11.7) Serviceable infrastructure (electricity and telecommunications) maintained			
Anti-malware software automatically regularly updated (see CISS Section 6.3) Precautionary scans of information systems done regularly (see CISS Section 8) Spam filtering activated (see CISS Section 6.5, 6.6 and 9.7) Sender policy framework and domain keys identified email (see CISS Section 6) Staff educated on email attachments (see CISS Section 6.6) All downloaded file segregated from network until scanned and established safe (seek advice from technical support) Use of unauthorised software prohibited (see CISS Section 8) Use of mobile code blocked (e.g. use web browser security to limit program add-ons (unknown ActiveX)) (see CISS Section 6.3) Use of file transfer/peer-to-peer applications limited unless essential to normal operations (see CISS Section 10) Use of external and personal devices such as USBs controlled or prohibited (see CISS Section 10.4)			
Backup procedures are effective and monitored (see CISS Section 7) Breach reported to authorities (see CISS Section 2.9) System utilities segregated from application software (seek advice from technical service provider) Access to system utilities limited (see CISS Section 11.8)			
Intrusion detection system configured to detect DoS (see CISS Section 9.4) Firewall configured to block specified network traffic (see CISS Section 9) Outgoing connections to internet relay chat (IRC), instant messaging and peer-to-peer services blocked (seek advice from technical service provider)			

Threat/risk source	Disruption/impact	Vulnerability
Environmental		
Flood	Disruption of operational activities Endangerment of personal safety	Incomplete business continuity and information recovery plans
Earthquake	Disruption of operational activities Endangerment of personal safety	Incomplete business continuity and information recovery plans
Fire (including bushfire)	Disruption of operational activities Endangerment of personal safety	Incomplete business continuity and information recovery plans
Storm/cyclone	Disruption of operational activities Endangerment of personal safety	Incomplete business continuity and information recovery plans

Suggested appropriate solutions and mitigation strategies	Solutions		Person responsible
	Existing	Required (to action)	
Business continuity and information recovery plans completed and tested and alternative site identified (see CISS Section 5) Effective, monitored backup procedures in place (see CISS Section 7) Critical equipment located away (and protected) from accidental damage (see CISS Section 11.3) Equipment raised off floor to minimise impact of flood, for instance, burst water pipes (consider) Equipment not positioned immediately beneath air-conditioning units Staff trained in emergency procedures relating to flood and electrical issues Other occupational, health and safety provisions applied			
Business continuity and information recovery plans completed and tested and alternative site identified (see CISS Section 5) Backup procedures effective and monitored (see CISS Section 7)			
Business continuity and information recovery plans completed and tested and alternative site identified (see CISS Section 5) Backup procedures effective and monitored (see CISS Section 7) Electrical-based fire fighting equipment available in close proximity to critical equipment Staff trained in emergency (electrical fire) procedures Other occupational, health and safety provisions applied			
Business continuity and information recovery plans completed and tested and alternative site identified (see CISS Section 5) Backup procedures effective and monitored (see CISS Section 7) Other occupational, health and safety provisions applied			

Template 2.25: Security management and reporting, including monitoring compliance and review planning

Risk assessment – review schedule

	Agreed interval	Date of last review	Date of next review
1.			
2.			
3.			

Template 2.26: Education and communication

Risk assessment – staff education record (all staff)

Education method	Date last undertaken	Next date
Induction training including CISS and the personally controlled electronic health record (PCEHR) system		
Formal ongoing training including CISS and PCEHR		
Discussion at meetings		

Template 2.27: Data breach response and reporting

What to do if you have or suspect a data breach

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), 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.
- Notification of the breach
  - Determine who needs to be notified, both internal and external to the practice, and where relevant:
    - notify the organisation's privacy officer
    - notify the police if theft or criminal activity is suspected
    - notify the PCEHR System Operator
    - 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 e-health 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? See Section 9: Computer network perimeter controls in the RACGP *Computer and information security standards* (CISS).

Data breach reporting

Use the following template.

Data incident/breach report

Practice name

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.

Standard 4: Managing access

For explanatory notes refer to Section 4 of the RACGP *Computer and information security standards*.

Template 4.1: Access control – staff access levels and healthcare identifiers

Staff member (Practice nurse)	Healthcare provider identifier – individual (HPI-I)
Practice unit (Name of the practice)	

Program/application (Name of software)	Access level (Restricted information only, full user access and/or PCEHR access)
Healthcare provider identifier – organisation (HPI-O)	

Standard 5: Business continuity and information recovery

For explanatory notes refer to Section 5 of the RACGP *Computer and information security standards*.

Template 5.1: Business continuity – critical business functions

Critical function	System/requirements normally used	Alternative resources
Patient consultations and treatment: – recording clinical notes – prescriptions – referrals This will include any processes that are now or will be in future electronic such as e-prescriptions, pathology requests and e-referrals	Clinical records system Internet connection or electronic messaging service	Paper based/printed forms to be completed by hand *Keep all paper forms in one place for a quicker switch to manual procedures when required*
Appointments	Appointment scheduling program	Copy of current appointment schedule (today's) showing patient telephone numbers Copy of future appointment schedule showing patient telephone numbers
Accounts and billing	Practice management (billing) program	Account holder and patient list Manual invoice/receipts Paper Medicare forms
Practice financial activities (payroll, Medicare claims, banking)	Financial software	Manual banking forms
Communication (e.g. email)	Internet connection	Post or fax
Receiving test results	Internet connection or electronic messaging service	Request printed copies
Recalls and reminders		Paper form to record patients needing a recall or reminder to be entered into computer when back online
Practice to complete		

Template 5.2: Business continuity – additional resources required for continuity and recovery

Resource	Potential reason	To be used for	Who to contact and contact details
People			
Locum staff	Absence of medical staff Additional demand for services	Consulting	(e.g. local GP recruitment services)
Temporary administration staff	Absence of key staff	Reception duties Entering backlog of data	
Practice to complete			
Information and documents			
Hard copies of appointments and patient list	Inoperable computer systems or power outage	Access information	
Staff contact list			
External contact list (healthcare providers, Medicare)			
Practice to complete			
Equipment – computer and telecommunications			
Telecommunications: landline or mobile telephone	Loss of phone system (e.g. power outage)	Contact authorities, patients, healthcare providers	
Alternative infrastructure (e.g. power, lighting, water) generator	Power outage, flooding, natural disaster events	Physical safety (lighting) Resumption of operation (power)	Electricity provider
Alternative computer resources (e.g. a laptop) and copy of electronic information	Server non-operational or power failure	Access critical information such as patient details or appointments	
Dictaphone and batteries			
Practice to complete			
Budget			

Template 5.3: Business continuity – contact and responsibility list in event of incident or disaster

1. Name

Position

Mobile no.

Other contact no.

Responsible for

2. Name

Position

Mobile no.

Other contact no.

Responsible for

3. Name

Position

Mobile no.

Other contact no.

Responsible for

4. Name

Position

Mobile no.

Other contact no.

Responsible for

5. Name

Position

Mobile no.

Other contact no.

Responsible for

6. Name

Position

Mobile no.

Other contact no.

Responsible for

7. Name

Position

Mobile no.

Other contact no.

Responsible for

8. Name

Position

Mobile no.

Other contact no.

Responsible for

Template 5.4: Business continuity – workarounds for critical practice functions

Critical function	Alternative procedure	Person responsible
Patient consultations and treatment: – recording clinical notes – prescriptions – referrals Secretarial services (formatting reports, etc.) *This will include any processes that are now or will be in future electronic such as e-prescriptions, lab requests and e-referrals*		
Appointments	Set up alternative computer (laptop) if possible with copy of appointment system on it or a daily appointment schedule electronic copy to refer to only. Unless the practice has a tested method of updating and integrating appointments made on this copy, use it to refer to only Locate daily printout of appointment schedule (with patient contact numbers). Contact patients in circumstances where appointments need to be rescheduled Record diligently in a manual appointment book all changes to appointments and requests for appointments	Reception staff
Accounts and billing	Manually swipe Medicare cards Manually issue receipts Retain copies of all receipts in a secure location to be entered into the system later	Reception staff
Practice financial activities (payroll, Medicare claims, banking)	Banking	Practice manager
	Medicare claims	
	Payroll	
Communication (e.g. email)		
Receiving test results		
Recalls and reminders		

Template 5.5: Business continuity – corrective actions

Incident *(practice to complete)*	Recovery procedure	Person responsible
Server failure	Write down or capture any error messages Check that no computers are accessing the server (log off all computers) Reboot the server (by authorised staff only) If the server does not reboot correctly: – write down or capture any error messages – call technical support If the server does reboot correctly: – check that the last transactions that are entered (e.g. in a patient record) are correctly recorded on the system	Practice computer security coordinator
Malware (malicious codes and viruses)	Disconnect internet (and email) connection Virus scan all computers Isolate infected computers (disconnect from network) Remove malware (if anti-malware program can fix it) or call technical service provider for assistance Review virus update procedures	
Power failure	Shut down server in orderly manner Establish reason for and extent of power failure. Check power (meter) box for master switch override not tripped and that fuses are intact Call electricity provider to confirm how long power will be off for Post-event: ensure UPS is charging and batteries are functional	
Data file corruption or data loss	Contact technical service provider to ascertain extent of problem Restore affected file from backup or restore system if required	
Network problem	Contact technical service provider to ascertain extent of problem	
Denial of service (DoS): This is where use of the network or systems is prevented by preoccupying the computer resources such as processing power, memory, disk space or bandwidth	Contact technical service provider to ascertain extent of problem Disconnect internet (and email) connections Post-event: notify relevant authorities such as law enforcement; get technical service provider to check configuration and correct vulnerability	
Unauthorised access	Contact technical service provider to ascertain extent of problem Disconnect affected computer or service from network Disable user accounts accessed Disable post-event: notify relevant authorities such as law enforcement	
Inappropriate usage		

Template 5.6: Business continuity – backlog of information schedule

Data entry from manual processing	What needs to be entered?	Person responsible
Re-enter appointments		
Re-enter invoices and payments		
Run banking and administration processes if already processed manually		
Process Medicare claims		
Request re-send of results electronically that may have been received in printed form while computer system was inoperable		
Update consultation notes		

Template 5.7: Business continuity – staff education record

Education method	Date last undertaken	Next date
Practical (physical) exercise		
Review plans and manual scenario walk through		
Raised and discussed at staff meeting		

Template 5.8: Business continuity – business continuity and information recovery plan testing schedule

Testing method	Date of last test	Date of next test
Manual walk through (i.e. Is plan complete? Is it current?)		
Practical (physical) exercise		

Template 5.9: Business continuity – business continuity and information recovery plans update schedule

	Agreed interval	Date of last review	Date of next review
1.			
2.			
3.			

Template 5.10: Business continuity – fault log

1. Date | By whom

   Fault noted | Remedial action performed

2. Date | By whom

   Fault noted | Remedial action performed

3. Date | By whom

   Fault noted | Remedial action performed

4. Date | By whom

   Fault noted | Remedial action performed

5. Date

By whom

Fault noted

Remedial action performed

6. Date

By whom

Fault noted

Remedial action performed

7. Date

By whom

Fault noted

Remedial action performed

8. Date

By whom

Fault noted

Remedial action performed

Standard 7: Information backup

For explanatory notes refer to Section 7 of the RACGP *Computer and information security standards*.

Template 7.1: Backup – example procedure

Backup procedure	Activity	When	Person responsible	Media cycling	Offsite storage procedure
For an automated backup	At the end of the day: Insert backup media for the day in the server Ensure that all other computers have logged out of the server Next morning: Check for any error messages on the server Check that the files on the backup media look correct (name, size and date) Remove backup media and store in secure location	Daily	Receptionist	Daily backup media Weekly Monthly Annual (end of financial year)	

Template 7.2: Backup – backup rotation schedule and checking

	Mon	Tues	Wed	Thurs	Fri	Sat	Sun
Week 1	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked
Week 2	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked
Week 3	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked
Week 4	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked
Week 5	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked	☐ Done ☐ Checked

Note: Weekly backups – have backup media labelled ‘Week #1’, ‘Week #2’ and so on. 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.

Template 7.3: Backup – data restoration and testing procedure

Restoring procedure in the event of a server failure	Person responsible
Locate backup media for the previous day Insert backup media in the server Ensure that all other computers have logged out of the server Perform restore for particular system/files Check that the system/files restored look correct (name, size and date) Check that the system functions correctly Remove backup media and store in secure location	Practice Computer Security Coordinator or technical service provider

Check/test recovery procedure	When	Person responsible
Restore file/system on a different computer to the one on which the system normally runs Check that the restored system functions correctly Compare the records to ensure that the restored files contain the latest information	Quarterly and when system changes are made	Practice Computer Security Coordinator or technical service provider

Standard 8: Malware, viruses and email threats

For explanatory notes refer to Section 8 of the RACGP *Computer and information security standards*.

Template 8.1: Malware software protection record

1. Date | Software (name and version) | Computers

Support | Upgrade procedure

Person responsible | Annual subscription renewed

2. Date | Software (name and version) | Computers

Support | Upgrade procedure

Person responsible | Annual subscription renewed

3. Date | Software (name and version) | Computers

Support | Upgrade procedure

Person responsible | Annual subscription renewed

4. Date | Software (name and version) | Computers

Support | Upgrade procedure

Person responsible | Annual subscription renewed

5. Date | Software (name and version) | Computers

Support | Upgrade procedure

Person responsible | Annual subscription renewed

6. Date | Software (name and version) | Computers

Support | Upgrade procedure

Person responsible | Annual subscription renewed

7. Date | Software (name and version) | Computers

Support | Upgrade procedure

Person responsible | Annual subscription renewed

Standard 9: Computer network perimeter controls

For explanatory notes refer to Section 9 of the RACGP *Computer and information security standards*.

Template 9.1: Network perimeter controls – intrusion detection system configuration

1. Date | Name and version

Hardware configuration | Software configuration

Maintenance required | Support

2. Date | Name and version

Hardware configuration | Software configuration

Maintenance required | Support

3. Date | Name and version

Hardware configuration | Software configuration

Maintenance required | Support

4. Date

Name and version

Hardware configuration

Software configuration

Maintenance required

Support

5. Date

Name and version

Hardware configuration

Software configuration

Maintenance required

Support

6. Date

Name and version

Hardware configuration

Software configuration

Maintenance required

Support

7. Date

Name and version

Hardware configuration

Software configuration

Maintenance required

Support

Template 9.2: Network perimeter controls – firewall configuration

1. Date

Name and version

Hardware configuration

Software configuration

Maintenance required

Support

2. Date

Name and version

Hardware configuration

Software configuration

Maintenance required

Support

3. Date

Name and version

Hardware configuration

Software configuration

Maintenance required

Support

4. Date

Name and version

Hardware configuration

Software configuration

Maintenance required

Support

5. Date

Name and version

Hardware configuration

Software configuration

Maintenance required

Support

6. Date

Name and version

Hardware configuration

Software configuration

Maintenance required

Support

7. Date

Name and version

Hardware configuration

Software configuration

Maintenance required

Support

8. Date

Name and version

Hardware configuration

Software configuration

Maintenance required

Support

Standard 10: Mobile electronic devices

For explanatory notes refer to Standard 10 of the RACGP *Computer and information security standards*.

Template 10.1: Mobile devices and uses

	List the mobile devices (e.g. laptops, portable hard drives, tablets, smart phones)	Briefly describe the mechanism for securing their data
1.		
2.		
3.		
4.		
5.		
6.		
7.		

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

For explanatory notes refer to Section 11 of the RACGP *Computer and information security standards*.

Physical protection

Template 11.1: Physical, system and software protection – UPS

1. Type | Equipment attached | Battery life

   Maintenance required | Support contact

2. Type | Equipment attached | Battery life

   Maintenance required | Support contact

3. Type | Equipment attached | Battery life

   Maintenance required | Support contact

4. Type | Equipment attached | Battery life

   Maintenance required | Support contact

Template 11.2: Physical, system and software protection – procedure for controlled shutdown of server

	When is it necessary to use this procedure?	What to do?	Person responsible
1.			
2.			
3.			
4.			

Template 11.3: Removal of assets record

1. Asset and offsite location

Date out	Name	Signature

Date returned	Name	Signature

2. Asset and offsite location

Date out	Name	Signature

Date returned	Name	Signature

3. Asset and offsite location

Date out	Name	Signature

Date returned	Name	Signature

4. Asset and offsite location

Date out	Name	Signature

Date returned	Name	Signature

5. Asset and offsite location

Date out	Name	Signature

Date returned	Name	Signature

6. Asset and offsite location

Date out	Name	Signature

Date returned	Name	Signature

7. Asset and offsite location

Date out	Name	Signature

Date returned	Name	Signature

8. Asset and offsite location

Date out	Name	Signature

Date returned	Name	Signature

System maintenance

Template 11.4: Physical, system and software protection – system maintenance log

	Date	System maintenance task performed	By whom
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Software maintenance

Template 11.5: Physical, system and software protection – software maintenance procedures

	Task	Person responsible	Frequency	Procedure
1.				
2.				
3.				
4.				
5.				
6.				

Software maintenance log

Template 11.6: Physical, system and software protection – software maintenance log

	Date	System maintenance task performed	By whom
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Standard 12: Security for information sharing

For explanatory notes refer to Section 12 of the RACGP *Computer and information security standards*.

Template 12.1: Secure electronic communication – messaging system record

	Secure messaging system used by practice	Purpose
1.		
2.		
3.		
4.		
5.		
6.		
7.		

RACGP

Healthy Profession.
Healthy Australia.