RACGP
Royal Australian College
of General Practitioners

Information security in general practice

Last updated: 08 11 2022

About this resource

About this resource

Information security is essential in general practice. Creating an informed, proactive cyber secure workplace culture requires continuous learning and is essential to the resilience and success of your practice and the provision of safe, high-quality healthcare. This resource is designed to give you and your practice team the confidence to protect your information systems. It will equip you with key tools to:

- implement robust information security protocols to protect critical clinical and practice data
- manage the ever-evolving cyber security risk landscape
- successfully prepare for, respond to and recover from crisis situations (i.e., cyber-attacks, privacy breaches and hardware system failures)
- align with requirements and legal obligations of the current health technology environment
- keep your patients, staff and business safe.

The information in this resource will also assist you in meeting the requirements necessary for accreditation against the Royal Australian College of General Practitioners (RACGP) *Standards for general practices* (5th edition).

Relevant sections of this resource will:

Standards indicator

- refer you to the relevant indicators under Criterion C 6.4 – Information security from the RACGP *Standards for general practices (https://www.racgp.org.au/running-a-practice/practice-standards/standards-5th-edition)* (5th edition)

These include:

- **C6.4▸A** Our practice has a team member who has primary responsibility for the electronic systems and computer security
- **C6.4▸B** Our practice does not store or temporarily leave the personal health information of patients where members of the public could see or access that information.
- **C6.4▸C** Our practice's clinical software is accessible only via unique individual identification that gives access to information according to the person's level of authorisation.
- **C6.4▸D** Our practice has a business continuity and information recovery plan.
- **C6.4▸E** Our practice has appropriate procedures for the storage, retention, and destruction of records.
- **C6.4▸F** Our practice has a policy about the use of email.
- **C6.4▸G** Our practice has a policy about the use of social media.

Create a policy

- provide specific policy content information

Questions and considerations

- provide critical questions to consider

Tips and information

- offer tips and checklists

Case studies

- provide relevant case studies

About information security in general practice

About information security in general practice

Effective information security in general practice is not optional, it is a way of doing business. It is a continual process, rather than a one-off investment, that involves prevention of inappropriate access, protection of sensitive information and preservation of practice data. Patient or practice team data that is lost, stolen, or inappropriately used or accessed can negatively result in many ways including identity theft or privacy breaches, reputational damage, substantial fines, disruption of daily business activities, along with creating a significant emotional burden on all involved. Patients and staff rely on your practice being proficient in safe and effective data management. This trust can only be maintained when information security is enacted as a business priority. Information security spans across several areas including:

- information that is stored electronically or on paper within your practice
- information that is in transit to or from your practice
- checking and preserving information integrity
- being able to audit changes made to it
- protecting information from unauthorised access
- protecting information from loss

As the digital healthcare landscape in Australia continues to evolve, so do the cyber security risks for general practice and the healthcare sector more broadly. Technologies are rapidly innovating, including digitally supported modes of care and platforms. This creates complexity around the secure and appropriate sharing of data with other health professionals, patients and medical researchers.

Video available at: YouTube (https://www.youtube.com/embed/sTJs8Gc63A4?rel=0 &showinfo=0)

'With the collective global spend on cyber security projected to reach $433bn by 2030, the impact of cyber risk – be it reputational, financial or regulatory – must now be front of mind'[1] for all practice owners. According to a recent report from the OAIC (https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021) , health service providers consistently report the highest number of data breaches compared to other sectors in Australia.

OAIC report: Top industry sectors to notify data breaches (2021)[2]

Australian Government Office of the Australian Information Commissioner (2021) Notifiable Data Breaches Report (http://https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021)

Accessed 5 August, 2022.

The threat of cybercrime – inappropriate or unauthorised criminal access to practices' electronic data – has grown significantly, both in frequency and seriousness. Following the onset of the COVID-19 pandemic in 2020, cybercrime increased by 600 percent, which saw phishing attacks soaring. [3] General

practices frequently faced new forms of malicious software such as ransomware and cleverly designed phishing attacks which, in some cases, led to their sensitive clinical and business data being exposed to the public.

Case study: Australian Red Cross Blood Service

'In 2017, the Australian Red Cross Blood Service was compromised when a file containing information relating to 550,000 blood doners was publicly exposed. This was the result of human error by a third-party supplier. Their prompt response and honesty with affected individuals ensured continued trust after investigations were complete' [4].

Leading risk – human error

The single leading potential risk in a general practice's information security is an internal breach through human error or malicious intent. Cyber-criminals are known to target smaller businesses, such as general practices, as their information security defences are more easily breached in contrast to larger businesses that often dedicate more resources to digital information security. Your entire practice team has a responsibility to ensure cybersecurity measures are in place to protect your practice information systems from cybercrime and online threats. Each person in the practice needs to actively contribute to protecting the practice's information systems.

Information security requires regular investment of time and financial resources. It is important to organise regular team information and training sessions to keep everyone at pace with the changing risk landscape, foster the protection of information assets and build confidence in business continuity when an incident inevitably arises.

It is important to create a culture of open disclosure and a clear process for prompt notification of any incident to practice management.

[1] Leibel, A., & Pales, C. (2001). *The Secure Board.* Haberfield: Longueville Media Pty Ltd.

[2] Australian Government Office of the Australian Information Commissioner . (2001). Notifiable Data Breaches Report . Retrieved from https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021

[3] Leibel, A., & Pales, C. (2001). The Secure Board. Haberfield: Longueville Media Pty Ltd.

[4] Leibel, A., & Pales, C. (2001). The Secure Board. Haberfield: Longueville Media Pty Ltd.

Information security strategy

Information security strategy

To ensure effective information security procedures, it is recommended to have clear policies and procedures to support your practice.

Topics in this module:

- Policies and procedures for managing information security (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-strategy/policies-and-procedures-for-managing-information-s)
- Governance (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-strategy/governance)

Roles and responsibilities of your practice team

- Information security lead (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-strategy/roles-and-responsibilities-of-your-practice-team/information-security-lead)
- Internal and external staff roles for managing information security (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-strategy/roles-and-responsibilities-of-your-practice-team/internal-and-external-staff-roles-for-managing-inf)
- Allocate resources (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-strategy/roles-and-responsibilities-of-your-practice-team/allocate-resources)
- Manage access to your systems and your data – passwords and administration rights (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-strategy/roles-and-responsibilities-of-your-practice-team/manage-access-to-your-systems-and-your-data-passwo)
- Internet and email use (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-strategy/roles-and-responsibilities-of-your-practice-team/internet-and-email-use)

Business continuity and information recovery

- Business continuity and information recovery (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-strategy/business-continuity-and-information-recovery)
- Crisis and disaster management (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-strategy/crisis-and-disaster-management)

Business continuity and information recovery

Business continuity and information recovery

Your general practice needs a documented business continuity plan which includes information on recovery procedures to preserve access to your practice data. In the event of an 'information disaster', this will ensure you can respond as soon as possible to minimise potential loss or corruption of information.

An effective business continuity and information recovery plan brings your practice information systems back to working order when a system failure occurs. The plan should detail how to maintain critical business functions when there is an unexpected system event. It is also important to include how your practice will function in the event of an environmental or natural disaster.

Business continuity and information recovery plans should be reviewed, updated and tested periodically. This includes when there is a technology or procedure change in the practice, or when any changes to legislative requirements occur.

Create a policy: Business continuity and information recovery processes

Ensure all business continuity and information recovery processes are fully documented in your policy so your practice team knows their individual roles and responsibilities in the event of an emergency or disaster.

Standards indicator

C6.4▸D Our practice has a business continuity and information recovery plan.

You must operate a server backup log, maintain and test a business continuity plan for information recovery and have a privacy policy.

Business continuity

Your business continuity plan should cover:

- access to education and training for your practice team on business continuity processes and procedures
- how your general practice functions in the event of an environmental or natural disaster
- how to transfer information between your practice, other healthcare providers, services and government bodies.

When creating your business continuity and information plan, you should:

- identify the functions and resources required to operate your practice at a minimum acceptable level without functional computers
- train your practice team on how your practice systems will be managed 'manually', and which information needs to be collected for re-entering after recovery
- provide advice on how to revert to a paper-based system
- provide advice on 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
    - issuing of prescriptions
    - business financial operations (e.g. payroll, Medicare claims)
    - payroll processing
    - financial reconciliations.

If you are using cloud-based services, you will need to consider creating a cloud services plan. This could include:

- documenting an internet failover plan, including setting up multiple internet connections with different service providers
- establishing manual workarounds (if available) for when your business and clinical applications cannot be accessed
- migration plans to accommodate a sudden change of cloud provider
- documenting key contacts for your cloud service provider including the support desk, account manager, and the address of any websites that display service status.

Information recovery

[See module on Data recovery and restoration for more information. (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/data-recovery-and-backup-restoration)](https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/data-recovery-and-backup-restoration)

Governance

Governance

Addressing information security at a governance level is crucial. A security governance framework will define the acceptable use of information technology (IT) in your practice and outline responsibilities.

Information security roles and responsibilities should be allocated to members of your practice team. These team members should coordinate security-related activities and determine when it is appropriate to engage external technical service providers.

Information security requires regular attention at a practice level. Your practice team members need to be aware of their responsibilities to protect practice information. Information security processes should be documented and followed.

Your information security governance framework should include the following areas:

- protecting your WIFI network (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-equipment/software-requirements/protecting-your-wifi-network)
- allocating resources (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-strategy/roles-and-responsibilities-of-your-practice-team/allocate-resources)
- creating a culture of information security (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-workplace-culture)
- managing access to your systems and data (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-strategy/roles-and-responsibilities-of-your-practice-team/manage-access-to-your-systems-and-your-data-passwo)
- how you will measure the effectiveness of your security controls
- risk assessment (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/prevention-and-risk-assessment-1)
- a business continuity plan with information recovery procedures (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-strategy/business-continuity-and-information-recovery)
- a resilient backup and restoration process for practice data (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/data-recovery-and-backup-restoration)
- regular updates of software and systems (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-equipment/software-requirements/software)
- education and training for your practice team
- security of mobile devices (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-eq

uipment/hardware-requirements/mobile-electronic-devices)

- security of any external devices team members use to remotely access practice data
- information privacy

When developing your information security governance framework, it is important to consider:

- What are the legal and professional requirements for protection of the information held in your practice? Under the Australian Privacy Principles (APPs), APP 11 requires that reasonable steps are taken to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure. Further information is available in the Office of the Australian Information Commissioner's (OAIC's) Guide to securing personal information (http://www.oaic.gov.au/agencies-andorganisations/guides/guide-to-securing-personal-information) .
- what capabilities your practice has in terms of security knowledge and expertise?
- who makes the decisions about the security protections required?
- what processes are in place to assist in decision making about the use of information for purposes other than for what it was collected (e.g. providing health information to external organisations for research or population health planning [secondary use of data])
- how do you know the system and process are working as intended?

Roles and responsibilities of your practice team

Roles and responsibilities of your practice team

It is vital for practice team members to be aware of their roles in information security. All practice team members require a position description clearly defining and documenting their roles and responsibilities and access to clinical and/or business information.

Information security lead

Roles and responsibilities of your practice team

It is vital for practice team members to be aware of their roles in information security. All practice team members require a position description clearly defining and documenting their roles and responsibilities and access to clinical and/or business information.

Information security lead

It is recommended that your practice appoints an information security lead to champion and manage information security.

The information security lead does not need to have advanced technical knowledge, but should be comfortable with your practice's computer operating systems and other relevant software. They should also possess management skills to develop information security policies and to raise awareness of information security governance, help foster a strong security culture and ensure access to adequate and appropriate training for your practice team.

The information security lead will determine what aspects of information security in the practice are outsourced to external technical service providers.

Standards indicator

C6.4▸A Our practice has a team member who has primary responsibility for the electronic systems and computer security.

You must have at least one team member who has primary responsibility for the electronic systems and computer security.

Create a policy

Your practice policy should include the specific information security roles and responsibilities of each practice team member.

Your policy should cover:

- specific information on the roles and responsibilities of each practice team member in relation to information security, including the required levels of access to information systems
- assignment of an information security lead who has access to ongoing training as required
- who is responsible for specific information security tasks
- access to ongoing training for your practice team as required
- education for your practice team in identifying errors or abnormal software behaviour and who/how to notify promptly of any concerns.

☑ **The position description of the information security lead can include:**

- overseeing development of information security policies and procedures
- testing business continuity and information recovery plans
- reviewing and updating policies and procedures as practice and legislative changes occur
- regular monitoring to ensure practice security policies are followed
- maintaining an up-to-date risk assessment
- ensuring technical advice is sought where required
- ensuring secure transfer of electronic information
- arranging access to ongoing information security awareness training for the practice team
- updating the practice management on outstanding security issues
- regular reporting on information security to the practice team
- regular monitoring of system logs and audit reports.

Internal and external staff roles for managing information security

Internal and external staff roles for managing information security

Practice team agreements

You should document all confidentiality and privacy agreements for practice team members, together with an appropriate internet and email use agreement. Practice team members and relevant external providers should sign these agreements.

These agreements act to protect practice owners in the event of legal action, should a security breach occur.

External service provider agreements

Your practice has a responsibility to ensure anyone who has access to practice clinical and/or business information is aware of their obligations to comply with your information security policies.

Technical service providers are usually granted unrestricted access to practice data.

Third-party access for support and problem solving is an issue requiring careful consideration. This is often undertaken remotely, and trust is placed in software and external support service staff. While technical support personnel will be knowledgeable in information security, they may not fully understand the sensitivity and confidentiality requirements of health information. All external technical support providers with access to any of your practice's information should sign confidentiality agreements.

☑ **Technical service provider contractual agreements can include:**

- what can or cannot be viewed when accessing your practice systems. If 'everything', including files saved on workstations can be viewed, all practice team members should be aware of this
- details of backup procedures and testing that meet the needs of your practice
- set response times to provide technical support via telephone, remote access to your systems, in person and onsite, and outside of business hours
- the cost for routine maintenance, additional work in case of system malfunction and the differences in costs for support during business hours and outside of business hours

- details of maintenance schedules
- information on system audits and reporting details on how information assets are disposed of safely and securely
- a signed confidentiality agreement.

☑ **Cloud service provider agreements will require additional details, including:**

- your practice retaining legal ownership of the data
- appropriate internet connection to support the amount of data transferred and any other online functions required
- a Service Level Agreement (SLA) to define the level of service and availability expected from the provider
- storage and management of data in line with Australian Privacy Law
- processes for redundancy and backup protecting data from loss or corruption
- the ability to move your cloud services or data either to another cloud service provider or back into your business for local management.

See module on cloud-based information security for more information (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-equipment/software-requirements/cloud-computing)

Allocate resources

Allocate resources

Your practice needs to recognise and plan for the fixed costs of maintaining hardware and software that supports information security.

Many businesses assume spending money on information security means they are adequately protected. The right budget for your security requirements will depend on the specific needs of your practice. Having an information security professional review your security requirements can help identify security gaps and save costs in the long term.

Manage access to your systems and your data – passwords and administration rights

Manage access to your systems and your data – passwords and administration rights

Standards indicator

C6.4▸C Our practice's clinical software is accessible only via unique individual passwords that give access to information according to the person's level of authorisation.

You must maintain the security of the clinical software passwords of each individual practice team member and maintain a privacy policy.

Administration rights

You should reduce security risks in your practice by introducing access controls. Practice team members only need access to the data required to do their work. Access management ensures accountability and allows you to ascertain who has entered or altered data.

Your practice team should have access to appropriate training in the relevant software, potential risks associated with the software and how to identify errors or abnormal software behaviour before access and passwords are provided.

Your information systems should be set up to generate audit logs providing details of who is accessing, downloading, changing and deleting information. The audit logs should be reviewed periodically and retained in case information is required following an information security incident.

It is good practice to separate your data on different servers, if possible. Ensure your clinical data is on a separate network and server to your website and other business data. Data separation helps contain the risk of data exposure across your entire system.

Create a policy: Administration rights and access to systems

Your practice should develop a policy specifying who has administration rights and access to specific systems. Access to systems should be consistent with the responsibilities outlined in the position description of your practice team members.

Your policy should cover:

- password security to ensure passwords are not written down and placed near practice monitors - keeping written records of passwords introduces unnecessary risk to your information security
- how often passwords are changed – the longer the same password is used, the greater the risk it will become known and used inappropriately
- who in the practice team has the authority to reset or disable user passwords
- restriction of who in the practice team can create and remove users on each practice information system
- a process for recording different access levels and software access for your practice team members
- an established password structure (numbers, characters and symbols)
- the need for each practice team member to create their own password and be responsible for keeping it secure
- not using a shared common password
- the need for passwords to be changed immediately if they have been or are suspected to have been compromised
- the implications when practice team members terminate their employment. Ensure these accounts are deactivated, remote access disabled, and computer equipment, backup media and any access devices (such as keys or entry swipe cards) as well as practice name badges are returned.

The power of passwords

To ensure access to systems is controlled and secure, establish a strong and unique password policy.

While passwords are the most common form of access authentication, password management can be complex as users often have multiple passwords to access various systems.

Remember - keeping written records of passwords introduces unnecessary risk to your information security. Each team member is responsible for creating and remembering their own passwords. Should a password be forgotten, an authorised team member should be able to organise password reset. Most software will allow new passwords to be generated in such cases.

☑ Tips for software password settings

Most software will allow password requirements to be set up so all users can create safe and secure individual passwords. Software can be configured to require:

- default user account passwords to be changed on first login to the system
- a minimum password length (i.e. number of characters)
- a mixture of alphabetic (lower and upper case) and numeric characters and symbols
- that passwords do not use familiar and family names or words that can be found in a dictionary
- that passwords be set to expire to enforce periodic changes
- that dates of birth are not used
- that passwords are not reused
- multi-factor authentication (a combination of two types of authentication) if appropriate for your practice

You should also be able to customise how automatic password saving is addressed in browsers, and whether this function is disabled across the practice network

🗁 Useful RACGP resource:

- Privacy policy template (http://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/privacy)

Internet and email use

Internet and email use

Your practice should have processes in place to ensure the safe and proper work-related use of internet and email.

Your practice team should be educated and trained in best practice processes when using the internet and email. This includes learning about protection measures against malicious software.

Standards indicator

C6.4▸F Our practice has a policy about the use of email.

C6.4▸G Our practice has a policy about the use of social media.

You must maintain a social media and email policy.

Create a policy: Internet and email use

Your policy should clearly define and describe the management and reasonable work-related use of internet and email by practice team members.

Your policy should cover:

- reasonable private use of internet and email by practice team members during business hours
- how email may or may not be used to communicate with patients
- how your practice handles requests to communicate via unencrypted email
- how downloaded files are scanned for viruses
- details of any internet sites or specific content that cannot be accessed
- internet browser security setting requirements
- access to social networking websites such as Facebook and Twitter.

Tips for safe email use

- If you rely on information in your emails, make sure these emails are backed up with the

rest of your data.
- Do not download or open any email attachments when the sender is unknown.
- 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 reply to spam mail and never try to unsubscribe from spam sites.
- Remain vigilant: do not provide confidential information in response 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.

Useful RACGP resources

- Resources on using email in general practice (http://www.racgp.org.au/running-a-practice/technology/business-technology/using-email-in-general-practice)
- Internet and email use template (http://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice)
- Social media in general practice (http://www.racgp.org.au/running-a-practice/technology/social-media/guide-for-the-use-of-social-media)

Policies and procedures for managing information security

Information security strategy

To ensure effective information security procedures, it is recommended to have clear policies and procedures to support your practice.

Policies and procedures for managing information security

Polices should be created to support information security processes in your general practice. Your practice should document all policies and procedures for managing information security.

A policy and procedures manual provides information and guidance to your practice team on the protocols used in managing your information systems. This manual is used to clarify roles and responsibilities, and to facilitate induction of new practice team members.

☑ **To be effective, your policies should be:**

- communicated and provided to all existing and new members of your practice team
- easily accessible (i.e.. made available on your intranet which can be kept current more easily than a paper practice manual)
- explained to team members through regular education and training sessions, at team meetings and during induction
- discussed regularly to maintain relevance
- periodically reviewed to ensure they are current (either six monthly or annually), and updated when changes are made in information security processes in your practice or to relevant legislationre-issued to the practice team when updated.

☑ **Policies should include:**

- a purpose and objectives

- scope (i.e. to whom and what the policy applies, and under what circumstances)
- definition of information security incidents and their consequences
- organisational structure and defined roles, responsibilities and levels of authority
- reporting requirements and contact forms
- processes for providing access to training for your practice team.

Use the RACGP practice policy template (http://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice) sample to create your practice policies.

Create a policy: How practice information is secured

Your policy:

- should reflect the overall strategy of how practice information is secured
- can be kept as a manual, folder or suite of documents accessible to your practice team
- should be made available to the practice team with training offered on all policies and procedures to ensure compliance and implementation, including education for your practice team
- should ensure your practice has a physical layout that means that members of the public cannot view patient health information

Standards indicator

C6.4▸B Our practice does not store or temporarily leave the personal health information of patients where members of the public could see or access that information.

C6.4▸F Our practice has a policy about the use of email.

C6.4▸G Our practice has a policy about the use of social media.

You must maintain a privacy policy, email policy and social media policy.

Useful RACGP resources:

- Privacy policy template (http://www.racgp.org.au/running-a-practice/security/protectingyour-practice-information/privacy)
- Social media in general practice (http://www.racgp.org.au/running-a-practice/technology/social-media/guide-for-the-use-of-social-media)
- Resources on using email in general practice (http://www.racgp.org.au/running-a-practice/security/managing-practice-information/using-email-in-general-practice)

Crisis and disaster management

Crisis and disaster management

It is important to have a plan as to how you would keep your business running should something go wrong (e.g. a natural disaster, cyber-attack or power failure). The RACGP has several documents available (https://www.racgp.org.au/running-a-practice/practice-management/managing-emergencies-and-pandemics) to assist general practices with information security in response to emergency planning, including the Emergency Response Planning Tool (ERPT) (https://www.racgp.org.au/running-a-practice/practice-management/managing-emergencies-and-pandemics/emergency-response-planning-tool) .

The ERPT (https://www.racgp.org.au/running-a-practice/practice-management/managing-emergencies-and-pandemics/emergency-response-planning-tool) is designed to help general practices better prepare for, respond to and recover from the impacts of emergencies and pandemics. The ERPT guides you through a series of planning templates, where critical information about your practice can be entered and saved. This information will be used to create an emergency response plan that is individually tailored to your general practice.

Customised emergency response plans can be accessed on any computer or mobile device that is connected to the internet using your specific username and password. You can and should also print a hard copy resource for future reference, which should be stored offsite.

Prevention and risk assessment

Prevention and risk assessment

Clinical and business information system risk assessments should be performed frequently and documented each time.

A structured risk assessment requires you to:

- record the assets in your practice (an asset register] can be used to document your hardware, software and any other information systems)
- perform a threat analysis
- perform a measurement and analysis of your information security controls

Topics in this module:

- Asset register (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/prevention-and-risk-assessment-1/asset-register)
- Performing a threat analysis (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/prevention-and-risk-assessment-1/performing-a-threat-analysis)
- Analysis of information security (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/prevention-and-risk-assessment-1/analysis-of-information-security-procedures-and-to)

Hidden risks

- Electoronic sharing of information (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/prevention-and-risk-assessment-1/hidden-risks/electronic-sharing-of-information)
- Risks of running unsupported software (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/prevention-and-risk-assessment-1/hidden-risks/risks-of-running-unsupported-software-or-hardware)
- Third party software security (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/prevention-and-risk-assessment-1/hidden-risks/third-party-software-security)
- Patient communication via electronic media – including email (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/prevention-and-risk-assessment-1/hidden-risks/patient-communication-via-electronic-media-includi)
- Social media (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/prevention-and-risk-assessment-1/hidden-risks/social-media)

Asset register

Prevention and risk assessment

Clinical and business information system risk assessments should be performed frequently and documented each time.

A structured risk assessment requires you to:

- record the assets in your practice (an asset register] can be used to document your hardware, software and any other information systems)
- perform a threat analysis [hyperlink to relevant section]
- perform a measurement and analysis of your information security controls

Asset register

Your practice should maintain an asset register. This should include details of the following:

- Physical assets
  - computer and communications equipment
  - mobile electronic devices
  - medical equipment that interfaces with your practice information systems
  - backup media and uninterruptible power supplies
- Information assets
  - databases
  - electronic files
  - image and voice files
  - system and user documentation
  - business continuity and information recovery plans
- Software assets
  - operating systems
  - application programs
  - clinical and practice management software
  - communications software
  - software license keys
  - original software media and manuals
- Personnel assets
  - contact details of key members of the practice team and external service providers including internet service providers, telecommunication service providers, cloud service providers
  - Paper documents

- contracts
- patient records
- other paper documents important to your practice

Performing a threat analysis

Performing a threat analysis

A threat analysis should be included as part of your risk assessment to assess the impact of potential threats to your systems. Ensure plans are in place to minimise threats and vulnerabilities which could lead to financial loss, breaches in confidentiality, loss of information integrity and availability, practice reputation and patient confidence.

Risk assessments can be complex. Your practice may find it valuable to employ a technical service provider or specialist security firm to undertake your practice risk assessment.

Threats can be grouped into three categories:

- **Human** (unintentional and deliberate) – for example, cybercrime using ransomware, the theft of a laptop containing clinical or business information, or unintentional 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

Standards indicator

Criterion C6.4▸D Our practice has a business continuity and information recovery plan.

You must:

- **operate a server backup log**
- **maintain up-to-date antivirus protection and hardware/software firewalls**
- **maintain and test a business continuity plan for information recovery**
- **maintain a privacy policy**
- **store backups offsite in a secure location.**

You should also a add multi factor authentication process for remote access

Please note, additional considerations need to be made if you use cloud-based systems. For example, rather than maintaining a server backup log and backups offsite, you should have a policy to test your cloud-based system.

Create a policy

Develop a policy for assessing the risks to your practice information systems.

This policy should document your risk assessment processes and procedures, detail how a threat analysis is performed, and outline information security breach reporting procedures for your practice.

Your policy should cover:

- the roles and responsibilities of your practice team and technical service providers
- details of the reporting and monitoring schedule for security risks and mitigations
- how your asset register is managed and updated
- details of how data breaches are reported and documented
- details of how breaches are reviewed and analysed when they occur.
- access to ongoing training for your practice team as required
- education for your practice team in identifying errors or abnormal software behaviour.

☑ **Potential risks and threats to consider in your risk assessment include:**

- errors and omissions (e.g. accidental file deletion, inability to restore data from backups)
- unintentional access to information systems by practice staff or non-practice staff
- non-compliance with legislative requirements
- theft or damage of equipment
- inappropriate disclosure or theft of information
- employee sabotage
- fraud
- email threats
- deliberate misuse of information systems
- malicious software and viruses
- unauthorised system or network access
- software/hardware failure (including loss of remotely hosted practice database or software)
- power disruptions
- natural disasters e.g. flood, earthquake, fire, storm/cyclone
- physical protection of data that is stored offsite (e.g. data storage devices such as hard disks.)

Analysis of information security procedures and tools

Analysis of information security procedures and tools

Securing the information held in your practice systems is essential to running your general practice, maintaining professional responsibilities to your patients and ensuring practice information is available when required.

The effectiveness of any information security control procedures you have in place need to be measurable. This will allow you and your practice team to monitor and assess if your information security controls and processes are working.

The challenge with information security is to find a balance between good protection and ease of use.

Make sure your security controls are regularly tested. Ideally, test would take place every three to six months.

To measure your information security controls, consider the following questions:

- How will you know if your information security controls are effective?
- Are they too restrictive? Do they make your systems difficult for the practice team to use?
- What resources are needed if changes to your practice's information security controls are required?

The Essential Eight Maturity Model

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies (https://www.cyber.gov.au/acsc/view-all-content/strategies-to-mitigate-cyber-security-incidents) to help organisations protect themselves against various cyber threats.[5]

Eight mitigation strategies have been identified by the ACSC as essential in achieving adequate cyber security in organisations, including your practice. These strategies are known as the Essential Eight.

Implementing the Essential Eight (https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model-faq) proactively can be more cost-effective in terms of time, money and effort than having to respond to a large-scale cyber security incident.[6]

☑ **The Essential Eight Maturity Model:**

- The *Essential Eight Maturity Model* (https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model) is designed to assist organisations to implement the Essential Eight in a graduated manner, based upon different levels of *adversary tradecraft* (i.e. tools, tactics, techniques and procedures) and *targeting*.[7]
- The likelihood of being targeted is influenced by the desirability of the data you hold. The consequences of a cyber security incident will depend on any confidentiality requirements associated with the data you hold, as well as your requirement for the availability and integrity of your systems and data.[8] Practices are often the target of cyber attacks as they hold private and confidential information and tend to rely heavily on their electronic systems.
- The Essential Eight mitigation strategies include:
    1. application control
    2. patch applications
    3. configure operation system settings
    4. user application hardening
    5. restrict administrative privileges
    6. patch operating systems
    7. multi-factor authentication
    8. regular backups.

Links to other key resources:

The Australian Cyber Security Centre – Essential Eight Maturity Model FAQ (https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model-faq)

[5] Australian Governement. (2022). *Essential Eight Maturity Model FAQ* (https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model-faq) . Retrieved from Australian Cyber Secuirty Centre [6] Australian Governement. (2022). *Essential Eight Maturity Model FAQ* (https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model-faq) . Retrieved from Australian Cyber Secuirty Centre [7] Australian Governement. (2022). *Essential Eight Maturity Model FAQ* (https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model-faq) . Retrieved from Australian Cyber Secuirty Centre [8] Australian Governement. (2022). *Essential Eight Maturity Model FAQ* (https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model-faq) . Retrieved from Australian Cyber Secuirty Centre

Hidden risks

Hidden risks

There are a rage of potential information security risk areas that your practice needs to ensure are not overlooked. These include:

- electronic sharing of information
- running unsupported software or hardware
- fax and paper documents
- patient communication via electronic mediums – including email and social media.

Electronic sharing of information

Hidden risks

There are a rage of potential information security risk areas that your practice needs to ensure are not overlooked. These include:

- electronic sharing of information
- running unsupported software or hardware
- fax and paper documents
- patient communication via electronic mediums – including email and social media.

Electronic sharing of information

'Use of electronic communication in the general practice setting is essential, and yet it generates significant medicolegal risk' .[9]

Your practice may electronically share information via your practice website or social media channels. Sharing information electronically requires a certain level of security to prevent it from being intercepted, changed during transmission or received by unintended recipients. Health information is sensitive by nature, so any communication of this information via electronic or other means must adequately protect your patients' privacy.

Communication of clinical information to and from healthcare providers should be from within your practice's clinical software using secure electronic messaging.

Secure electronic messaging involves two processes: encryption and authentication. *Encryption* means data is electronically 'scrambled' so it cannot be read unless the information is decrypted using a digital key. *Authentication* means the sender can be verified using electronic signatures.

eHealth 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.

There are two key types of information that your practice may electronically share:

1. information that your practice publishes on your practice's website or social media channels, accessible by anybody or by restricted groups of people. Your practice should take reasonable steps to prevent others from changing that information.
2. identified clinical information about your patients.

Systems for electronic communication of clinical information are changing with the development of newer technologies, including those that use Fast Health Interoperability Resources (FHIR). Some of the first common uses of FHIR have been to provide two-way communication between GPs' clinical software and the Australian Immunisation Register and the National Cancer Screening Register.

Currently, the most widely used method of communicating clinical information securely between healthcare providers is secure message delivery, commonly known as SMD.

Providers of SMD are required to meet Australian standards. These SMD packages enable letters and other messages to be sent from within clinical software, and incoming messages to be received into the GP's electronic clinical inbox, where reports of pathology and medical imaging are received.

Email

In the past, standard email lacked security features, making it susceptible to interception. The security of email has increased as a result of the use of encrypted connections between mail servers.

Some clinical software packages now enable documents to be emailed from within the clinical package to other health professionals and organisations, and to patients. These offer protection via the use of a password to access the email.

Create a policy

Your practice should take reasonable steps to make any electronic communication of health information safe and secure.

Your policy should cover:

- how patient-related and other confidential information is sent electronically between healthcare providers
- your practice's approach to using email to communicate patient-related and otherconfidential information between healthcare providers and patientsrecording of patient consent for electronic transmission of their health information
- the maintenance of your website to ensure information is current and correct
- encryption for online transactions such as appointment bookings
- who in your practice team is responsible for maintaining the practice website
- use of social media for your general practice.

Use the RACGP practice policy template (http://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice) sample to create your practice policies.

[9] Carter, D., & Hartridge, S. (2002). Privacy breaches and electronic communication: Lessons for practitioners and researchers. *Australian Journal of General Practice, 51*(7), 497-499.

Risks of running unsupported software or hardware

Risks of running unsupported software or hardware

If your practice is running unsupported software or hardware, you can face some serious risks.

Some of these risks include:

- **No security patches or updates** – most software vendors will release updates and security patches to protect against new security threats. When your software stops being supported, these updates stop for your system. Not using supported hardware and software can place your general practice at risk of data breaches and subsequently of complaints being filed, audits taking place and fines being issued.
- **Software incompatibility** – software vendors may no longer provide support for their software if other software installed on your system is out of date.
- **Loss of functionality** – software relies on the hardware it is installed on, so running unsupported software or hardware compromises information security.
- **Increased data breach risk** – the damage to your practice's reputation if you lose practice information to a data breach can be detrimental.

Third party software security

Third party software security

Third-party software, including ‘add-on’ programs, are commonly used in general practice to enhance practice and clinical systems and to transfer clinical information. For example, data extraction tools, administrative products, and online medical appointment scheduling applications are used to analyse and improve business and clinical performance. Third-party software is also used for electronic prescription exchange and to send secure communications.

Using third-party software can expose your general practice system to threats. Using this software without appropriate information security processes in place can result in core database integrity compromise, unauthorised access into your practice system and data breaches.

Third party software security

When choosing to use any type of third-party software in your practice, consider the following:

- Have you developed policy around the use of third-party software that meets your security requirements?
- How is the third-party software updated? By whom, and will this impact your other systems?
- Does the third-party software meet the necessary APPs requirements? Where and how is extracted and transferred data stored?
- Are you able to test and audit the use of the third-party software?
- What contractual arrangements are in place?
- Where is the data stored?

Your practice may be using multiple software packages from different vendors that access clinical and/or administrative data to perform a range of functions. It is important to consider how these packages send or store data outside the practice and its systems. This includes for 'comprehensive clinical packages'.

Third-party software often uses practice data to complete functions and produce reports. For example, it can be used to provide health information to external organisations for research or population health planning. Your practice team needs to know what the third-party software is doing with any practice data, as consent should be sought for any secondary use of data – that is, information used for purposes other than for what it was originally collected.

See section on secondary use of data for more information.

Patient communication via electronic media – including email

Patient communication via electronic media – including email

The ease of and widely available access to sending and receiving messages electronically means patients are using this medium more frequently to contact their general practice.

The Australian Health Practitioner Regulation Agency's *National Board policy for registered health practitioners: Social media policy* (https://www.ahpra.gov.au/Resources/Social-media-guidance.aspx) is an adjunct to the Medical Board of Australia's Good medical practice: A code of conduct for doctors in Australia and should be read concurrently. Its provisions apply to all registered health practitioners. Another useful resource is the Electronic Transactions Act 1999 (https://www.legislation.gov.au/Details/C2011C00445) .

Create a policy: patient communication via electronic media

Your practice needs to address what content is appropriate to send and discuss via electronic messaging. A policy should be developed concerning the safe use of electronic communication for both practice staff and patients.

- Password protected emails should be utilised. This is now available within Best Practice Software.
- Patients are highly unlikely to send encrypted emails, so content within an email should be limited in scope, with patient consent.
- You should inform patients of possible risks to their privacy if standard unencrypted email is used, this could be included in your standard patient consent forms.
- You should verify and update email addresses, at least on an annual basis.
- Where possible, secure message delivery should be used with compatible encryption processes.

Use the RACGP practice policy template (http://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice) sample to create your practice policies.

It should be noted that the Privacy Act applies to any electronic communication. Refer to section on safe use of internet and email use for further information.

Social media

Social media

The past few years have seen a rapid increase in the number of GPs and general practices embracing social media for business purposes.

While there are clear benefits to using social media for business purposes, there are also potential risks associated with GPs and general practice staff participating in social media.

The RACGP has developed a series of webinars and guides (https://www.racgp.org.au/running-a-practice/technology/business-technology/social-media) which provide guidance around safe and professional use of social media in general practice settings.

Transmission of images of documents by Facsimile ('fax')

Individuals and organisations need to exchange sensitive patient information in a way that is safe, secure and efficient. The RACGP advocates for the use of secure messaging systems because they are the safest, most secure and most efficient communication method. However, despite the considerable efforts of professional bodies, government agencies and industry, the lack of interoperability between secure messaging systems remains a significant barrier to widescale adoption. As such, the use of email in a way that aligns with advice provided in the RACGP's Using email in general practice guide (https://www.racgp.org.au/running-a-practice/technology/business-technology/using-email-in-general-practice) is preferable to the other less secure methods for exchanging patient information, such as fax. With nearly all general practices neither making nor keeping paper records, fax is now a less useful method of sharing information between health professionals and others who make and keep their records electronically. Where paper documents are being faxed (by being passed through a scanner), it is critical to:

- include a cover sheet indicating that the fax is confidential, addressing it to the intended reader without any patient-sensitive information
- ensure fax machines are kept in a secure area to protect information from unauthorised visitors
- verify the recipient's fax number and confirm that the fax was received by the correct recipient/s
- not leave sensitive documents unattended.

To maintain privacy of documents that are received and printed on to paper, the fax device needs to be kept somewhere inaccessible to unauthorised people. Paper documents that have been faxed or received by fax or post need to be disposed of securely once scanned/imported into the clinical record.

Paperless sending and receiving of faxes

The efficiency and security of using fax can be improved, and costs reduced, by eliminating paper. This can be done through virtual fax printing and virtual fax receiving. In virtual fax printing, the document is ‘printed’ to the fax modem instead of on to paper. The networked fax modem is listed as one of the printers on the system. This results in a clearer image at the receiving end. In virtual fax receiving, incoming fax messages are received as images, which are moved to the GP’s electronic clinic inbox or other location as needed.

Information security workplace culture

Information security workplace culture

Often, information security incidents in businesses occur due to misfortune or a lack of knowledge. Practice owners and managers must empower staff with relevant awareness and education to assist in minimising the occurrence and potential impacts of such incidents.

A culture of learning

An information security culture should be promoted within your practice. Educate your practice team on risks to your practice information systems and ensure practice policies outlining responsibilities to manage security risks are up to date and communicated.

You can read more about this in the module on Roles and responsibilities of your practice team (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-security-strategy/roles-and-responsibilities-of-your-practice-team) .

Practice team education

It is essential for you to provide comprehensive education and training for your practice team to support information security in your general practice. Records of when team members have undertaken training should be kept.

Education can include:

- induction training
- discussion at practice team meetings
- formal ongoing training
- ad hoc training sessions when changes are made in the practice or to legislative requirements
- practice drills and exercises to test processes (e.g. a training activity to test your practice's business continuity and information recovery plan can be undertaken using practical exercises in the same way fire drills are practiced).

A reporting culture

Investing in adequate time and education for practice staff will help to establish a confident information security culture that is well informed and willing to report potential threats such as cyber attacks or accidental privacy breaches related to human error.

Train your practice team to identify and report when systems are not working as expected. Make sure your team has a process to follow to report suspicious activity, or if issues with existing security measures arise.

The principles of open disclosure apply to any data breaches that involve potentially identifiable patient

information.

Case study: Creating a security culture

Mandy, a practice manager at a general practice in southeast Melbourne, was alerted to a malicious software cyber-attack that had a detrimental effect on several general practices' computers. The affected practices' electronic systems were rendered completely unavailable, preventing access to all electronic patient and business-critical information.

In response to this news, Mandy immediately organised a meeting to inform her practice team of the rapidly spreading cyber-attack. The team then discussed their previous training and the practice's preparedness for such an incident. They confirmed the practice's information systems were backed up, and the latest systems and software security updates had been installed.

Mandy reviewed online security bulletins for advice and highlighted the necessity for all staff to be vigilant and to be able to recognise a suspicious email. She reminded the practice team not to download files or access links in emails where they did not recognise the sender.

If there was any suspicion a computer had been attacked, its network cable was to be disconnected from the network. This would also disconnect any WiFi access and reduce the chances of the cyber- attack spreading across the entire general practice network.

Useful RACGP resources

- Confidentiality agreement template (http://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice)
- Internet and email use template (http://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice)

Cybersecurity attacks and how to respond

Cybersecurity attacks and how to respond

A cybersecurity incident is a malicious IT event that can involve an attempt to steal data, money or intellectual property, destroy data, or prevent computers or networks from operating.

Such an event can be devastating for a general practice. In addition to the very serious risk of compromising patient data and other sensitive information, it can lead to financial loss, reputational damage, possible legal liability, identity theft and potential for loss of access to critical business systems.

General practices are particularly vulnerable to cybersecurity incidents as they hold valuable data and can be seen as an easy target for cybercriminals.

The RACGP has created a fact sheet on responding to a cybersecurity incident to (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/responding-to-a-cybersecurity-incident) help GPs and practice staff understand:

- signs of a cybersecurity incident
- common types of incidents including phishing, malware and ransomware
- how to prepare and prevent a cybersecurity incident
- how to respond to a cybersecurity incident and ransom demands
- step-by-step information on what to do to limit the damage, resume clinical practice, and prevent future incidents.

Standards indicator

C6.4▸D Our practice has a business continuity and information recovery plan.

You must maintain up-to-date antivirus protection and hardware/software firewalls.

Please note, if using cloud-based systems, you must develop policies that ensure strong security features, and backups must be available. It is recommended that you test your cloud systems to ensure efficiency.

Create a policy: Protecting against malicious software

Your policy should specify monitoring procedures to detect malicious software and provide advice on what to do if malicious software is detected.

Your policy should cover:

- the malicious software protection used and enabled on all practice computers
- access to disable, bypass, or adjust the setting on malicious software protection
- how updates of malicious software protection occur
- the process for scanning all incoming email attachments
- the process for scanning all documents imported into your practice information systems
- how automatic data/signature file updates are managed
- managing the ‘cookies’ feature in web browsers so it is turned off (although some legitimate software may need this turned on to function properly)
- access to training for the practice team in malicious software prevention and how to report all incidents
- automatic upgrades occurring on computers left running out of practice hours.

Notifiable data breaches

Notifiable data breaches

A data breach occurs when personal information held by your practice is lost or subjected to unauthorised access. All breaches or suspected breaches should be recorded in a data breach register and practice management must be notified whether they are from a cybersecurity attack or otherwise.

Data breaches can occur:

- through unauthorised access to your databases
- through intentional and inappropriate disclosure of information by practice team members
- when personal information is incorrectly disclosed
- when sending a patient's personal details and/or health information to the wrong recipient
- if a practice team member is deceived into improperly releasing the personal information of another person
- through loss or theft of laptops, mobile devices, or removable storage devices
- when discarded hard drives or digital storage media still contain your practice information
- through lost or stolen paper records.

Source of breaches

According to the Australian Government Office of the Australian Information Commissioner (OAIC) (2021), (https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021) malicious or criminal attacks were the largest source of data breaches notified to the OAIC, accounting for 55% of breaches. Human error remained a major source of breaches, accounting for 41% of breaches.

This indicates that staff training is critical in minimising your practices risk of data breaches as part of a robust information security culture.

OAIC: Source of breaches (2021)[10]

Australian Government Office of the Australian Information Commissioner (2021) Notifiable Data Breaches Report (https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021) Accessed 5 August, 2022.

Top causes of human error breaches included:

- personal information emailed to the wrong recipient (43%)
- unintended release of publication (21%)
- loss of paperwork or data storage device (8%)[11]

Leading risk – personal information emailed to the wrong recipient

A leading potential risk in a general practice's information security is the high incidence of personal information being emailed to the wrong recipient, otherwise known as human error. To reduce such occurrences, it is critical to regularly confirm with each patient that the email address you have listed against their name on your Patient Management System is correct and up to date. Aim to confirm patient email addresses every six months or, at a minimum, annually. Your entire practice team has a responsibility to ensure cybersecurity measures are in place to protect your practice information systems from cybercrime and online threats. Each person in the practice needs to actively contribute to protecting the practice's information systems.

Notifiable data breaches

The Privacy Amendment (Notifiable Data Breaches) Act 2017 establishes a Notifiable Data Breaches (NDB) scheme. Organisations covered by the Australian Privacy Act 1988 are required to notify individuals at risk of serious harm caused by a data breach. For further information on notifiable data breaches, visit the OAIC website (https://www.oaic.gov.au/privacy/notifiable-data-breaches) .

If your practice believes an eligible breach occurred resulting in serious harm to patients, the mandatory notification law requires you to:

- prepare as soon as practicable a statement for the OAIC detailing the breach
- subsequently notify each affected patient of the content of that statement (if not practical, your practice must publish a copy of the statement on its website). website

Case study: Privacy breaches and electronic communication

The Australian Information Commissioner ordered a Victorian general practice to pay $16,400 in compensation following a breach of privacy. This is the largest award of compensation made by the Commissioner in the context of a medical or healthcare privacy matter. The practice had inadvertently sent an email containing sensitive information to an incorrect email address. The email included information concerning the human immunodeficiency virus status of the complainants. Read the full story, complete with recommendations here (https://www1.racgp.org.au/ajgp/2022/july/privacy-breaches-and-electronic-communication) .[12]

Useful RACGP resources

- Notifiable Data Breaches (NDB) scheme (http://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/notifiable-data-breaches-scheme) – Fact sheet
- Managing notifiable data breaches in general practice flowchart (http://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/notifiable-data-breaches-scheme)
- Article: The Age - The fire drill: Why everyone in a firm needs cyber security awareness (https://www.theage.com.au/business/companies/the-fire-drill-why-everyone-in-a-firm-needs-cyber-security-awareness-20210331-p57fnf.html)

[10] Australian Government Office of the Australian Information Commissioner . (2001). *Notifiable Data Breaches Report (http://https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021)* .

[11]Australian Government Office of the Australian Information Commissioner . (2001). *Notifiable Data Breaches Report (http://https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021)* .

[12] Carter, D., & Hartridge, S. (2002). Privacy breaches and electronic communication: Lessons for practitioners and researchers. *Australian Journal of General Practice, 51*(7), 497-499.

Information backup

Information backup

Your practice should have reliable information backup systems to support timely access to business and clinical information.

Topics in this module:

- About backups (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/about-backups)
    - The cost of data loss (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/about-backups#loss)
    - What types of data need to be backed-up? (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/about-backups#types)
- Equipment needed (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/equipment-needed)
- Backup storage (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/backup-storage)
    - Offsite backup storage (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/backup-storage#offsite)
- Validate and test your backups (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/validate-and-test-your-backups)
    - Planned server shutdown (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/validate-and-test-your-backups#server)
- Practice roles for the backup and recovery plan (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/practice-roles-for-the-backup-and-recovery-plan)
    - Working with a third-party IT provider (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/practice-roles-for-the-backup-and-recovery-plan#provider)
- Types of backup (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/types-of-backup)
    - Cloud backup (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/types-of-backup#cloud)
    - Local backup (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/types-of-backup#local)
    - Offsite backup (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/type

s-of-backup#offsite)
- Online backup (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/types-of-backup#online)
- Information backup video (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/types-of-backup#video)

About backups

Information backup

Your practice should have reliable information backup systems to support timely access to business and clinical information.

About backups

Backup is the process of copying files or databases so that they are preserved in the event of equipment failure or other catastrophes. It is essential that practices have robust backup procedures in place. For practices using cloud-based systems, it is recommended to consider cloud-to-cloud backup solutions.

It is highly recommended to keep separate copies of your critical business data in multiple places in case data loss occurs. This data needs to be kept safe, offsite and, if possible, encrypted. The more secure copies of data you have, the safer it will be.

Backing up business-critical information is a requirement for a general practice to achieve accreditation (refer to the RACGP's *Standards for general practices* [4th edition], Criterion 4.2.2 Information security). It is recommended that practices have a reliable and robust information backup system to support prompt and secure access to business and clinical information.

The creation of a backup process may require assistance from a technical service provider.

☑ Backup processes and accreditation

To meet accreditation, and for purposes of business continuity, ensure your practice backup process:

- is checked at regular intervals (i.e. daily), including the ability to recover the data
- is consistent with the business-continuity plan your practice has developed, tested and documented
- details how to access backed up information and in which offsite locations information is securely stored, both digitally and in hard copy.

About backups

All practice management and clinical systems data, as along with other relevant documents, email files and user profiles should be backed up. You may require different backup and recovery procedures to manage these requirements.

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

The cost of data loss

The loss of critical data has the potential to create substantial financial and operational costs to your practice when trying to restore day-to-day business operations.

> The amount of data lost, along with the reliability and efficiency of your practice's data recovery system and processes, will determine the magnitude of the cost.

A severe disruption and loss of data could cause significant downtime in daily operations, as well as loss of financial revenue. Additionally, if a business continuity plan is not in place, the cost of restoring data by outsourcing to a data loss prevention company can be expensive.

Case study: The cost of not regularly testing your backups

A practice in New South Wales suffered a devastating failure when a power outage occurred during the night and the uninterrupted power supply (UPS) did not correctly shut down the servers. The UPS instead ran until it was exhausted, and the servers were suddenly without any power. This corrupted the database.

When IT support tried to restore the data from the previous night's backup and earlier versions, it was discovered that those three most recent backups were unusable. Unfortunately, no one in the practice was aware the backups were unusable as they had not been tested for readability.

The practice consequently lost three days' worth of patient and business data, which proved to be disruptive and expensive for months afterwards.

The loss of data resulted in patients arriving for previously booked appointments that were no longer recorded in the practice systems, due to the faulty backups. GPs in the practice had to rely on patients to provide information on what had occurred during visits on the days where the clinical information system data was missing. The total cost resulting from the loss of data for a practice with 12 full-time equivalent (FTE) GPs is likely to have run into the tens of thousands of dollars.

☑ Press print on appointments

To prepare for a computer failure, you may wish to consider printing out a copy of the following day's appointments each evening. Doing so will allow your practice to continue running and keep appointments while the computer issue is being resolved.

☑ Backup terminology

Backup is the process of copying files or databases so they can be restored in the event of equipment failure or other catastrophes.

Optimal backup processes are where multiple security controls are layered throughout an IT system to reduce the risk of a network attack. This is an extremely thorough backup process. It provides extra assurance that business-critical information is secure and easily recovered in the event of a disaster or system failure.

Redundancy is the method of using more internal drives than necessary to duplicate and store data, storing it in more than one place. It offers immediate data protection against drive failure. Another benefit is that the system will indicate if one of the internal drives has failed, offering you the chance to backup important data and replace the failed drive.

Synchronisation is a process in which files in multiple locations update each other, copying changes back and forth, whether it be real-time local or offsite. There are many different file synchronisation software packages available.

☑ Optimal backup process

- When using the 'optimal backup' approach, the primary physical server database (both clinical and financial) is synchronised to a secondary onsite physical server every 15 minutes and checked daily.
- Additionally, the backup is synchronised over the internet to a cloud-hosted storage site

overnight. This occurs automatically.
- Data is backed-up daily to a NAS and a USB hard drive (which is rotated) and is then stored offsite.
- It is recommended to backup up your entire server system daily using third-party software in case a 'bare-metal restore' is required. Archived backups dating back at least three years are kept offsite and stored in a dedicated archive server, allowing your computer system to be restored following a catastrophic failure of some sort.
- If a backup is not completed successfully, failure notification email messages are automatically sent to the IT team and practice manager.
- The entire process must also be documented and reviewed periodically.
- Implementing thorough 'defense in depth' backup protocols across your practices will ensure the entire database can be restored and that your practice can return to normal working order quicker in the event the system completely fails.

What types of data need to be backed-up?

All information that is critical to the operation of your general practice should be backed-up. This includes:

- clinical information system data, including patient healthcare information
- patient demographic and contact details, billing and financial information, appointments and practice management
- business management information including staff details, payroll, IT and any relevant third-party contact details
- web page data.

The type of data you are backing up will determine your method and process:

- **Critical data** – e.g. your patient healthcare information and any data required to run your business. You may want to have redundant backup sets that extend for several backup periods. Critical data must be encrypted and kept secure.
- **Sensitive data** – e.g. personal health information details. It is recommended that you ensure backup data is physically secured and encrypted.

Create a policy: Information backup

Your policy should outline all processes and procedures for backing up your practice data.

Your policy should cover:

- how to complete all practice backup procedures correctly
- how your backups are encrypted
- where copies of your business-critical data and backup are stored (both onsite and offsite are recommended)

- how your backup data is restored
- how long it takes to restore your backup data
- managing your archived data in a format readable by your current hardware
- your practice's obligations under national and state records legislation relating to the retention of patient information
- practice team education and training for those with authorisation for backup access on backup processes
- details of which practice team members are trained and authorised to perform backup procedures
- details of any automated backup processes
- testing data restoration regularly (daily is recommended)

Standards indicator

- **C6.4▸E** Our practice has appropriate procedures for the storage, retention, and destruction of records.

  You must maintain and test a business continuity plan for information recovery and maintain a privacy policy.

Equipment needed

Equipment needed

Backup hardware and technology must be prioritised as a key budget item, as it offers a fundamental step to ensuring business continuity of your practice.

You must have appropriate backup hardware and software in order to perform backups. Timely backups may require several backup devices and sets of backup media.

There are several types of backup hardware:

- portable hard drives
- USBs
- transfer of data to another computer or hard drive (i.e. network backup)
- or data backup to the cloud.

It is recommended that you use different types of backup media to provide you with multiple options for restoring data and to keep your backup media up to date with the technology available.

Your data storage strategy and the types of backup media you use will depend on the volume of data and available budget.

See the Types of backup module (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/information-backup/types-of-backup) for more detailed information on the benefits and challenges of each.

Backup rotation

More than one backup method should be used, if it is practical to do so. Backup media should be cycled, or rotated, so that there are multiple backup copies of the practice data at any point in time.

Avoid offshore data storage where possible

It is essential to consider where your practice's backed-up data is held. Online and cloud servers may be located outside of Australia. It is the responsibility of each general practice to ensure that their information is stored only in countries with privacy protections that are compatible with Australian law.

Backup storage

Backup storage

The physical protection of backup media is important. All of your practice's backup media should be securely stored with carefully controlled access. A record of who has taken any backups offsite should be kept, and the most recent backup should be maintained. Lost or stolen data can lead to identity theft and breaches of patient privacy.

If your main backup is to NAS, an air-conditioned room will keep it and other hardware from overheating.

Offsite backup storage

For general practice accreditation, it is recommended that your backups are stored offsite as this is essential to recovering your information in the case of a natural disaster. Your offsite storage location should also include copies of the software you might need to install to re-establish and restore operational systems.

Ensure you have offsite copies of:

- installation media for practice software
- license information
- operating system details.

It is important to be aware of the physical environment in which backup media is stored (i.e. a cupboard or a safe). The storage location/s you choose should be hazard-free to ensure your media does not become damaged.

Validate and test your backups

Validate and test your backups

It is vital that you have a process established to determine your backups have successfully completed. Backup failures are often only detected when it is necessary to use the backup to restore data. It is recommended you have a system of daily, weekly, monthly and annual backups to ensure backup reliability.

It is important to regularly test the integrity of your backup data. This ensures the backup has been successful and that the data is accurate, correct, complete and preserved for future use.

Backup testing

You can check your backups by validating the data against what is in your live system via a test computer. This can be done automatically by your software, by your IT provider or manually by your practice team.

Planned server shutdown

As part of your normal IT maintenance processes, it is good practice to routinely back up your entire server and schedule a planned server shutdown. This allows you to test the recovery process in your practice.

You should choose the time for a controlled shutdown process wisely, as it can often take up more time than you may have anticipated (i.e. try to schedule controlled shutdowns at a times when the process is less likely to impact day-to-day business, such as out of business hours or overnight).

The processes and procedure for a controlled shutdown should be fully documented.

Your clinical information system is likely to have an inbuilt automated backup function. You should consult with your vendor regarding how these backups are undertaken and how they can be accessed if required.

Case study: The severe repercussions of not performing backups

A medical centre that had been operating the same clinical information system for the past five years encountered a serious and prolonged power outage.

This power outage left the medical centre's hardware to rely on its battery backup system to help 'softly' shut down its systems in the correct manner and sequence to avoid hardware damage and data corruption. Unfortunately, in the same way data backups need to be tested for validity, the battery backup had not been tested and failed when it was needed for the first time, leaving the server unprotected when power was cut.

The consequences of not shutting down or restarting the practice's computers safely were catastrophic.

As a result of the power outage, the medical centre discovered it had not performed any backups of patient data, or of the server itself. The failure of the server hard drives and the subsequent data corruption due to the sudden power outage left the medical centre unable to recover any electronic patient files. This loss of data was a major disruption, as the medical centre had been in operation for 15 years and had converted to electronic records five years earlier.

Practice roles for the backup and recovery plan

Practice roles for the backup and recovery plan

It is critical that you have a primary contact for your practice's backup and recovery plan and have a written agreement clearly outlining their role and accountabilities. This role is a key responsibility. You must ensure that the designated person has the required skills, including the ability to navigate and minimise the impact a data loss or backup failure will have on your practice. This staff member may also be responsible for performing and/or monitoring the daily backup and recovery of data.

Alternatively, your practice may contract a third-party IT company to manage your backup and recovery processes. This option requires a written agreement that outlines the third-party organisation's roles and accountabilities.

Working with a third-party IT provider

PART A: Selecting a third-party IT provider to manage your backups

If you decide to employ the services of an external IT provider, there are several questions to consider in order to choose the right one to suit your practice needs:

- What is the history and background of the IT business? Does it have experience in the healthcare industry?
- What are the qualifications and expertise of the business' staff members?
- What type of hardware (if any) is supplied and what is the warranty period?
- What are the details of the service agreement? You should request a copy of the service agreement prior to finalising your decision and ensure that you and the IT provider have agreed on the same terms of the service delivery.
- What insurance cover does the business have?
- What risk management strategies are in place? Are these reviewed on a regular basis?
- Will the business be available to provide support if you run into trouble? What does this process look like?
- Does the business provide remote monitoring and maintenance systems?
- Is there remote monitoring of backup and regular restoration from backup?
- Does the business' area of expertise cover site servers or cloud-based systems, or both?
- What is the cost of the service? Are there differing price structures depending on the level of support required (e.g. 24 hour monitoring to ensure there is no down time)?
- What support does the business provide when the practice is undergoing accreditation?
- Has the company experienced a data breach previously? How did they respond to this and

what was the impact on the business it was providing service for?

Refer to the checklist in the 'Contracts' chapter of the RACGP's *Guide for hardware and software requirements in general* (http://www.racgp.org.au/download/Documents/e-health/requirements/Contracts.pdf) *practice* (http://www.racgp.org.au/download/Documents/e-health/requirements/Contracts.pdf) for further information on reviewing contracts and service-level agreements with external IT providers.

PART B: Consulting with your selected IT provider to manage your backups

When considering different types of backups for your practice, it is essential to consult with a trusted and validated IT professional about your specific, unique requirements. Once you have selected a suitable IT provider, you may wish to ask them questions such as:

- Who is responsible for ensuring the backup happens?
- How often should we backup our data?
- Where is the data being held offsite and is it being held securely?
- What information do we need to back up?
- What is your role in our practice's business continuity plan?
- How quickly can our practice recover in the event of a disaster?
- Is our practice backing up all the data it requires?
- How do we perform routine checks to validate that our backup data is complete and correct?
- How do we regularly test the restoring of our backup data?
- What type of security is used to protect our practice backups?

Useful RACGP resources

- Guide to information backup in general practice (http://www.racgp.org.au/running-a-practice/security/managing-practice-information/guide-to-information-backup)
- Effective solutions for e-waste in your practice (http://www.racgp.org.au/running-a-practice/security/managing-practice-information/e-waste)
- Privacy and managing health information in general practice (http://www.racgp.org.au/running-a-practice/security/protectingyour-practice-information/privacy)

Other resources

- Office of the Australian Information Commissioner (OAIC), Guide to securing personal information (http://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information)
- Australian Digital Health Agency, Information security guide for small healthcare businesses (http://www.digitalhealth.gov.au/about-the-agency/digital-health-cyber-security-centre/information-security-guide-for-small-healthcare-businesses)

Types of backup

Types of backup

Cloud backup

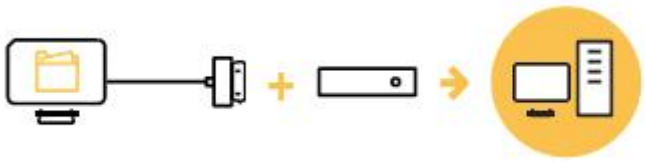
Login and upload to the cloud

This process allows ongoing backup to a storage medium that is always connected to the internet. The term ‘cloud’ refers to the backup storage facility being accessible from the internet.

Cloud backup is different to online backup in that the data can be accessed securely from any other computer with an internet connection.

Pros	Cons
☑ Good physical protection ☑ Easy to access ☑ Files are automatically backed-up ☑ Data is replicated across several storage media	☒ More expensive than local backups ☒ Slow initial backups ☒ Slow to restore ☒ Requires fast internet connection for optimal performance ☒ Increased cyber security risk

Local backup

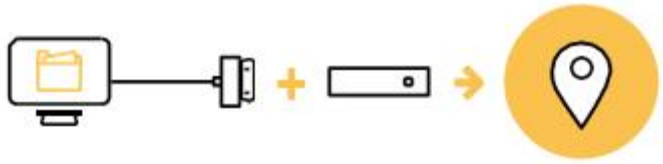


Backup by connecting directly to a storage device

This involves any backup where the storage medium is kept close at hand. Typically, the storage medium is plugged directly into the computer that is being backed-up.

Pros	Cons
• ☑ Good protection from hard-drive failures, virus attacks, accidental deletes • ☑ Fast backup and restore • ☑ Low cost • ☑ Backups are easily obtained • ☑ Full internal control over the backup device (no third party involved)	☒ Does not offer good physical protection from theft and natural disaster ☒ Prone to virus attack and accidental deletes

Offsite backup



Backup by connecting to a storage device which is then relocated offsite

This is where the backup storage medium is kept at a different geographic location from the source. The backup is initially completed locally on the usual storage devices. The storage medium becomes an offsite backup once it is taken to another location.

Pros	Cons
☑ Offers additional protection from natural disasters in comparison to local backup	☒ Requires more due diligence to bring the storage media to the offsite location ☒ Increased handling increases risk of damaging the device

Online backup

Login via internet and upload directly to a storage device offsite

This is a storage medium that is always connected via the internet and is usually located offsite.

Pros	Cons
☑ Good physical protection ☑ Data is replicated across several storage media ☑ Frequent backups ☑ Requires little manual interaction after setup	☒ More expensive than local backups ☒ Initial backups are slow ☒ Slow to restore

Information backup video

Video available at: YouTube (https://www.youtube.com/embed/FHG1hkZSW-w?rel=0 &showinfo=0)

Securing your network and equipment

Securing your network and equipment

Computer systems need to be physically protected from theft and unauthorised access. The role of your technical service provider is not only to provide an emergency response when problems arise, but to also undertake regular and ongoing maintenance of your systems and provide advice on what physical protections are required.

Topics in this module:

- Maintenance of your computer hardware, software and operating system (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-equipment/maintenance-of-your-computer-hardware-software-and)

Software requirements

- Software (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-equipment/software-requirements/software)
- Network perimeter controls (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-equipment/software-requirements/network-perimeter-controls)
- Vulnerability assessment and penetration testing (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-equipment/software-requirements/vulnerability-assessment-and-penetration-testing)
- Protecting your WIFI network (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-equipment/software-requirements/protecting-your-wifi-network)
- Cloud computing (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-equipment/software-requirements/cloud-computing)

Hardware requirements

- Hardware (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-equipment/hardware-requirements/hardware)
- Mobile electronic devices (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-equipment/hardware-requirements/mobile-electronic-devices)
- Protecting and maintaining your physical hardware (https://www.racgp.org.au/running-a-practice/security/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-equipment/hardware-requirements/protecting-and-maintaining-your-physical-hardware)
- Secure destruction and de-identification (https://www.racgp.org.au/running-a-practice/securit

y/protecting-your-practice-information/information-security-in-general-practice/securing-your-network-and-equipment/hardware-requirements/secure-destruction-and-de-identification)

Software requirements

Software requirements

Software is a program (or group of programs) that performs specific functions that are stored and run by hardware. Software is important to a general practice as these programs are used to store information and run the business side of practices.

Network perimeter controls

Network perimeter controls

Network perimeter controls protect your practice systems and local network by controlling data entering and leaving your local network. They are essential for anyone using the internet.

Your practice should have reliable network perimeter controls in place including multiple protection mechanisms such as firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS), virtual private networks (VPNs), content filtering and malicious software protection. Qualified technical support can be engaged for installation and configuration of these mechanisms.

Remote access to your practice information systems via a wireless network is convenient, but requires additional security measures. Any type of remote access should have encryption, such as multifactor authentication, set up to ensure information confidentiality is maintained.

WiFi networks and devices should have encryption set up to ensure information confidentiality. It is important that you follow vendor guidelines and speak to your technical service provider about secure WiFi configuration for your practice.

Software

Software requirements

Software is a program (or group of programs) that performs specific functions that are stored and run by hardware. Software is important to a general practice as these programs are used to store information and run the business side of practices.

Software

Software is a program (or group of programs) that performs specific functions that are stored and run by hardware. Software is important to a general practice as these programs are used to store information and run the business side of practices.

Examples of common practice software include:

- operating systems, software versions and licences
- security software
- backup software
- monitoring software
- clinical and business software
- patch management software
- remote access software and secure messaging capability.

All software should support your business requirements. It is recommended to seek guidance from an IT professional on your specific requirements and how to mitigate any security risks associated with these requirements.

Create a policy: System and software maintenance

Your practice policy and procedures should include system and software maintenance.

Your policy should confirm the requirement for:

- all system maintenance performed by your practice team or technical service provider to be documented
- Regular system maintenance to occur, including:
    - upgrades to clinical desktop system software
    - preventive maintenance

- planned upgrades
- maintaining and updating testing environments
- monitoring for intrusions and installations of unauthorised programs
- checking system and error logs
- ensuring antivirus and other protective software is up to date
- checking disk capacity (hard disk space)
- running patching updates to rectify security weaknesses in earlier software versions
- software version control to maintain software in accordance with the vendor's guidelines.

Vulnerability assessment and penetration testing

Vulnerability assessment and penetration testing

Vulnerability assessment and penetration testing (VAPT) is commonly used to test the security of information networks. Vulnerability assessment works to identify security weaknesses in an IT network. Penetration testing simulates real-world scenarios to discover and exploit security gaps that may lead to unauthorised system access and stolen records.

VAPT should be performed regularly:

- as part of standard IT and network security management
- when new infrastructure or applications are added to the network
- when user policies are changed
- when there are significant system upgrades.

For more information on VAPT, contact your IT professional.

Standards indicator

C6.4▸A Our practice has a team member who has primary responsibility for the electronic systems and computer security.

You must have at least one team member who has primary responsibility for the electronic systems and computer security.

Create a policy: Network perimeter controls

Your network perimeter control policy should provide details of the hardware and software protecting your network, including remote and wireless access networks.

Your policy should cover:

- the configuration details of all network perimeter control hardware and software
- how network perimeter controls are managed
- version details of all hardware and software
- details of ongoing maintenance and support requirements
- configuration of your network perimeter controls and appropriate settings for your practice

- details of who can access your network through the perimeter controls and how this is done
- details on downloading or installing additional programs and utilities
- third-party and vendor access rights and confidentiality agreements
- the use of a VPN for all remote access
- information on avoiding the use of public or open and unsecured networks when accessing your practice systems remotely
- the importance of regularly scanning of your networks to identify security weaknesses
- how and when to audit logs for unauthorised access and unusual or inappropriate activity.

Protecting your WIFI network

Protecting your WIFI

If your practice has a WiFi network, or offers free WiFi for patients, have a policy for its use.

Ensure you have strong authentication and encryption standards and isolate your internal WiFi network from other networks to limit exposure if compromised. Make sure to set up a strong password to restrict access to the WiFi network so it is only accessible to authorised people.

☑ Tools to secure your network

- An **intrusion detection system (IDS)** monitors your network and system activity to detect malicious and unauthorised action. It does not prevent attacks on your system, but informs you if there is a potential problem so action can be taken.
- An **intrusion prevention system (IPS)** monitors and controls access to your IT network and takes action to block and prevent malicious and unauthorised action.
- **A demilitarised zone (DMZ)** acts as a neutral zone or protected space between your internal practice networks and external- facing connections such as the internet, web services and email. It prevents access to internal servers holding practice and patient data.
- **Secure remote access** provides a secure and reliable connection over the internet, most commonly using a VPN. A VPN uses encryption to prevent unauthorised reading of messages and authentication to ensure only authorised users have access to the system being connected to, and to ensure messages are not altered.
- **Content filtering** is the use of software programs to 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 also commonly used.
- **Firewalls** act as a gateway or barrier between a private network and an external or unsecured network (e.g. the internet). A firewall can be used to filter the flow of data through the gateway according to specific rules.
- It is recommended your practice information security lead works with your technical service provider to understand your practice's unique environment and ensure your network is correctly monitored.

Cloud computing

Cloud computing

Cloud computing refers to using a server located outside the practice. Typically, these off-site servers are operated by a provider in contract with the practice or its service company. This relieves the practice from having to own and maintain servers and data storage hardware, and from having to perform and check backups of its data.

Cloud-based services in general practice are more commonly used for data storage or for public services such as website hosting. As cloud-based technology has advanced, a number of clinical software vendors now offer cloud alternatives for general practices and there are new opportunities to move more business functionality into a cloud environment.

Cloud computing services can be an efficient way for practices to manage their IT, as they allow access to practice information from anywhere there is an internet connection.

Moving to cloud-based services can reduce the cost of managing and maintaining your local IT systems. Rather than purchasing expensive hardware for your business, it may be useful to do a cost analysis to see if you can use the resources of your cloud service provider. Doing so may reduce the costs associated with:

- organising and running system upgrades
- purchasing and maintaining new hardware and software
- hiring external IT staff
- energy consumption, because you no longer have to provide specific environmental conditions for servers and other hardware.

Cloud-based services can improve your practice's ability to communicate and may increase efficiencies through:

- the easy sharing of records with third parties
- the ability to access patient records outside of your practice during home visits or case conferences
- creating more flexible work practices through the ability to quickly and easily access data
- regular and automated updates or upgrades included in your contract
- improved backups and restoration that can be much simpler and timelier.

However, information security in a cloud-based environment requires additional considerations. When patient and practice data is surrendered to a third-party cloud service provider, you may need to consider the increased potential for data breaches, ownership rights to the data and ongoing data access.

☑ **If using cloud services, your risk assessment will also need to consider:**

- accessing cloud-based data in the event of an outage or service interruption to your internet connection
- technical issues with your cloud service provider such as hardware failures, faulty vendor software, lack of software and hardware version control
- scheduled or unplanned outages from the cloud service provider
- accessing data stored across multiple locations
- increased risk of attacks by malicious software for data stored offsite
- unauthorised access as data travels across networks
- physical security of offsite cloud storage facilities
- appropriate data governance concerning privacy and security
- access to data in the event of changing to another cloud service provider.

For more information on risks refer module on risk management

Hardware requirements

Hardware requirements

Hardware refers to the physical components that make up a computer network.

Hardware

Hardware requirements

Hardware refers to the physical components that make up a computer network.

Hardware

Hardware refers to the physical components that make up a computer network.

There are many different kinds of hardware device configurations, including:

- network equipment (i.e.. modems and routers)
- servers
- backup devices
- personal computers and laptops
- remote monitoring devices
- uninterruptible power supply (UPS)
- mobile electronic devices

Mobile electronic devices

Mobile electronic devices

Mobile electronic devices include laptops, tablets, USBs, removable hard drives, mobile phones, backup media and portable electronic clinical equipment.

Your practice should decide whether or not to use mobile devices for business and clinical purposes. Mobile devices used for business purposes may be owned by the practice, or personally owned by members of the practice team.

It is important to remember that mobile devices are at a high risk of being lost, stolen or left unsecured which increases the risk of a data breach.

Create a policy: Mobile electronic devices

Your policy should include guidance on which mobile electronic devices are authorised for use in your practice, and how these devices should be managed.

Your policy should cover:

- whether or not your practice allows the use of personal/private mobile electronic devices for work-related purposes
- information on using password protection on all mobile devices
- the protection of health data via encryption on all mobile devices
- how mobile devices are securely stored when not in use
- guidance on safely installing and using wireless network access
- who can have remote access to your practice systems, and how they have access
- third-party providers and access to practice systems via web-based portals
- processes and procedures for practice team members working from home to ensure information is protected
- security on your practice team's personal devices which are taken home and connected to your practice's network
- data encryption on mobile devices
- controls for bulk downloading or transfer of information using mobile devices.

Useful RACGP resource

- mHealth in general practice – A toolkit for effective and secure use of mobile technology (http://www.racgp.org.au/running-a-practice/technology/clinical-technology/mhealth-in-general-practice)

Protecting and maintaining your physical hardware

Protecting and maintaining your physical hardware

There are several ways to ensure your practice's physical hardware is maintained and protected.

Tips for protecting your physical hardware

- All computers should be kept reasonably dust free, especially over the intakes for the cooling fans.
- Be familiar with the operating temperature limits of your servers, as overheating is one of the major causes of server failure.
- Server room temperatures should be regularly monitored, and dedicated air conditioning installed if required. You should consider installing a thermometer in the server room.
- Take extra precautions over the summer months – run air-conditioning overnight on hot days or install ceiling suction fans.
- Always follow vendor guidelines, and seek professional advice from your technical service provider.
- Ensure your technical service provider assesses the **'computer heartbeat'**. This is a signal occurring at regular intervals to indicate a computer is working correctly, or synchronised with other parts of the system. If the heartbeat is not available, an error may have occurred.

Create a policy: Hardware maintenance

Your practice policy and procedures should include hardware and physical maintenance.

Your policy should confirm the requirement for:

- all system maintenance performed by your practice team or technical service provider to be documented
- regular hardware maintenance to be undertaken. This may include:
    - checking battery life on the UPS
    - preventive maintenance
    - planned upgrades
    - monitoring server room temperatures regularly

Create a policy: Physical protection

Your practice policy and procedures should include physical network and hardware protection.

Your policy should cover:

- how all removable computer equipment is secured from theft or damage
- the physical location of your server to ensure it is secured with limited and controlled access
- how the server is identified so practice team members know which computer is the server
- how software disks and backup media are physically protected
- how computer monitors are positioned in open-access areas to prevent unintentional viewing of information
- appropriate use of screensavers
- your clear screen policy
- your clear desk policy
- appropriate paper document management
- the secure disposal of hardware
- how to delete all data on devices
- How and when to perform a routine clean around the back of computers and other equipment
- Controlling environmental conditions (e.g. extreme heat)

Secure destruction and de-identification

Secure destruction and de-identification

Unnecessary health information should be destroyed securely to prevent unauthorised access. Prior to destruction, consideration needs to be given to the relevant retention requirements under any applicable health legislation (refer to Section on Retention and destruction of medical records).

Secure deletion occurs when the relevant records are no longer accessible through normal or forensic means. Ordinarily, deletion from a database does not totally erase a record, nor does it remove the record from the hard disk or other storage medium. Unless data is erased and overwritten multiple times, the data may remain on the storage medium and be accessible forensically.

Deleting individual patient records may not be possible due to practice software limitations. Where relevant, advice should be sought from software vendors or other professionals.

Useful RACGP resource

- More information on secure deletion of data can be found in the RACGP's resource Greening up: Environmental sustainability in general practice in your practice (https://www.racgp.org.au/running-a-practice/security/managing-practice-information/e-waste) .

Maintenance of your computer hardware, software and operating system

Maintenance of your computer hardware, software and operating system

Preventive strategies are required to keep your practice information security systems running properly. Undertaking regular and ongoing software and system maintenance can ensure computers and other equipment run smoothly and that your practice information is protected.

Computer systems need to be physically protected from theft and unauthorised access. The role of your technical service provider is not only to provide an emergency response when problems arise, but to also undertake regular and ongoing maintenance of your systems and provide advice on what physical protections are required.

☑ **Uninterruptible power supply (UPS)**

UPS is a device that provides power to enable computers (especially mission-critical hardware) to shut down normally and safely on an occasion when the main electricity is lost.

Put a sticker on your UPS with the date of the battery change as part of your maintenance program.

Data recovery and backup restoration

Data recovery and backup restoration

It can take longer than expected to restore data. It is important that you take this into consideration when creating a backup plan.

Frequent testing and validation of data readability will assist with a timely data recovery process. This also provides reassurance and peace of mind for your practice that its backup and recovery system is working efficiently.

Backup restoration is rebuilding a system or server after a software or hardware failure. Your backup restoration process needs to be documented, regularly tested and validated.

How do you know the backup has succeeded?

It is important to regularly test that your backup has worked and to test the integrity of your backup data once it has been restored. This ensures the backup has been successful and the restored data is accurate, correct, complete and preserved for future use.

You can ensure that your backup software performs these tests and restores to 100% accuracy by validating the restored data against what is held in the live system.

☑ Information recovery review

An information recovery review will help you to identify the reasons behind a system failure.

Your review should include how your information was recovered and what changes need to be made to your systems, processes and procedures to ensure the same type of system failure does not happen again.

Your information recovery review should include:

- details and screenshots of any error messages
- changes made prior to the system failing
- results of the system failure
- how the system failure was rectified
    - a fault log detailing
    - the date of the fault
    - who logged the fault
    - when the fault was discovered
    - how the fault was rectified
- a communications strategy to provide information and updates on the system failure and

recovery for practice team members, patients, other healthcare providers, technical support providers and relevant authorities who may have been affected.

Privacy and managing health information in general practice

Privacy and managing health information in general practice

General practice has a fundamental role in ensuring the privacy of patient health information. It is important that practices have up-to-date information on the current legislative framework for the management of health information.

Useful RACGP resources

- Privacy and managing health information in general practice (http://www.racgp.org.au/running-a-practice/security/protectingyour-practice-information/privacy)

Disclaimer

Disclaimer

The information set out in this publication is current at the date of first publication and is intended for use as a guide of a general nature only and may or may not be relevant to particular patients or circumstances. Nor is this publication exhaustive of the subject matter. Persons implementing any recommendations contained in this publication must exercise their own independent skill or judgement or seek appropriate professional advice relevant to their own particular circumstances when so doing. Compliance with any recommendations cannot of itself guarantee discharge of the duty of care owed to patients and others coming into contact with the health professional and the premises from which the health professional operates.

Whilst the text is directed to health professionals possessing appropriate qualifications and skills in ascertaining and discharging their professional (including legal) duties, it is not to be regarded as clinical advice and, in particular, is no substitute for a full examination and consideration of medical history in reaching a diagnosis and treatment based on accepted clinical practices.

Accordingly, The Royal Australian College of General Practitioners Ltd (RACGP) and its employees and agents shall have no liability (including without limitation liability by reason of negligence) to any users of the information contained in this

publication for any loss or damage (consequential or otherwise), cost or expense incurred or arising by reason of any person using or relying on the information contained in this publication and whether caused by reason of any error, negligent act, omission or misrepresentation in the information.

Recommended citation

The Royal Australian College of General Practitioners. Information security in general practice. East Melbourne, Vic: RACGP, 2022.

The Royal Australian College of General Practitioners Ltd 100 Wellington Parade

East Melbourne, Victoria 3002

Tel 03 8699 0414

Fax 03 8699 0400

www.racgp.org.au (https://www.racgp.org.au)

ABN: 34 000 223 807

ISBN: 978-0-86906-481-8 (web)

ISBN: 978-0-86906-533-4 (print)

Published February 2018; updated October 2022, September 2022

© The Royal Australian College of General Practitioners 2022

This resource is provided under licence by the RACGP. Full terms are available at www.racgp.org.au/usage/licence. In summary, you must not edit or adapt it or use it for any commercial purposes. You must acknowledge the RACGP as the owner.

We acknowledge the Traditional Custodians of the lands and seas on which we work and live, and pay our respects to Elders, past, present and future.

Practice resource

Practice resource

Download our practice poster

Effective **information security** in general practice is essential

As the digital healthcare landscape in Australia continues to evolve, so do the information and cyber security risks. Creating an informed, proactive cyber secure workplace culture requires continuous learning and is essential to the resilience and success of a practice and the provision of safe, high-quality healthcare.

Access the new RACGP *Information security in general practice* resource

RACGP
Royal Australian College of General Practitioners

Resources

Resources

Glossary

The Australian Governments *Australian Cyber Security Centre* (ACSC) has published comprehensive First Nations small business guide on cyber security – including case studies and videos.

Access the full guide here (https://www.cyber.gov.au/firstnationsresources)

First Nations resources

The Australian Governments *Australian Cyber Security Centre* (ACSC) has published comprehensive First Nations small business guide on cyber security – including case studies and videos.

Access the full guide here (https://www.cyber.gov.au/firstnationsresources)

Translated information

Find information in your language. The Australian Governments *Australian Cyber Security Centre* (ACSC) have developed easy-to-follow cyber security information and resources to support people from non-English speaking backgrounds to be more cyber secure.

Access the full guide here (https://www.cyber.gov.au/information/translated)

Self assessment quizzes

Find out if your cyber awareness knowledge is tracking. The Australian Governments *Australian Cyber Security Centre* (ACSC) have developed self assessment quizzes that may be useful – including information backup and multi-factor authentication.

Access the full guide here (https://www.cyber.gov.au/information/translated)