RACGP

Royal Australian College *of* General Practitioners

Information security in general practice

Prevention
Protection
Preservation

racgp.org.au

Healthy Profession.
Healthy Australia.

Information security in general practice

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, 2017.

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

ABN: 34 000 223 807
ISBN: 978-0-86906-481-8

Published February 2018

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.

Contents

Introduction

Information security is critical to the provision of safe, high-quality healthcare and the efficient running of a general practice. It is a fixed cost of doing business, and requires adequate allocation of financial and human resources to ensure business continuity and the protection of information assets.

Information security involves **prevention** of inappropriate access, **protection** of personal information and **preservation** of practice data.

The threat of cybercrime – inappropriate or unauthorised criminal access to practices' electronic data – is growing significantly. General practices frequently face new forms of malicious software and cleverly designed social engineering scams that can place your clinical and business data at risk. 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, like 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.

Patient or practice team data that is lost, stolen, inappropriately used or accessed can result in identity theft or privacy breaches that could ultimately place your practice at risk of incurring substantial fines or penalties.

About this resource

Information security in general practice reflects the changing technology environment and new security risks and threats. It does not impose new professional obligations but is designed to assist you to meet your legal obligations for information security and the requirements necessary for accreditation against The Royal Australian College of General Practitioners (RACGP) *Standards for general practices* (5th edition).

This resource details and recommends essential business practice, policies and procedures to help you protect your general practice information systems. It is not designed to be a technical document, but as an educational and training resource for you and your practice team.

Each section of this resource:

- refers you to the relevant indicator under Criterion C 6.4 – Information security from the RACGP *Standards for general practices* (5th edition), available at www.racgp.org.au/your-practice/standards/standards-for-general-practices-(5th-edition)
- provides specific policy content information.

Relevant indicator

Where there is a 'must have' in the *Standards for general practices* (5th edition), we direct you to the relevant indicator for each section.

Recommendations are provided to assist general practices to meet the required accreditation standards.

Practice information security policies

Polices should be created to support information security processes in your general practice.

To be effective, your policies should be:

- publicised and provided to all existing and new members of your practice team
- easily accessible (eg kept in policy manuals or available on your intranet)
- explained to team members through information and training sessions, at team meetings and during induction
- reiterated and discussed regularly to maintain relevance
- periodically reviewed to ensure they are current, and updated when changes are made in information security processes in your practice or to relevant legislation
- re-issued to the practice team when updated.

Policies should include:

- a purpose and objectives
- scope (ie 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 sample to create your practice policies, available at www.racgp.org.au/your-practice/ehealth/protecting-information/information-security

Practice team education

This resource recommends you provide access to education and training for your practice team to support information security in your general practice. You should keep a record of when team members have undertaken training. Education can include:

- induction training
- discussion at practice team meetings
- formal ongoing training when changes are made in the practice or to legislative requirements
- practice exercises to test processes (eg 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 practised).

Overview for practice owners and managers

Information security in general practice describes the fundamentals of implementing information security controls into your general practice. As a practice owner or manager you need to ensure these processes are in place to safeguard your practice systems, and appoint a member of your practice team to be accountable and responsible for monitoring information security controls across your practice.

Introduce information security 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 and your practice team members need to be aware of their responsibilities to protect practice information. Information security processes should be documented and followed.

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

- 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*
- 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 (eg providing health information to external organisations for research or population health planning [secondary use of data])
- how you know the system and process are working as intended.

You can read more about this in 1.1 Roles and responsibilities of your practice team.

Protect your WiFi network

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 if using an internal WiFi network and isolate it from other networks to limit exposure if compromised. Set up a strong password to restrict access to the WiFi network so it is only accessible to authorised people.

You can read more about this in 3.1 Network perimeter controls.

Allocate resources

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 business. Having an information security professional review can help identify security gaps and save costs in the long term.

Create a culture of information security

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.

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.

You can read more about this in 1.1 Roles and responsibilities of your practice team.

Manage access to your systems and your data

Reduce security risks in your practice by introducing access controls. Practice team members only need access to the minimum data required to do their work. This limits the risk of data breaches and protects your practice data. Establish a strong and unique password policy to make sure access to systems is controlled and secure. Access management ensures accountability and allows you to ascertain who has entered or altered data.

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.

You can read more about this in 1.3 Managing access to your information systems and data.

Measure the effectiveness of your security controls

The effectiveness of any information security control procedures you have in place in your practice needs to be measurable. This allows 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.

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?

Use the 'List of information security considerations' on page 8 to assist with monitoring and measuring your controls.

Perform a risk assessment

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.

It is important to analyse and understand the security risks and threats to business and clinical information in your practice. Identify gaps in security and implement strategies to lessen any potential risks.

You can read more about this in 2.1 Risk assessment.

Have a business continuity plan with information recovery procedures

Your general practice needs a documented business continuity plan which includes information 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. This plan should detail how to maintain critical business functions when there is an unexpected system event. The plan should be reviewed, updated and tested periodically.

You can read more about this in 2.2 Business continuity and information recovery.

Have a resilient backup and restoration process for practice data

Critical data in the practice should be regularly backed up and validated. The backup procedure needs to be documented and routinely tested to ensure the backup system functions correctly and data can be quickly restored if an incident such as a server failure occurs. A robust backup process enables you to restore your business functionality in the shortest time possible. Ensure your backup media is secure from unauthorised access and copies are held at an alternative location in case of theft or a natural disaster at the primary location. Backup and restoration may not apply if your practice data is stored in the cloud and provided as Software as a Service (SaaS). In this case, it becomes an obligation of your cloud service provider and should be included as part of your contractual agreement.

You can read more about this in 2.3 Information backup.

Educate and train your practice team

Your practice team needs to know and understand that security breaches can and will happen. You need to educate your practice team about the importance of data protection and how to recognise signs of a security breach. You should have a process for your practice team to access training so they approach their jobs with a security focus. Share information on security breaches, no matter how small, when they happen. Show your practice team why they need to be careful.

You can read more about this in 1.1 Roles and responsibilities of your practice team and in 4.2 Malicious software.

Regularly update software and systems

Ensure your software is current and supported by your software provider. All of your practice software, including web browsers and operating systems, should have the latest security updates installed. Ideally, operating system and application security updates should be deployed automatically and be scheduled to update at a time that suits your practice. These updates are key in your defence against malicious software and other online threats.

You can read more about this in 4.2 Malicious software.

Keep mobile devices secure

Have a policy on the use of mobile electronic devices for both business and clinical purposes. Mobile electronic devices can contain confidential business information or easily access information via your local network. If you allow the use of mobile devices, these should be password protected, have data encrypted where possible, and have appropriate security applications or software installed. When using public and potentially unsecured networks on such devices, do not send or access sensitive data in case your communication is intercepted.

You can read more about this in 3.3 Mobile electronic devices.

Information security considerations

This list is a guide to help you assess, achieve and maintain effective information security controls in your practice.

1 Setting up your information security governance framework		
	Security consideration	**Explanatory notes and recommendations**
1.1 Roles and responsibilities of your practice team	Does your practice have designated practice team members for championing and managing information security? Do these team members have their roles and responsibilities documented in their position descriptions? Does your practice have training scheduled for these roles and responsibilities?	Your practice should have a documented policy outlining the specific roles and responsibilities of all team members. Practice team members should receive regular training on all of the practice policies and procedures to ensure they understand their roles in maintaining information security.
1.2 Policies and procedures for managing information security	Does your practice have documented policies and procedures for managing information security?	Your practice should have a policy and procedure manual outlining the security requirements for your practice. These policies and procedures should be clear and contain simple instructions.
1.3 Managing access to your information systems and data	Does your practice have well-established and monitored authorised access to health information?	Your practice should have a policy containing information on access rights, unique password maintenance, password management, remote access controls, and auditing and appropriate software configuration.

2 Assessing the risks and keeping your practice running		
	Security consideration	**Explanatory notes and recommendations**
2.1 Risk assessment	Does your practice have a structured risk assessment of information security and identified improvements as required?	Your practice should have a policy detailing vulnerability management, risk assessment and security breach reporting procedures. This will include recording assets in the practice, a threat analysis and a reporting schedule.
2.2 Business continuity and information recovery	Does your practice have documented and tested plans for business continuity and information recovery?	Your practice should have a documented business continuity plan to ensure the practice can continue to operate when a practice information systems failure occurs. This includes an information disaster recovery plan to restore data so the practice information systems can be brought back to working order as quickly as possible. The practice team should be aware of their roles in relation to business continuity and disaster recovery and receive training as required.
2.3 Information backup	Does your practice have a reliable information backup system to support timely access to business and clinical information?	Your practice should have documented procedures for the backup of your practice systems. This should include: • how often backups are run • the type of backup, media type and rotation • the use of encryption • reliability testing and restoration checking • where the backups are stored • who has access to the backups • access to data from previous practice information systems.

3 Securing the network and your equipment

	Security consideration	Explanatory notes and recommendations
3.1 Network perimeter controls	Does your practice have reliable network perimeter controls?	Your practice should have documented information on the systems protecting your practice network and any remote or WiFi networks. This should include firewall and intrusion detection and prevention hardware and software, and content filtering software with configuration and settings appropriate for your practice security needs.
3.2 Maintenance of your computer hardware, software and operating system	Does your practice manage and maintain the physical facilities and computer hardware, software and operating system with a view to protecting information security?	Your practice should have documented information on how team members can prevent the unauthorised viewing of confidential information such as using lock screensavers. Your practice should document how access is managed to restricted areas such as server rooms and how equipment can be secured from theft or damage. Your practice needs to document how hardware is disposed of safely and how software and hardware is maintained.
3.3 Mobile electronic devices	Does your practice have processes in place to ensure the safe and proper use of mobile electronic devices?	Your practice should have a documented policy on the use of mobile devices, including using wireless networks and remote access to your practice systems. The practice team should be made of aware of what devices can be used in the practice and how to use their personal mobile devices in line with practice policies.

4 Online safety

	Security consideration	Explanatory notes and recommendations
4.1 Internet and email use	Does your practice have a process in place to ensure the safe and proper use of internet and email?	Your practice should have a policy clearly defining and describing how the practice team use email and the internet for business purposes. This may include access to social media and what is considered acceptable personal use of email and the internet by the practice team.
4.2 Malicious software	Does your practice have reliable protection against malicious software?	Your practice should document the installation and monitoring of protection against malicious software.
4.3 Electronic sharing of information	Does your practice have reliable systems for the secure electronic sharing of confidential information?	Your practice should document how information is sent outside of the practice using secure electronic communication. This will include the appropriate configuration of secure electronic messaging, digital certificate management and your practice website.
4.4 Third party software security	Does your practice know how third-party software is using your practice data?	Your practice should have a policy around the use of any third-party software that is installed, and how it meets your security requirements. Third-party software regularly uses practice data to perform its function, but can also open up your practice to security threats. Ensure that you can demonstrate an understanding of how it is using your practice data and that consent has been obtained for any secondary use of data.

Information security for cloud computing

Cloud computing involves storing and accessing data and programs over the internet instead of locally from a computer or server. Most general practices currently run their IT environment from a physical server located at the practice. 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 your general practice to manage your IT, providing access to your practice information security systems 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, you use the resources of your cloud service provider, reducing the costs associated with:

- system upgrades
- new hardware and software
- 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
- 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 more timely.

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.

1

Setting up your information security governance

1.1 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.

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

Relevant 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 practice team members.

Your policy should cover:

- specific information on the roles and responsibilities of each practice team member in relation to information security, to determine 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.

The position description of the information security lead can include responsibilities such as:

- 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

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.

Case study
Creating a security culture

Mandy, a practice manager at a general practice in southeast Melbourne, was recently alerted to a malicious software cyber-attack that had a detrimental effect on several general practices' computers.

The practices' electronic systems were rendered completely unavailable, preventing access to all electronic patient and business-critical information. To ensure her practice was not subject to the cyber-attack, which was predicted to spread rapidly across Australia, Mandy immediately organised a meeting to inform and update her practice team on this latest cyber-attack.

The team 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 also disconnected any WiFi access and reduced the chances of the cyber-attack spreading across the entire general practice network.

Useful RACGP resources

- *Confidentiality agreement template*, available at www.racgp.org.au/your-practice/ehealth/protecting-information/information-security
- *Internet and email use template*, available at www.racgp.org.au/your-practice/ehealth/protecting-information/information-security
- More information on cloud services, available at www.racgp.org.au/digital-business-kit/cloud-computing

1.2 Policies and procedures for managing information security

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.

Create a policy

Your policy should reflect the overall strategy of how practice information is secured. Policies can be kept as a manual, folder or suite of documents accessible to your practice team. The practice team should have access to training on all policies and procedures to ensure compliance and implementation.

Relevant 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*, available at www.racgp.org.au/your-practice/ehealth/protecting-information/privacy
- *Guide for the use of social media in general practice*, available at www.racgp.org.au/your-practice/ehealth/social-media/guide
- Resources on using email in general practice, available at www.racgp.org.au/your-practice/ehealth/protecting-information/email

1.3 Managing access to your information systems and data

Each practice team member should only have access to the necessary systems and information to enable them to perform their role in the practice. Your practice needs to establish and monitor authorised access to health information. Your practice team should have access to appropriate training in the relevant software and on potential risks before access and passwords are provided.

Passwords are the most common form of access authentication. Password management can be complex as users often have multiple passwords to access various systems. Your practice team needs to be aware that most software will allow new passwords to be generated if they are forgotten, so it causes an unnecessary risk to your information security to keep a written record of passwords.

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.

Relevant 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 a privacy policy, and the security of the clinical software passwords of each individual practice team member.

Create a policy

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
- 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)
- each practice team member creating their own password and being responsible for keeping these 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.

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 be changed on first login to the system
- a minimum password length (ie number of characters)
- a mixture of alphabetic (lower and upper case) and numeric characters, and symbols
- passwords do not use familiar and family names or words that can be found in a dictionary
- passwords should be set to expire to enforce periodic changes
- dates of birth are not used
- passwords are not reused
- two-factor authentication method (a combination of two types of authentication) if appropriate for your practice
- how automatic password saving is addressed in browsers and if this is disabled across the practice network.

Useful RACGP resource

- *Privacy policy template*, available at www.racgp.org.au/your-practice/ehealth/protecting-information/privacy

2

Assessing the risks and keeping your practice running

2.1 Risk assessment

You should complete a periodic risk assessment to assess the security of your practice's clinical and business information systems. Documenting your risk assessment provides evidence of a systematic approach to information security. A structured risk assessment requires you to record the assets in your practice. An asset register documents the hardware, software and other information systems used.

A threat analysis should also be included as part of your risk assessment to assess the impact from potential threats to your systems. Ensure plans are in place to minimise threats and vulnerabilities, which includes financial loss, breaches in confidentiality, information integrity and availability, and patient confidence. Risk assessments can be complex and your practice may find it valuable to employ a technical service provider or specialist security firm to undertake your practice risk assessment.

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.

Relevant indicator

Criterion 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.

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.

Threats may 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

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

- errors and omissions (eg accidental file deletion, inability to restore data from backups)
- unintentional access to information systems by practice staff
- unintentional viewing of information systems by 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
- unauthorised system or network access
- software/hardware failure
- power disruptions
- natural disasters eg flood, earthquake, fire, storm/cyclone
- physical protection of data that is stored offsite (eg data storage devices such as hard disks.)

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 cloud services refer to page 10.

Your practice asset register 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 licence 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

Data breach response and recording

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 notified. 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
- 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.

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.

2.2 Business continuity and information recovery

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 focus on internal system malfunction or failure. It is 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 tested and updated when there is a technology or procedure change in the practice or when any change to legislative requirements occurs. It is recommended you consult a technical service provider for advice on creating your plan.

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.

Relevant 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.

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
- transferring 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 (eg payroll, Medicare claims)
  - payroll processing
  - financial reconciliations.

If you are using cloud-based services you will need to consider creating a cloud services plan which 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 review

An information recovery review will help you identify the reasons for 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.

What to include in your information recovery review:

- Details and screen shots of any error messages
- Changes prior to the system failing
- Result 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 advise practice team members, patients, other healthcare providers, technical support providers and relevant authorities who may have been affected.

2.3 Information backup

Your practice should have reliable information backup systems to support timely access to business and clinical information. The creation of a backup process can require assistance from a technical service provider.

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

Relevant indicator

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

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

Your policy should cover:

- your complete backup procedure
- how your backups are encrypted
- where copies of your business-critical data are stored
- how your practice data is backed up
- how your backup data is restored
- how long it takes to restore your backup data
- how you ensure your backups are completed and correct
- 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
- details of which practice team members perform the backup
- details of any automated backup processes
- testing data restoration regularly.

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

Defence in depth is a strategy where multiple security controls are layered throughout an IT system to reduce the risk of a network attack.

Retention and destruction of records

- General practices should keep health records for the length of time specified in state or territory legislation.
- Once this time has expired, the Australian Privacy Principles (APPs) require you to take reasonable steps to destroy or permanently de-identify health information.
- APP 11 requires that reasonable steps are taken to destroy or de-identify personal information that is no longer needed. The reasonable steps will be dependent on whether the personal information is held in a paper or electronic format.

About backups

All practice management and clinical systems data as well as 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.

Backup media

Choose a backup media option appropriate for your practice. Common backup media include portable hard drives, USBs, transfer of data to another computer or hard drive, or data backup to the cloud. You can use different types of backup media to provide you with multiple options for restoring data.

Backup storage

The physical protection of backup media is important. This 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.

Backup reliability

It is vital 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.

Backup restoration

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.

Case study
3-2-1 backup strategy

A busy healthcare centre just outside of the Brisbane CBD uses the '3-2-1 backup strategy' to protect their practice data. The practice has approximately 20 GPs and provides a range of general practice and allied health services. GPs and healthcare providers in the practice use electronic health records as part of their consultations to record patient information, generate prescriptions, request pathology and diagnostic imaging and to create referrals to other healthcare providers. All of the practice's billing and administration is computer-based and each day a large volume of electronic data is collected.

To protect this data and ensure it is available, the practice has a 3-2-1 backup strategy. The practice keeps three copies of their data: the original and two backup copies. Each of the backup copies are stored on different storage media and one copy of the data is stored offsite. Having multiple copies of the practice's data means there is less risk of losing data in the event of a disaster.

The practice data is backed up locally onsite to a separate server. The second copy is backed up to the cloud at an offsite location. If there is a local disaster that damages data held at the practice, the cloud data is still available to maintain business continuity. The practice's IT lead and external technical service providers are aware there is no 'perfect' backup system, but also know that using the 3-2-1 strategy is a great starting point to keep most businesses up and running.

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.

Choose the time for a controlled shutdown process wisely, as it can often take up more time than you may have anticipated. Ideally, the downtime should be as short as possible. The process and procedure for a controlled shutdown should be fully documented.

Test your backups

It is important to regularly test the integrity of your backup data. This ensures the backup has been successful and the data is accurate, correct, complete and preserved for future use. You can check your backups by validating the data against what is in your live system. This can be done automatically by your software or manually by your practice team.

Useful RACGP resource

- *Guide to information backup in general practice*, available at www.racgp.org.au/your-practice/ehealth/protecting-information/guide-to-information-backup-in-general-practice
- *Effective solutions for e-waste in your practice*, available at www.racgp.org.au/your-practice/ehealth/protecting-information/e-waste
- *Privacy and managing health information in general practice*, available at www.racgp.org.au/your-practice/ehealth/protecting-information/privacy

Other resources

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

3

Securing the network and your equipment

3.1 Network perimeter controls

Network perimeter controls are essential for anyone using the internet. Your practice should have reliable network perimeter controls in place to protect your practice systems and local network. Use 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.

Remote access to your practice information systems via a wireless network is convenient but requires additional security measures. WiFi devices should have encryption set up to ensure information confidentiality. Follow vendor guidelines and speak to your technical service provider about secure WiFi configuration for your practice.

Create a policy

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

Relevant 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.

Network perimeter controls protect your practice systems and local network by controlling data entering and leaving your local network.

Your policy should cover:

- the configuration details of 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
- regular scanning of your networks to identify security weaknesses
- reviewing audit logs for unauthorised access and unusual or inappropriate activity.

3.2 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 information is protected. Computer systems need to be physically protected from theft and unauthorised access.

The role of your technical service provider is not just to provide an emergency response when problems arise. They should undertake regular and ongoing maintenance of your systems and provide advice on what physical protections are required.

Uninterruptible power supply (UPS) is a device that provides power to enable computers (especially mission-critical hardware) to shut down normally 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.

Create a policy

Your practice policy and procedures should include system and software maintenance as well as physical network and hardware protection.

Your policy should cover:

Software and hardware maintenance

- All system maintenance performed by your practice team or technical service provider should be documented
- Regular system maintenance can include
  - upgrades to clinical desktop system software
  - preventive maintenance
  - planned upgrades
  - maintaining and updating testing environments
  - monitoring for intrusions and installations of unauthorised programs
  - checking disk capacity (hard disk space)
  - checking system and error logs
  - ensuring antivirus and other protective software is up to date
  - checking battery life on the UPS
  - running patching updates to rectify security weaknesses in earlier software versions
  - software version control to maintain software in accordance with the vendor's guidelines.

Physical protection

- 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 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
- Paper document management
- The secure disposal of hardware
- How to delete all data on devices
- How the server is identified so practice team members know which computer is the server
- Routine cleaning around the back of computers and other equipment
- Controlling environmental conditions (eg extreme heat)
- How to limit damage from power interruptions and/or fluctuations

Clear screen policy

- Remember to exit the previous patient's electronic file before the next patient enters the consulting room.
- Position computer monitors to keep information private, including computers used by reception staff at the front desk.
- Use 'clear screen' function keys, which instantly close down an open file or switch off the monitor.
- Use password protected screensavers.
- Log off when leaving computers unattended or use automatic session time-outs.

Clear desk policy

- At the end of each day, each practice team member clears their desks of all documents, notes and media.
- All documents should be removed from printers and fax machines immediately after being copied, sent or received.

Tools to secure your network

- An 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 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 (eg 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 environment to ensure your network is correctly monitored.

Tips for protecting your physical hardware

- All computers should be kept reasonably dust free, particularly over 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.

You may have heard your technical service provider mention a '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.

Useful RACGP resource

- *Effective solutions for e-waste in your practice*, available at www.racgp.org.au/your-practice/ehealth/protecting-information/e-waste

3.3 Mobile electronic devices

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. Mobile devices include laptops, tablets, USBs, removable hard drives, mobile phones, backup media and portable electronic clinical equipment. These devices are at a high risk of being lost, stolen or left unsecured which increases the risk of a data breach.

Vulnerability assessment and penetration testing

Vulnerability assessment and penetration testing (VAPT) are ways to test the security of your 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 normal IT and network security management, when new infrastructure or applications are added to the network, when user policies are changed and when there are significant system upgrades.

Relevant 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 a privacy policy, and the security of the clinical software passwords of each individual practice team member.

Create a policy

Your policy should include which devices are authorised for use in your practice and how these devices are managed. Your policy should direct your practice team on the use of privately owned mobile devices for business purposes.

Your policy should cover:

- whether or not your practice allows the use of personal mobile electronic devices for work-related purposes
- the password protection of 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 resources

- *mHealth in general practice – A toolkit for effective and secure use of mobile technology*, available at www.racgp.org.au/your-practice/ehealth/additional-resources/mhealth-in-general-practice
- *Implementation guidelines for video consultations in general practice* (3rd edition), available at www.racgp.org.au/your-practice/guidelines/implementation

4

Online safety

4.1 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.

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

Relevant 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 privacy policy, social media policy and email policy.

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
- appropriate personal use of the internet on business devices during business hours
- 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 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 to an email (especially by return email) no matter how credible the sender's email seems (eg apparent emails from your bank).
- Use a spam filtering program.

What is spyware and how do you protect your practice against it?

Spyware is programs downloaded from the internet onto your computer (sometimes without your knowledge) to covertly send information back to the sender.

- Learn how to recognise spyware.
- Know how to safely delete or remove spyware.
- Do not accept certificates or downloads from unknown senders.

Useful RACGP resources

- *Using email in general practice – guiding principles*, available at www.racgp.org.au/download/Documents/e-health/using-email-in-general-practice-%E2%80%93-guiding-principles.pdf
- Internet and email use template, available at www.racgp.org.au/your-practice/ehealth/protecting-information/information-security
- *Using email in general practice* – Privacy and security matrix, available at www.racgp.org.au/download/Documents/e-health/using-email-in-general-practice-privacy-and-security-matrix.pdf
- *Guide for the use of social media in general practice*, available at www.racgp.org.au/your-practice/ehealth/social-media/guide

4.2 Malicious software

Your practice should have reliable protection against malicious software including viruses, worms and trojans. These intentionally seek to corrupt, destroy or steal data, or use your computer for unauthorised purposes.

Malicious software is generally introduced into a system through external electronic communication via email or the internet. It can also arrive in your computer via image and video files, CDs/DVDs, USBs and other portable devices and media.

Create a policy
Your policy should cover monitoring procedures to detect malicious software and advice on what to do if malicious software is detected.

Relevant 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.

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 occurs
- 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.

4.3 Electronic sharing of information

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.

Create a policy

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

Relevant 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 a privacy policy, and the security of the clinical software passwords of each individual practice team member.

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 other confidential information between healthcare providers and patients
- 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.

Digital certificates

- Digital certificates for electronic communication software (the original disk and serial numbers) should be stored securely.
- Documentation on where certificates are installed should be maintained, and the expiry of each recorded.
- Some software automatically renews your Public Key Infrastructure (PKI) certificate. Other software will require manual reinstalling, so make sure you know how to keep these current.

Risks of running unsupported software or hardware:

- **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 and fines.
- **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.

4.4 Third-party software security

Third-party software, including 'add-on' or 'bolt-on' programs, is regularly used in general practice to enhance practice and clinical systems and to transfer clinical information. This includes electronic prescription exchange and secure communications. For example, data extraction tools, administrative products, and online medical appointment scheduling applications are used to analyse and improve business and clinical performance. However, using third-party software can also expose your general practice system to threats including the potential to compromise core database integrity, open up security weaknesses that allow unauthorised access into your practice system, and data breaches.

Security measures need to be taken into account when choosing to use any type of third-party software in your practice. Consider:

- 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?

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.

Useful RACGP resources

- *Using email in general practice – Guiding principles*, available at www.racgp.org.au/download/Documents/e-health/using-email-in-general-practice-%E2%80%93-guiding-principles.pdf
- *Using email in general practice – Privacy and security matrix*, available at www.racgp.org.au/download/Documents/e-health/using-email-in-general-practice-privacy-and-security-matrix.pdf
- *Guide for the use of social media in general practice*, available at www.racgp.org.au/your-practice/ehealth/social-media/guide
- *Digital Business Kit – Social media*, available at www.racgp.org.au/digital-business-kit/social-media
- *Secondary use of general practice data*, available at www.racgp.org.au/download/Documents/e-health/Secondary-use-of-general-practice-data.pdf