Information Security Guide
for small healthcare businesses

Protect Your Healthcare Business

Australian Government
Australian Digital Health Agency

STAY SMART ONLINE

Information Security Guide
for small healthcare businesses

Your healthcare business or practice has access to valuable digital information entrusted to you by healthcare consumers, suppliers and employees. The information and systems your business uses to access and store this information are critical to its ability to operate.

If criminals compromise your computer systems or steal important business information, your business may suffer significant financial loss, possible legal liability, reputational damage and your customers' personal information may be misused for fraudulent purposes. Some cyber attacks may cause you to lose access to critical business systems or Internet bandwidth making it difficult to run your business.

This guide has been developed by the Australian Digital Health Agency (the Agency) and the Australian Government's Stay Smart Online service. The Agency promotes the use of safe and secure digital health services and systems to improve health outcomes. The Stay Smart Online service provides advice to help people and small businesses protect their personal and financial information when using computers and other internet connected devices.

Australian Government
Australian Digital Health Agency

STAY SMART ONLINE

Data breaches in Australia resulted in average costs of **$108 per capita**, with direct costs of $47 for forensic and legal advice and $68 in indirect costs for investigating and notifying relevant parties.[1]

Only a third of Australian Healthcare organisations **embed cyber security awareness and training** into their organisational policies and procedures.[2]

58%

of healthcare breach victims report being breached due to a vulnerability for which a patch was available.[3]

Sources:

1 Ponemon Institute 2018 Cost of a data breach study. Available from: https://www.ibm.com/account/reg/us-en/signup?formid=urx-33316

2 Cyber Security Across the Australian Healthcare Sector 2018. Available from: https://www.hisa.org.au/wp-content/uploads/2018/07/HISA-Healthcare-Cybersecurity-Report_June-2018.pdf

3 Ponemon. The state of vulnerability response in healthcare. Available from: https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ar-ponemon-healthcare-report.pdf.

Information security – it's your business

A balanced diet, regular exercise and good hygiene practices, such as brushing teeth and washing hands, contribute to good health. Similarly, by adopting good information security practices as part of your business' day-to-day activities you can protect individual health information and important business computers and devices.

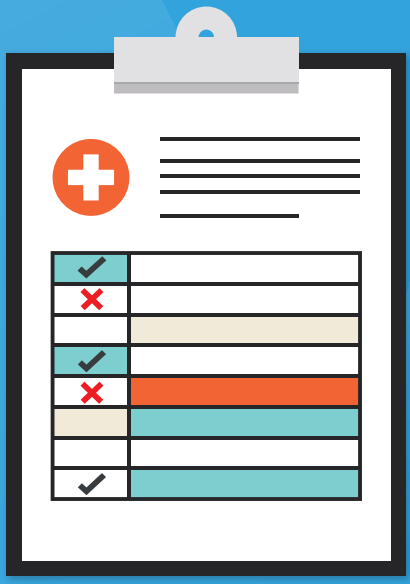
Your business is your business – you are responsible for its success. As a health service provider, your business has an obligation to protect the security and privacy of individual health information.

This short guide was developed to help your business put in place some basic information security practices. It only takes a few minutes to read through these five easy steps, which will provide you with the basics on how to protect the information entrusted to you.

You may also want to consult the other cyber security guidance materials available at www.digitalhealth.gov.au (search for security guidance).

Privacy

Keep your friends close and
your information closer



Privacy

In Australia, all health service providers are required by law to protect the security and privacy of individual health information. The applicable privacy legislation for public and private entities may vary depending on jurisdiction. The Commonwealth's *Privacy Act 1988* (Privacy Act) applies to Australian government entities and all health service providers in the private sector, regardless of size.

The Privacy Act requires that health service providers take "reasonable steps to protect the information from misuse, interference and loss, as well as unauthorised access, modification or disclosure" (APP 11.1). In the event that individual health information is compromised, health service providers may need to prepare a data breach response plan and manage the breach notification process, which is mandatory under the Privacy Act.

Action:

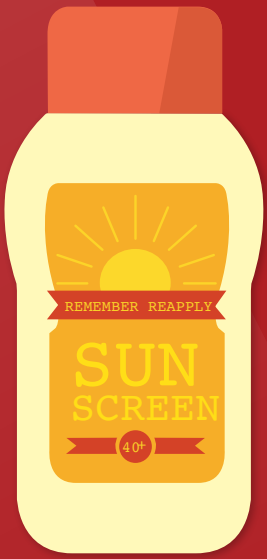
- ✓ Consult the Office of the Australian Information Commissioner's (OAIC) guidelines to understand what steps are 'reasonable' for your business to undertake to secure individual health information.

More information about privacy is available here:

- State and territory health privacy: **www.oaic.gov.au/privacy-law/other-privacy-jurisdictions#state-and-territory-health-privacy**
- Search for: 'Steps and strategies which may be reasonable to take' on the OAIC website: **www.oaic.gov.au**
- Notifiable Data Breaches Scheme - understand your responsibilities: **www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme**

Passphrases

Sunscreen protects your skin:
Passphrases protect your information



Passphrases

Passphrases help protect your information from exposure and consequent loss or damage. Passphrases are a series of words that are longer, easier to remember, and harder to guess than traditional passwords.

A passphrase is one of many mechanisms that together help prevent unauthorised access to information and systems. Cyber criminals use a range of methods to compromise passphrases. It is particularly important that passphrases for systems that contain patient records are protected. It is therefore vital that passphrases are long with at least 12 characters. Include upper and lowercase letters, numbers and symbols for extra strength.

With so many online systems for your personal and business use, it is very hard to remember a strong and unique passphrase for each of your accounts. By using a password manager, your staff only need to remember two strong passphrases – one for their computer where the password manager is installed and one to access their password manager. All other passphrases are stored securely within the password manager. The downside is that if the password manager is breached, all your passwords could be accessed.

Two factor authentication can protect against phishing and other passphrase attacks. Instead of just entering a username and password, two factor authentication typically requires the user to provide a secret only the user knows (like a passphrase or PIN) and something they have in their possession (like a one-time code sent to their mobile phone; an EFTPOS card; or a digital certificate installed on their computer or on a portable secure USB token).

Actions:

- ✓ Ensure that all staff members use their own strong, unique usernames and passphrases.
- ✓ Where possible, use two-factor authentication for additional protection.

Network and device security

Lock down your computers (and networks)!

Network and device security

Washing hands and brushing teeth are basic hygiene practices that can make a big difference to our health. Like viruses and bacteria that seek to attack our bodies, cyber criminals attempt to attack network and information systems. Any network connected to the internet is potentially within reach of criminals from anywhere in the world. By adopting basic, effective information security practices, your business will be more resistant to attack.

Software is complex and prone to coding errors. These errors (or security bugs) create holes, through which cyber criminals can potentially access business computer systems connected to the internet. By keeping software 'up-to-date' or 'patched', you fix these bugs and can prevent common attacks compromising your systems.

Cyber criminals also compromise computers and devices using malicious software (malware), which can be delivered by email or while browsing the web. Some malware is delivered through advertisements on the web.

Treat any network that your business does not control as insecure, particularly public or guest Wi-Fi networks that do not require a password. With the right tools, anyone connected to the same public Wi-Fi network as you, can see unencrypted information you send and receive. Potentially they may also be able to log on as you, even if they don't know your username and password.

Actions:

- ✓ Ensure all operating systems and application software on business computers update automatically where possible.
- ✓ Install anti-virus software and an ad-blocking browser plugin on staff computers to help prevent malware compromising business computers.
- ✓ If you need to use public Wi-Fi, at the very least, make sure it requires password access.

Backups

Prepare for an emergency!

Backups

The blood service keeps a supply of blood products for emergency medical use. Like the blood service, you never know when you will need your backups.

Cyber criminals use malicious software (malware) to deny access to business computers and files, and demand a ransom to regain access. In most cases, the only reliable way to remove malware and recover from such an attack is to wipe the computer and re-install the operating systems, applications and data from backups. If you have a backup of your critical business systems and files, then your business is in a strong position to recover from such an incident.

In the event of a cyber attack, hard disk failure or other disastrous event, what would happen if you could not access your consumer health records, financial information or other critical systems? If the information on these systems was lost forever, how would that affect your business? Without backups, businesses risk losing their important information and may never recover.

In the event of an incident that affected the confidentiality or integrity of individual health information, do you know what your legal obligations are?

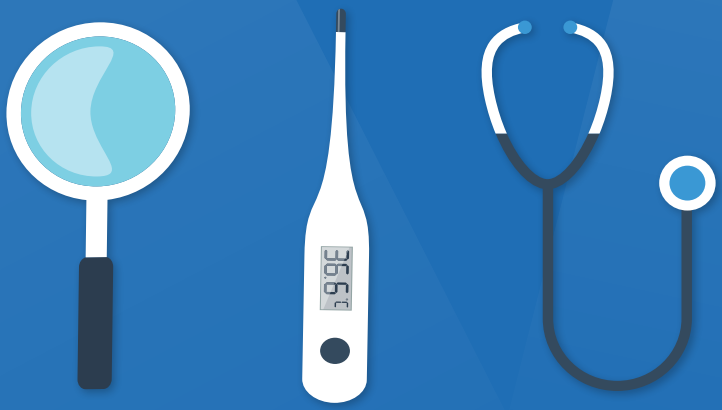
Actions:

- ✓ Be aware of your obligations to report breaches of individual information and have a plan for accessing technical and legal advice.
- ✓ Keep frequent backups of all critical information and systems, ensuring that backups are stored securely off site and not connected to the network to prevent their loss due to fire, theft or malware.

More information about backing up your data is available on the Stay Smart Online website: **www.staysmartonline.gov.au**

Awareness

All eyes open to stay secure



Awareness

Health professionals need to stay abreast of the latest health risks. Similarly, by keeping abreast of the latest information security risks, you will be able to apply that knowledge to protect your business.

Staff who are security aware are more likely to identify fraudulent requests to provide sensitive information such as personal information, passphrases and banking details; and less likely to open email attachments or click on web links which could infect business computers with malware.

Promote a 'stop and think before you click' message among staff to help raise awareness of online security risks. For example, think before you click on a link in a suspicious email or connect to a public Wi-Fi network. Don't assume that technology will protect you. Just because you can do something, doesn't mean you should.

Being security aware also means knowing when to seek professional advice and what questions to ask. An IT security consultant can review existing security measures and help address security gaps. If you are already using an IT service provider, make sure you have a clear understanding of the services and security measures being provided, so you can decide whether they meet your needs.

Actions:

Subscribe to alerts published by:

- ✓ Stay Smart Online: **www.staysmartonline.gov.au/alert-service**
- ✓ Scamwatch: **www.scamwatch.gov.au/news**
- ✓ Vendors for the software and devices your business uses.

For more information, read the 'Security Awareness Implementation Guide' available on the Stay Smart Online website: **www.staysmartonline.gov.au** and consult guidance materials on the **www.digitalhealth.gov.au** website.

Common online threats

Adware

Software that is covertly installed on your computer and designed to deliver advertisements or other content which encourages you to purchase goods or services.

Spyware

Software that is covertly installed on a computing device and takes information from it without your consent or the knowledge of the user.

Virus

Malware designed to infect and corrupt a computer and to copy itself. Viruses can disrupt programs installed on a computer.

Scam

A commonly used term to describe a confidence trick, relying on email or a website to obtain sensitive information or deliver malicious content (such as malware) to unsuspecting users.

Malicious software (malware)

A catch-all term used to describe software designed to be installed into a computer system for the purpose of causing harm to you or others. This would include viruses, spyware, trojans, worms, etc.

Worm

A self-replicating virus that does not alter files but resides in active memory and duplicates itself.

Ransomware

'Ransom Software' is a type of malware which handicaps computer functionality, for example, through browser hijacking or encrypting personal data, and offers to restore the functionality for a fee, which is extortion. Paying the fee does not guarantee removal of the ransomware, which can lay dormant ready for attack in the future.

Phishing (email/website)

Fraudulent email messages or web sites used to deliver malicious content (such as malware); or gain access to personal information for illegal purposes such as transferring funds or purchasing goods over the internet.

Trojan horse

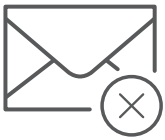
Malicious code that is hidden in a computer program or file that may appear to be useful, interesting, or at the very least harmless to you when using your computer. When this computer program or file is run, the malicious code is also triggered, resulting in the set up or installation of malware.

CryptoLocker

A particularly malicious type of ransomware which, once installed on your computer, encrypts and locks all of the files on the infected computer including documents, photos, music and video. A pop up window will then display on the computer screen requesting payment of a ransom in return for a CryptoLocker key to unlock the encrypted files. Paying the ransom does not guarantee removal of the CryptoLocker.

Keylogger

A keylogger is a program that records the keystrokes on a computer. It does this by monitoring a user's input and keeping a log of all keys that are pressed. The log may be saved to a file or even sent to another machine over a network or the Internet. Keylogger programs are often deemed spyware because they usually run without the user knowing it.



Spam

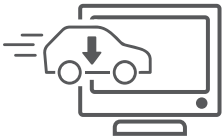
Unsolicited email. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or illegal services. Users are advised that if an offer in an email appears too good to be true then it probably is and should not be actioned in any way.

Scareware

Malware that causes frightening messages to appear (for example, that your computer is infected with malware or that you are guilty of a crime), and attempts to extort money from you to resolve the alleged issue. Similar to ransomware.

Man-in-the-middle

A man-in-the-middle attacker inserts themselves between two parties who are communicating with each other online, so they can disable or alter those communications.



Drive-by download

A drive by download occurs when a user's computer is infected with malware simply by visiting a compromised website.

Zombie or bot

A single compromised computer (a robot computer), called a zombie or a bot. Once infected, these computers can be used for malicious activity without the knowledge of the user.

Water-holes

Malware placed on a legitimate website that attempts to compromise visitors' computers.

Catfish

Internet predators who create fake online identities to lure people into emotional or romantic relationships for personal or financial gain.

Immunise your business, network and systems

Sometimes basic hygiene practices are not enough to maintain good health. Just as immunisation helps prevent some serious diseases, securely configuring your network and computer systems can make them more resistant to common types of attack. The following steps will further improve network and system security:

- Restrict the use of administrative privileges on computer systems. Staff with administrator privileges should only use their administrator account when required and not when reading email or accessing external websites.
- Consider using an IT service provider to securely manage your systems. If so, make sure you clearly understand the services and security practices they will provide.
- If you use cloud services, ensure the division of responsibilities for setting security configurations is clearly defined and understood.

Protect business computers and devices by keeping them separate from potential sources of contamination or attack.

- If you store individual health information on business computers, encrypt the disk drive in the event that these computers are stolen or lost.
- Change default passwords to long passphrases, including on your business' modem/router and systems that contain patient and customer information.
- If business Wi-Fi is enabled, use WPA2 encryption with a long passphrase.
- Non-business computers may have security bugs which could be exploited or malware which may compromise them. Create a 'bring your own device' policy which clearly outlines requirements for the use of non-business devices such as laptops, tablets or mobile phones, when connected to your business network and computers.
- Consider setting up a virtual private network (VPN) to enable secure remote access for staff.
- Ensure anti-virus software automatically scans USBs, external hard drives and DVDs when connected to business computers.
- Only install applications that are needed on business computers. Fewer applications means fewer security bugs, which could be exploited, and fewer applications which need to be kept up-to-date.

Just as doctors use tests to detect health problems, monitor business computers to find and treat security bugs that could be exploited.

- Use a vulnerability scanner to identify unpatched software or other insecure computer settings.
- If using an IT service provider to manage your network and systems, ask them to provide regular vulnerability reports and updates about security issues for systems they are managing on your behalf.

Poorly secured websites provide another way through which cyber criminals can access sensitive business information.

- By exploiting security holes on your website, a criminal can install malware in order to infect users' computers which connect to the website. Check that your IT service provider keeps your website software patches up-to-date and has a plan to fix your website if it is compromised.
- Ensure that the password that allows you to login and modify pages on your business web site is changed to a long passphrase.
- Make sure the login page uses a 'https' connection with a padlock in the browser address bar. This will ensure passphrases are encrypted and cannot be viewed by criminals.

Information Security Guide
for small healthcare businesses

Further information

More material about how to protect personal and business information is available on the Stay Smart Online website: **www.staysmartonline.gov.au**.

You can subscribe to security alerts on the Stay Smart Online (**www.staysmartonline.gov.au**) and Scamwatch (**www.scamwatch.gov.au**) websites.

More information about effective security measures is available on the following websites:

- **www.racgp.org.au** – The Royal Australian College of General Practitioners. Search for: 'Information Security in General Practice'.
- **www.healthit.gov** – The US Government has produced a list of security tips for small healthcare businesses. Search for: '10 tips cyber security healthcare'.
- **www.nist.gov** – The US National Institute of Standards and Technology has produced an information security guide for small businesses. Search for: 'Small Business Information Security: The Fundamentals'.
- **www.acsc.gov.au** – The Australian Cyber Security Centre has a range of useful information, including *Strategies to Mitigate Cyber Security Incidents*.

More information about the Digital Health Cyber Security Centre is available on the Australian Digital Health Agency website: **www.digitalhealth.gov.au**.

Notes

☐ Do you have an external hard drive to do a backup?

☐ Have you subscribed to the Stay Smart Online Alert Service?

☐ Is information security part of your business plan?

☐ Have you set your computer to automatically update its software?

☐ Have you set up an information security education program for your workers?

Notes

☐ Do you have an external hard drive to do a backup?

☐ Have you subscribed to the Stay Smart Online Alert Service?

☐ Is information security part of your business plan?

☐ Have you set your computer to automatically update its software?

☐ Have you set up an information security education program for your workers?

Australian Government
Australian Digital Health Agency

STAY SMART ONLINE

OFFICIAL

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should see appropriate independent professional advice in relation to your own circumstances.

This document has been prepared by the Australian Digital Health Agency and the Attorney-General's Department.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Second edition
ISBN - 978-0-9876434-0-7 (Print)
ISBN - 978-0-9876434-1-4 (Online)

Attribution

Using the Commonwealth Coat of Arms

The terms of use for the Coat of Arms are available from the It's an Honour website **www.dpmc.gov.au/government/its-honour**

STAY SMART ONLINE

Information Security Guide

for small healthcare businesses

Australian Government

Australian Digital Health Agency