Guidance

Cyber security guide for small healthcare businesses

Your healthcare business or practice has access to valuable digital information entrusted to you by patients, 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 cyberattacks may cause you to lose access to critical business systems or internet bandwidth making it difficult to run your business.

This guide will highlight good cyber security practices to assist in building cyber resilience and protecting critical information and assets in your business from cyberattack.

Protecting individual's health information

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 1988* 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" (Australian Privacy Principle 11.1). In the event 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.

The Office of the Australian Information Commissioner (OAIC) defines a data breach as:

"A data breach happens when personal information is accessed, disclosed without authorisation or is lost. For example, when:

- *a USB or mobile phone that holds an individual's personal information is stolen*
- *a database containing personal information is hacked*
- *someone's personal information is sent to the wrong person.*

A data breach can harm an individual whose personal information is affected. They can, for example, suffer distress or financial loss."

Understanding your responsibilities under the Notifiable Data Breaches scheme is an important part of building cyber security resilience. Establishing and implementing a response plan helps healthcare providers understand how to respond if a data breach occurs. This should be supported by appropriate cyber security practices that demonstrate what is reasonable for the business to do to protect individual health information.

Strong access controls - passphrases and multifactor authentication

Passphrases help protect your information from unauthorised access 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 techniques to obtain or 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 15 characters, including 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 the 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. As with any system, password managers should also be protected with a strong passphrase and multi-factor authentication (MFA).

MFA can protect against phishing and other passphrase attacks. Instead of just entering a username and password, MFA 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, a passkey or biometrics like your fingerprint, or on a portable security key (for example, a YubiKey).

Example of how to create a strong passphrase:

- Use at least 4 random words and aim for 15 characters or more.
- Avoid names, birth dates, clinic names, common phrases or predictable patterns.
- Use a different passphrase for each important account, especially email, remote access and business-critical systems.
- Store passphrases securely using approved tools or processes and never share them.

Passphrase example: riverteacupplanetlantern.

Passphrase example with extra complexity: River7-Teacup!Planet-Lantern42.
(Apply if a system requires extra complexity such as capital letters, numbers or special characters without losing the randomness of the words.)

Steps to secure devices, networks and websites

Cyber criminals routinely target networks and information systems. Any device connected to the internet is potentially within reach of criminals from anywhere in the world. By adopting basic, effective cyber security practices, your business will be more resistant to attacks.

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 and applying security patches, you can reduce the risk of common cyber attacks.

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. Public Wi-Fi networks may expose your information to unauthorised access if appropriate security controls are not in place. Potentially they may also be able to log on as you, even if they don't know your username and password.

Securely configuring your network and computer systems can help reduce the risk of common cyberattacks.

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 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 at a minimum, WPA3[1] if available, with a long passphrase.
- Security flaws or malware could affect non-business computers, putting them at risk. It's important to establish a clear 'bring your own device' policy that specifies the conditions under which personal laptops, tablets, or phones can be 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, and external hard drives when connected to business computers.
- Install only essential applications on business computers. Having fewer apps reduces potential security vulnerabilities and limits the number of programs that require updates.

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; you will require assistance from your IT services provider.
- If you use 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.

[1] Personal cyber security: Advanced steps guide | Cyber.gov.au

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

- By exploiting security holes on your website, a criminal can install malware 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 website 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.

Suggested actions to take:

- Check with your IT team or service provider to confirm the status of your operating systems and application software.
- Set business computers to automatically update operating systems and application software where possible.
- Install anti-virus software and an ad-blocking browser plugin on staff computers to help prevent malware infections.

Prepare for an emergency - 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. Secure and up-to-date backups can help your business recover more quickly from an incident.

In the event of a cyberattack, 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.

Suggested actions to take:

- 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.
- Be aware of your obligations to report breaches of individual information and have a plan for accessing technical and legal advice.

Cyber security awareness

Health professionals need to stay abreast of the latest health risks. Similarly, by keeping abreast of the latest cyber 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.

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.

Stay informed and subscribe to alerts published by:

- Australian Digital Health Agency: Digital Health Cyber Security Alerts
- Australian Cyber Security Centre: Sign up for alerts | Cyber.gov.au
- ScamWatch: Subscribe to scam alert emails | ScamWatch

Help create a more secure and cyber resilient healthcare sector for all Australians and register to join the Agency's Cyber Champion Network.