CyberWardens.

Keep your practice in good health

Small business cyber security guide for medical practices, allied health providers and healthcare professionals

COSBOA COUNCIL OF SMALL BUSINESS ORGANISATIONS AUSTRALIA

cyberwardens.com.au

Healthcare is a prime target for cyber criminals

The healthcare industry holds some of the most sensitive and valuable data: patient records, Medicare numbers, payment details, prescriptions, and clinical notes.

It's no surprise that healthcare is now the most targeted sector for cyber attacks in Australia.

Whether you run a busy medical centre, a physiotherapy practice, or a solo psychology clinic, the risks are real.

A single cyber incident can lead to a total loss of patient trust, costly service downtime, and even mandatory reporting to regulators.

And for small practices, the stakes are even higher. With limited time, IT support and resources, it's often up to the practice manager, receptionist, or clinician to keep systems secure.

To help, we have developed this dedicated Cyber Security Guide for the healthcare industry. Inside you'll find practical steps to protect your systems, patient data and reputation.

You can also enrol yourself and your team in the free Cyber Wardens training program designed for everyday Australians, with no jargon or tech skills required.

How does cyber crime affect healthcare?

Healthcare is the **#1 Target** for cyber crime in Australia

1 in 5 data breaches in Australia come from the **healthcare industry**

82% of Australians fear unauthorised access to their **health records**

In 2024 **88%** of healthcare professionals opened **phishing emails**

PRO TIP!

The Cyber Wardens Cyber Aid webinar is specifically designed for healthcare practitioners and medical professionals. You'll learn how to spot scams and identify cyber red flags.

Register today: cyberwardens.com.au/health

Recent cyber incidents in Australian healthcare

Cyber attacks on healthcare providers are no longer isolated events. They are becoming more frequent, targeted, and damaging. From large service providers to small specialist clinics, no part of the sector is immune.

These recent Australian incidents reveal how cyber criminals exploit vulnerabilities in digital systems to steal patient data, disrupt services, and erode public trust.

Genea Fertility Clinic data breach

FEBRUARY 2025

Genea, a leading IVF provider, was targeted by the ransomware group Termite. The attackers accessed and stole approximately 940.7GB of highly sensitive patient information, including medical records, appointment schedules, and personal details.

The stolen data was later published on the dark web, raising serious concerns about patient privacy and data handling practices in the sector.

Heart Centre cyber attack

JANUARY 2025

A network of cardiology clinics in New South Wales operating under the Heart Centre brand was infiltrated by the cybercriminal group DragonForce.

The attackers stole sensitive health information, underscoring vulnerabilities in IT infrastructure and the urgent need for enhanced cyber protections in private health clinics.

MediSecure data breach

MAY 2024

MediSecure, a major electronic prescription service provider, suffered a devastating ransomware attack.

The breach affected around 12.9 million Australians and exposed names, Medicare numbers, prescription information, and medical treatment details. This incident is considered one of the largest in Australia's history, affecting a significant portion of the population.

Following the breach, MediSecure went into voluntary administration, partly due to the financial strain of responding to the incident.

Why health data is a goldmine for cyber criminals

Health information is some of the most valuable data a criminal can steal. Unlike credit card numbers, which can be cancelled, your medical history, Medicare number, and personal details are permanent.

Cyber criminals use this data to commit identity theft, create fake Medicare claims, or sell the information on the dark web where it can be used for years to come. In some cases, sensitive health information is used to extort individuals or damage reputations. Because healthcare records link financial, personal, and medical details in one place, they offer criminals a complete profile that's far more useful and profitable than a stolen credit card alone.

In the case of the Genea Fertility Clinic breach, IVF patients had not only their names and contact details exposed, but deeply personal information about their treatments.

This type of data could be used by cyber criminals to impersonate patients, create fraudulent billing claims, or even blackmail individuals by threatening to release private medical details publicly.

For criminals, healthcare data represents a long-term investment. They can use it to build highly convincing scams, target people when they least expect it, and sell it repeatedly over time.

REAL LIFE STORY

Thien Trinh, podiatrist and small business owner

Podiatrist Thien Trinh, founder of Stepwell Podiatry and cork insole business Stryda, has faced significant challenges due to cyber crime.

Since 2022, his business's social media accounts have been hacked twice, resulting in a loss of $12,000 and countless hours spent on recovery efforts.

The first incident began with a seemingly harmless message from a friend on Facebook. Clicking on the accompanying link allowed cyber criminals to access his Facebook accounts, leading to unauthorised posts, including inappropriate content, and unauthorised purchases using stored credit card information.

This breach forced Thien to halt all Facebook operations for two years, significantly impacting his business's online presence and client acquisition. The second attack occurred just a week before his scheduled appearance on Network Ten's Shark Tank in 2023.

This time, Thien quickly identified the breach and managed to regain control within an hour.

These experiences have made him more vigilant, leading him to complete the Cyber Wardens training program.

> **If I had done this course years ago, I probably never would have been hacked," he says.**
>
> **"Using multi-factor authentication, and doing software updates as often as you can are among the most important things you can do. We are watertight now. Cyber security is so crucial."**

Thien's journey underscores the critical need for small healthcare businesses to prioritise cyber security measures to protect their operations and client trust.

Most common cyber attacks in healthcare

Ransomware

Cyber criminals lock down your files and demand payment to release them, often halting patient care and operations.

Phishing and email scams

Emails posing as Medicare, pathology labs, or software vendors trick staff into clicking malicious links or revealing credentials.

Malicious attachments or forms

Fake faxes or scanned referrals can contain malware when opened on reception computers.

Compromised systems

Insecure Wi-Fi networks, outdated antivirus software, or poor password habits can allow unauthorised access to practice systems.

Data Breaches

Unauthorised access to patient information due to poor password security, misconfigured software, or lost devices.

Payment redirection scams

Fake invoices or changes to bank account details, usually disguised as updates from regular suppliers or billing platforms.

How to protect your healthcare practice

Know your patient

- Confirm identity for unusual bookings or telehealth requests
- Don’t take Medicare or card details over email or text
- Treat every unsolicited request for information with caution

Secure your systems

- Use strong, unique passwords and multi-factor authentication for your medical software and email
- Keep all systems and antivirus software updated
- Limit admin access to sensitive data only to those who need it

Scrutinise every email

- Check sender addresses closely, especially if the message asks you to “verify”, “urgently review”, or “reset” something
- Don’t open unexpected attachments, especially if they claim to be faxes, referrals, or reports
- Call suppliers directly to confirm bank detail changes

Train your team

- Make sure front desk, billing and support staff know how to spot suspicious activity
- Include cyber security in staff onboarding
- Have regular discussions about cyber security with your team

Trust your instincts

- If something feels off, stop and check before clicking or replying
- Report anything suspicious to the Australian Cyber Security Centre (cyber.gov.au/report)
- Have a backup plan in place in case of system outages or breaches

Cyber security checklist

- [ ] Read this guide and look for gaps in your current practices
- [ ] Complete the free Cyber Wardens training and encourage your team to enrol
- [ ] Review who has access to what information in your systems
- [ ] Store and share patient data only through secure, approved platforms
- [ ] Be extra cautious with emails, invoices and any changes to payment details
- [ ] Follow Cyber Wardens on social media for tips and real-life scam warnings
- [ ] Regularly test your cyber response plan and backups

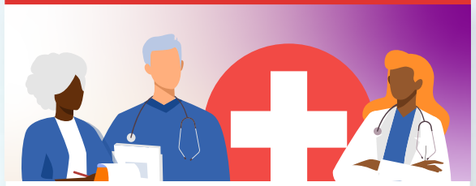
Prevention is better than cure

Cyber security is everyone's job, from receptionists and allied health staff to practice owners and managers. Make sure your whole team is equipped to help defend your business.

Cyber Wardens training is free, easy to follow, and designed with small businesses in mind.

Choose from our growing suite of options:

Cyber Aid for Health Professionals — 30 mins



Specialised training to help medical professionals protect sensitive patient data from cyber threats.

Format:	Live or on-demand webinar
Suitable for:	Healthcare professionals and support staff

Cyber Wardens **Foundations** — 10 mins

Learn to spot cyber security red flags and essential strategies to protect your business.

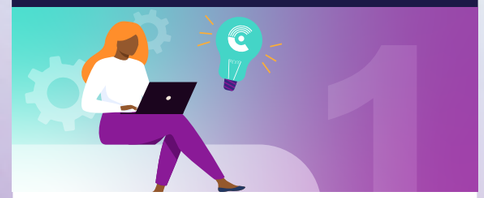
Format:	Online course
Suitable for:	Busy business owners and employees

Cyber Wardens **Foundations Webinar** — 30 mins

Expert-led session covering key cyber risks, warning signs, and practical security steps for small businesses.

Format:	Live or on-demand webinar
Suitable for:	Business owners and employees who prefer interactive, guided learning

Cyber Wardens **Level One** — 30 mins



Master four essential cyber security practices to protect your small business from common threats.

Format:	Online course
Suitable for:	Small businesses seeking improved cyber resilience

Cyber Wardens **Level Two** Safe AI for Small Business — 30 mins

Simple and effective ways to keep small businesses safe from complex AI scams.

Format:	Online course
Suitable for:	Small businesses seeking a deeper understanding of AI's cyber security threats

CyberWardens.

Help protect your practice with Cyber Wardens

Complete the Cyber Aid webinar and safeguard your practice with free and simple cyber security training

Enrol now at **cyberwardens.com.au/health**

Cyber Aid

Proudly supported by

Australian Government

COSBOA