PDSA PRACTICE GUIDE

Cybersecurity for Australian General Practices

A Plan, Do, Study, Act (PDSA) implementation guide

AUTHOR

Dr Chris Mitchell AM

CPD HOURS

Approximately 9 hours

COMPOSITION

3h EA + 3h RP + 3h MO

MBS ITEMS

None

TIMELINE

3 to 6 months

MEDIUS GLOBAL

mediusglobal.com.au

What a Plan, Do, Study, Act (PDSA) gives your practice

CPD for the whole team

GPs can meet a significant share of their 50-hour annual CPD requirement without leaving the practice. When submitted as a practice-based or group activity, hours can be logged across EA, RP and MO categories. Nurses maintain their own CPD records and declare compliance at annual registration renewal via AHPRA. Practice managers count it toward AAPM certification.

GP retention

A practice that runs structured QI activities absorbs a substantial portion of the 50-hour CPD obligation and its administration on behalf of its GPs. The GP gets CPD hours done within the practice, on problems relevant to their clinical work. The practice derives a retention benefit through this support.

Quality of care

Cybersecurity is a clinical governance issue. A data breach exposes patient health information, disrupts clinical services and triggers mandatory notification obligations. A documented PDSA demonstrates the practice has taken structured steps to reduce that risk. It is ready-made evidence for RACGP accreditation.

Risk reduction

Unlike clinical PDSAs, this topic does not generate MBS revenue. The value is in cost avoidance. The average cost of a data breach for an Australian organisation exceeds $4 million (IBM Cost of a Data Breach Report 2024). A GP practice will not face costs at that scale, but even a minor breach involves legal fees, notification costs, reputational damage and lost patient trust.

Cybersecurity in general practice

Cybercrime is a prevalent threat to all Australian industries. Healthcare is a high-value target because medical records contain identity, financial and clinical information that is harder to detect and more difficult to resolve than standard identity theft. Recent high-profile breaches (Medibank, MediSecure) have demonstrated that health sector organisations of any size are at risk. GP practices have fewer resources than large insurers or hospital networks, which makes them more reliant on structured security practices and staff awareness.

CYBERSECURITY STATISTICS

- 15% of data breaches involve healthcare organisations
- 75% of breaches were caused by people outside the organisation
- 81% of hacking-related breaches leveraged weak or stolen passwords
- 73% of breaches were financially motivated

Why health data is particularly valuable

- Medical records contain identity information that is harder to detect if compromised than standard identity theft
- Financial information in health records can be exploited for fraudulent claims

- Clinical information can be used for blackmail or extortion
- Health data is more valuable on the dark web and more difficult to resolve when stolen

The financial case for cybersecurity

Unlike clinical PDSAs, this topic does not generate MBS revenue. The value is in cost avoidance. The average cost of a data breach for an Australian organisation exceeds $4 million (IBM Cost of a Data Breach Report 2024). A GP practice will not face costs at that scale, but even a minor breach involves legal fees, notification costs, reputational damage and lost patient trust.

A documented PDSA on cybersecurity demonstrates the practice has taken structured steps to reduce risk. It is ready-made evidence for RACGP accreditation and shows prospective GPs that the practice invests in systems that protect patient information and staff workload.

CPD HOURS FROM THIS PDSA

Approximately 9 hours when submitted as a practice-based or group activity: 3 EA (cybersecurity education sessions and background material review), 3 RP (security audit, phishing data collection and analysis), 3 MO (the PDSA cycle itself). All participating GPs log via myCPD or their preferred portal. Nurses and practice managers claim separately under their own frameworks.

CPD hours from this PDSA

CATEGORY	FOCUS	HOURS
EA	Cybersecurity education sessions and background material review	3
RP	Security audit, phishing data collection and analysis	3
MO	PDSA cycle (plan, do, study, act with documented outcomes)	3
Total	All components when submitted as practice-based or group activity	9

Note on CPD requirements: The Medical Board of Australia (via AHPRA) requires all registered medical practitioners to complete 50 hours of CPD annually, including a minimum of 12.5 hours EA and a minimum of 25 hours combined RP and MO (with at least 5 hours of each). The RACGP currently classifies PDSAs under Measuring Outcomes. However, when submitted as a group or practice-based activity, each component can be logged to its correct category.

How this guide works

- ● Worked example from Dr Chris Mitchell's practice
- ○ Your practice: fill in your own details

Each section includes a worked example from a real cycle conducted by Chris Mitchell in a mixed rural practice, followed by space for your practice to document your own process.

CM

Dr Chris Mitchell AM

Rural GP and Rural Generalist with over 30 years of clinical and leadership experience. Member of the Order of Australia for contributions to general practice and eHealth. Chris has worked across practice operations, governance, digital health and quality improvement throughout his career.

Important notes

The educational materials at the end of this document contribute to EA (Educational Activities) hours. When you review and discuss this material with your practice team, those hours count toward the 3 EA hours for this PDSA.

All participating GPs log via myCPD or their preferred portal. Nurses maintain their own CPD records and declare compliance at annual registration renewal via AHPRA. Practice managers count it toward AAPM certification requirements.

This PDSA can be submitted individually or as a group/practice-based activity. When submitted as a group or practice-based activity, CPD hours can be allocated across EA, RP and MO categories as shown above.

The PDSA cycle

Idea

Cybersecurity is an increasing risk to practice staff and patients. Recent breaches (Medibank, MediSecure) have highlighted the vulnerability of health data. GP practices have fewer resources than large organisations, making structured risk reduction essential.

A practice that runs a cybersecurity PDSA demonstrates to staff and to prospective GPs that the practice takes data protection seriously. It creates a culture where security practices are discussed and reinforced, reducing the likelihood of staff bypassing security measures under time pressure.

This PDSA cycle can be completed in 3 to 6 months depending on your practice's schedule and IT provider's availability. It involves education sessions with your whole team, a structured conversation with your IT provider, and monthly tracking of phishing attempts to build awareness.

Plan

Risk can be reduced through two parallel activities: education of the whole practice team and implementation of technical security measures. The practice will conduct a security audit with its IT provider, deliver cybersecurity education sessions for all staff and independent doctors, and establish ongoing phishing awareness monitoring.

WORKED EXAMPLE

We decided to run the project over three months. Month one: security audit with our IT provider and first education session. Month two: begin phishing tracking and review perimeter protections. Month three: second and third learning sessions, consolidate findings and implement changes.

YOUR PRACTICE

Record the following details:

Timeline planned:	
IT provider contact:	
Education session dates planned:	
Phishing tracking start date:	

Do: Security audit

The security audit involves a structured conversation with the practice IT provider. The questions below cover the key domains. The worked example shows real responses from a practice IT provider (deidentified).

WORKED EXAMPLE

1. Software and security patches

Question: Can you confirm this is all under control?

Response: Servers have updates applied monthly unless a specific security advisory is received from Microsoft, then that would be applied at the earliest possible time. The laptop is typically updated monthly during the test restore of the BP database. For the desktops, currently, automatic updates are disabled but they are reviewed and installed during a BP upgrade. We can look at implementing a desktop update policy.

2. Multi-factor authentication

Question: Can you confirm the only access is via two-factor processes for access outside the practice building?

Response: Remote access for users is only available through VPN, requiring an authentication code to be appended to the password.

3. Antivirus and ransomware protection

Question: Can you confirm this is all automated? Is there a report of this process?

Response: Yes. Sophos Firewall and Endpoint signatures are updated automatically. In your monthly report, the security section shows the health of that protection. Your current level of Endpoint security is Intercept X Advanced. There are higher levels of Endpoint protection that can be employed using XDR (Extended Detection and Response) and MDR (Managed Detection and Response).

4. Geographic blocking

Question: Do we have geographic blocks? Do we need Russian or North Korean IP addresses to access our network?

Response: We can apply geo-blocking to the firewalls to drop all traffic from specific countries of origin. You need to provide us with the countries you want blocked. Sometimes clients source products or information from countries with a poor security profile but have a commercial reason.

5. USB and port security

Question: Are our USB ports shut down? Should they be? Will Sophos scan anything in a USB port before it does damage?

Response: No, at this point we have not blocked the use of USB ports. It can be done within the security policy but there would be consequences and users would need to be made aware of the change in advance. Yes, devices are scanned and that is the default policy. Note: If you find a USB or a disc, do not load it at the practice to see what it is.

6. Wi-Fi security

Question: Can you confirm that the Wi-Fi is segregated from access to Best Practice? Is any further segregation required?

Response: The Wi-Fi is connected to the LAN where the Best Practice server resides. The Wi-Fi is not publicly accessible and there is a complex password required to connect. Only the practice manager and the owners know or have access to that passphrase. If there is a requirement for general Wi-Fi access by users and the public, we could implement a separate network.

YOUR PRACTICE

Record the following:

Security audit date:

IT provider name:

Findings for each audit topic:

Do: Practice education

Deliver a cybersecurity education session for all staff. Cover phishing awareness, password security, social engineering and the practice data breach policy. The background and reference section at the end of this guide provides education material that can be used for this session. Review and discussion of this material with your practice team contributes to the 3 EA hours.

WORKED EXAMPLE

We held an initial education session covering phishing red flags, password security and our data breach notification obligations. All clinical and administrative staff attended. We then asked each doctor and staff member to keep a monthly record of suspicious emails and text messages received at work.

YOUR PRACTICE

Record the following:

Education session date:

Attendees:

Topics covered:

Follow-up actions:

Do: Meeting and action schedule

YOUR PRACTICE: RECORD YOUR DATES

Security audit with IT provider	
First education session	
Phishing tracking begins	
Perimeter protection review	
Second learning-together meeting	
Third learning-together meeting	
Follow-up meeting to confirm learnings	
RACGP portal upload	

Study: Phishing tracking data

Each doctor and staff member records the number of suspicious emails and text messages received at work each month. This data is collected across three learning-together meetings to track awareness and identify patterns.

WORKED EXAMPLE

Learning-together meeting 1:

DOCTOR	EMAIL PHISHING	TEXT PHISHING	ISSUES IDENTIFIED
	12	53	Wrong address for Linkt, not used
	20	12	Mostly wrong spelling or urgent action re bank
	24	4	
	30	38	
	22	46	
	16	8	
	24	16	
	22	29	

DOCTOR	EMAIL PHISHING	TEXT PHISHING	ISSUES IDENTIFIED
	24	23	
	16	88	
	18	40	
	36	43	Linkt, 'your package couldn't be delivered', Coles
	26	29	
	60	32	
	14	34	Linkt seems to track my travel, gave card and had to cancel it
	28	23	
	48	43	

Learning-together meeting 2:

DOCTOR	EMAIL PHISHING	TEXT PHISHING
	18	66
	22	8
	30	10
	28	42
	24	52
	14	12
	31	22
	25	32
	20	26
	14	65
	24	42
	38	52
	26	24

DOCTOR	EMAIL PHISHING	TEXT PHISHING
	66	26
	18	25
	32	12
	44	32

Learning-together meeting 3:

DOCTOR	EMAIL PHISHING	TEXT PHISHING
	22	78
	26	12
	28	14
	32	41
	27	39
	11	14
	26	31
	32	27
	12	32
	22	62
	21	32
	43	54
	34	27
	52	32
	23	26
	27	18
	49	39

YOUR PRACTICE

Create your own tracking table using the format above, collecting data from each doctor and staff member across three learning-together meetings.

Study: Perimeter protection review

WORKED EXAMPLE

The perimeter protection is provided by Sophos XG Firewall v20. We reviewed:

- Google handles inbox checking for spam and malicious code
- Whether Sophos Email Gateway is needed (quote sought)
- Sophos Central MDR Complete versus current Intercept X Essentials
- Sophos Intercept X for Server lockdown capability
- Monthly maintenance report reviewed

What we learned

WORKED EXAMPLE

- We need to look more closely at the segmentation of our drives
- Explore Cloudflare Gateway
- Consider CI-ISAC Intelligence for tailored threat intelligence across critical infrastructure sectors
- While we were not affected by the CrowdStrike incident, it is a risk for consideration

YOUR PRACTICE: RECORD YOUR LEARNINGS

Study: Education review

Based on the phishing tracking data and learning-together meetings, the practice revised its key education messages:

- Never provide your password
- Think critically: is this likely to be genuine?
- Check the sender address
- Hover your mouse over the sender's email address to see if it matches the address shown
- Look for spelling, grammar and punctuation errors
- Be wary of demands for urgent action
- Make sure your home computer and phone have antivirus and ransomware protection
- Do not use public Wi-Fi for practice-related work

Act: What to change and embed

WORKED EXAMPLE

The practice issued the following actions to all staff and independent doctors:

- Ensure the practice log-on is a complex passphrase that is not reused
- Avoid stored practice passwords in an internet browser such as Google Chrome
- Use multi-factor authentication
- Do not use USBs or CDs on your computer at work
- Never provide your password
- Complete phishing and social engineering education (see background section)
- Record the number of suspicious emails and texts received at work and submit monthly
- Share any learnings by email to the group

The practice will follow up with penetration testing and a report.

YOUR PRACTICE: RECORD CHANGES TO EMBED

Key cybersecurity actions checklist

ACTION	COMPLETED (DATE)
Update software and security patches	
Complex passwords or passphrases (not reused)	
Avoid stored passwords in browsers	
Multi-factor authentication implemented	
Phishing and social engineering education delivered	
Security audit completed with IT provider	
Geographic blocking reviewed	
USB port policy reviewed	
Wi-Fi segregation reviewed	
Network segmentation reviewed	
Data breach policy reviewed with all staff	
Staff access permissions reviewed (role-based)	
Systems backed up and tested	
Website login protected with MFA	
Penetration testing completed	
Devices reset before disposal	

Submitting for CPD hours

Log this PDSA via myCPD or your preferred CPD portal as a group or practice-based activity. Record the time as you go and document discussions in meeting minutes for AHPRA requirements. Consider how the activity addresses your reflections on professionalism and ethical practice.

The activity structure maps to all three AHPRA CPD types when each component is submitted separately under its correct category:

ACTIVITY COMPONENT	AHPRA CPD TYPE	ESTIMATED HOURS
Cybersecurity education sessions and background material review	Educational activities (EA)	3 hours
Security audit data collection and phishing tracking analysis	Reviewing performance (RP)	3 hours
PDSA cycle (plan, do, study, act with documented outcomes)	Measuring outcomes (MO)	3 hours

Nurses log separately via AHPRA/NMBA. Practice managers count toward AAPM certification requirements.

TIMING TIP

Check where you sit in the triennium before logging hours. If the project spans two triennium periods, start the new submission from the date the new triennium begins. Do not log hours to a period where you have already met your requirements.

Doctors involved

DOCTOR'S NAME	QI AND CPD NUMBER

EDUCATIONAL BACKGROUND MATERIAL

Background and reference

This section contains the educational and clinical background material that supports the PDSA. It forms part of the Educational Activities (EA) component of the CPD hours for this project. Review and discussion of this material with your practice team contributes to the 3 EA hours.

Resources

- RACGP Computer and Information Security Standards (CISS)
- Australian Cyber Security Centre (ACSC)
- ACSC Essential Eight Maturity Model

- ACSC Small Business Cyber Security Guide
- Office of the Australian Information Commissioner (OAIC) - Notifiable Data Breaches scheme
- CI-ISAC Australia (Critical Infrastructure Information Sharing and Analysis Centre)
- RACGP Practice Technology and Management guide
- Services Australia - PRODA security requirements
- KnowBe4 security awareness training platform
- IBM Cost of a Data Breach Report (annual)

Cybersecurity threats to general practice

Cybercrime is a prevalent threat to all Australian industries. 15% of breaches involve healthcare organisations. Information stolen from health records is particularly valuable because the theft can take longer to be identified than standard identity theft. Unlike stolen credit cards which can be cancelled, medical identity theft is more complex and difficult to resolve.

Key statistics:

- 75% of breaches were caused by people outside the organisation, with 51% involving organised criminal groups
- 81% of hacking-related breaches leveraged weak or stolen passwords
- 73% of breaches were financially motivated

Five core security measures

1. Update software and security patches
2. Complex passwords or passphrases that are not reused
3. Avoid stored practice passwords in an internet browser such as Google Chrome
4. Multi-factor authentication

5. Phishing and social engineering education for the entire team

Social engineering

Social engineering relies on the six Principles of Influence established by Robert Cialdini (Influence: The Psychology of Persuasion):

- **Reciprocity:** people tend to return a favour
- **Commitment and consistency:** people honour commitments that fit their self-image
- **Social proof:** people do what they see others doing
- **Authority:** people tend to obey authority figures
- **Liking:** people are persuaded by people they like
- **Scarcity:** perceived scarcity generates demand

Social engineering attacks commonly involve:

- **Pretexting:** masquerading as someone else
- **Baiting:** enticing the victim with promises of something of value
- **Blackmail:** threatening to reveal something the target wishes to keep secret
- **Quid pro quo:** promising a service or benefit in exchange for information or access

Phishing

Phishing attacks are the most common type of social engineering. Attackers use emails, social media, instant messaging and SMS to trick victims into providing sensitive information or visiting malicious URLs.

Common characteristics of phishing messages:

- Messages designed to attract attention with limited information, encouraging the victim to visit a specific website
- Sense of urgency to trick the victim into disclosing sensitive data
- Shortened URLs or embedded links redirecting to malicious domains
- Deceptive subject lines using forged sender addresses or spoofed organisational identity

Red flags to watch for:

- Spelling, grammar and punctuation errors
- Demands for urgent action
- Sender email address does not match the displayed name (hover to check)

Pretexting

Pretexting involves presenting oneself as someone else to obtain private information. The success of a pretexting attack depends on the attacker's ability to build trust. Advanced pretexting attacks manipulate victims into actions that expose organisational vulnerabilities. An attacker can impersonate an external IT services operator to extract information from internal staff.

Baiting and quid pro quo attacks

Baiting exploits human curiosity. A classic example is an attacker leaving infected USB drives in a car park, waiting for someone to insert them into a corporate PC.

Quid pro quo attacks promise a service or benefit in exchange for information or access. The most common scenario involves a hacker impersonating IT staff and offering software upgrades, then requesting the victim to temporarily disable antivirus software.

Password security

In organisations without multi-factor authentication, passwords are the only barrier between an attacker and unauthorised access. Users commonly choose simple passwords that are easy to remember and easy to guess.

Common vulnerabilities found in penetration tests:

- Passwords using the organisation name and a combination of numbers (e.g. current year)
- Password spraying: trying common passwords (123456, Password1) across many accounts
- Passwords stored in internet browsers (Google Chrome)

Recommendations:

- Use a passphrase instead of a simple password (e.g. H0wTh3BlueBunnyH0ps!51 instead of Bunny51)
- Choose a completely new passphrase each time, rather than changing a few characters
- Use a password manager (LastPass, 1Password) instead of storing passwords in the browser

Multi-factor authentication

MFA requires two or more pieces of authentication before granting access. The three types of evidence are: something you know (password), something you have (SMS code, token, authentication app), and something you are (biometrics).

A password plus security question is not true MFA because both are 'something you know'. A password plus an authentication app (Google Authenticator) is a better combination. For higher security, consider hardware 2FA (YubiKey, RSA token).

Network segmentation

Proper network segmentation prevents lateral movement attacks. If an attacker gains access through one device (e.g. an IoT device or compromised VPN), segmentation limits how far they can move through the network.

Recommendations:

- Systems that do not need to communicate should be in separate network segments
- Only select individuals should access critical and sensitive resources
- Implement a jump box for administering devices in separate security zones
- Review IoT devices connected to the network

Firmware and patching

After a vulnerability is discovered, developers release a security patch. Organisations that fail to install patches promptly leave themselves open to known exploits. Implement a proper patch management policy.

Steps to protect your data and personal health information

- Avoid sharing accounts (also a My Health Record use breach)
- Annual policy reviews (e.g. My Health Record)
- Antivirus and ransomware protection
- Geographic blocking
- USB port policy
- Antiviral scans on USB drives, external drives and DVDs
- Wi-Fi risk management
- Network segmentation
- Role-based access (revoke when staff leave)
- System backups
- Website login protection with MFA
- Penetration testing
- Reset devices before sale or disposal
- Keep devices physically secure
- Have a data breach plan

Data breach policy

Australia has moved from a voluntary to mandatory data breach notification scheme. Practices are required to notify individuals likely to be at risk of serious harm because of a data breach. The decision to notify the individual and the Office of the Australian Information Commissioner via a notification statement is to be based on the advice from your medical defence organisation.

Penetration testing

Penetration testing checks how far an attacker could get into your systems. Three types:

- **White-box:** done with full knowledge of the environment, simulating an insider
- **Grey-box:** done with partial knowledge, simulating an attacker with some insider information
- **Black-box:** done with no knowledge, simulating an external attack

Penetration tests should be performed annually. Organisations that test regularly have a better security posture overall.

Recommendations for the practice:

- Use security technology that checks all downloads from the internet, including cloud services

- Monitor downloads of executable files (.exe) and archive files (.zip, .rar)
- Block downloads from cloud applications and services employees do not need
- Consider solutions that block suspicious network traffic
- Understand your data breach policy and how to implement it
- Consider remote browser isolation (RBI) tools

Security awareness training

One of the most significant threats to an organisation's security is untrained users. Security awareness training should not be a one-time event. Implement ongoing quarterly training.

KnowBe4 recommendations:

- Avoid singling out users who click phishing links and making a public example of them
- Avoid sending the same phishing template instead of randomising
- Avoid starting with difficult-to-identify phishing templates