

Cyber security essentials for healthcare practices

Secure systems, protected patients, continuous care.

1

Use Multi-Factor Authentication (MFA)



- Turn on MFA for email, cloud services, remote access, banking, clinical systems and administrator accounts.
- MFA adds an extra step, e.g. a phone code, and can stop hackers even if they know your password.

2

Use a password manager



- Create and store long, unique passwords in a password manager.
- Use one strong passphrase for the password manager and protect it with MFA.
- Never share passwords or write them down.

3

Back up your data and test it



- Use the 3-2-1 rule: keep 3 copies of data, on 2 media types, with 1 copy stored offsite or offline.
- Test your backups regularly and include a recent restore test so you can restore systems when you need to.

4

Keep systems and software up to date



- Turn on automatic updates for all devices, operating systems, browsers, clinical software and business applications.
- Updates fix security weaknesses that cyber criminals exploit.

5

Be alert to cyber attacks



- Many cyber-attacks start with a phishing email, text or call. Report suspicious messages.
- Be wary of unexpected emails, attachments, urgent links, or requests for passwords or payments.
- If something looks unusual, stop and check with a known contact before clicking, replying or paying.

6

Use access controls



- Give staff access only to what they need to do their job.
- Add starter and leaver processes, least-privilege access and separate administrator accounts.
- Lock your computer when stepping away.

7

Have a simple cyber response plan



- Know who to call, what to disconnect, and where key account and backup details are kept.
- Keep important contacts and backup details in a safe place.
- If personal information is affected, you need to notify people via the Notifiable Data Breaches scheme.

Quick wins today

- ✓ Turn on MFA for all logins
- ✓ Set up a password manager.
- ✓ Check your last backup and test restoring a file.
- ✓ Ask your IT provider about application control and Essential Eight.

Need help, or think you've been breached?

Contact your practice's IT provider straight away or the Australian Cyber Security Centre 24/7 Hotline: 1300 CYBER1 (1300 292 371).