SECURED BY HealthIT

ACSC Australian Cyber Security Centre

NETWORK PARTNER

PROTECTING YOUR PRACTICE, PATIENT AND YOURSELF

A guide to help improve the Cybersecurity posture of a medical business

INTRODUCTION

Cybersecurity is a complex and ever evolving problem; and an enormous risk to any connected business.

The Essential Eight, our Australian security framework is a prescriptive and relatively easy framework to align to. Achieving compliance with at least maturity level 1 of this framework will mitigate the risk and limit the potential damage of a security event.

All practices should work to comply to maturity level 1 of the Essential Eight, then revisit and decide whether to further improve the maturity level against the Essential Eight, and / or to align to a more complex security framework like CIS, NIST or ISO27001.

HealthIT
Connecting Health

THE ESSENTIAL EIGHT

our security framework

While no set of mitigation strategies are guaranteed to protect against all cyber threats, organisations are recommended to implement eight essential mitigation strategies from the ACSC’s *Strategies to Mitigate Cyber Security Incidents* as a baseline. This baseline, known as the Essential Eight, **makes it much harder for adversaries to compromise systems.**

HealthIT
Connecting Health

THE ESSENTIAL EIGHT

Security Controls

1. Application Control
To prevent the execution of unapproved applications and other dangerous things

2. Configure MS Office Macro Settings
Block untrusted macros

3. Patch Applications
Scan for and mitigate security vulnerabilities

4. User application hardening
Disable unneeded vulnerabilities

5. Restrict Administrative Privileges
Limits the scope of damage

6. Patch Operating Systems
Scan for and mitigate security vulnerabilities

7. Multi-Factor Authentication
Massive increase in external security

8. Regular Backups
Our last line of defense is recovery

ACSC
Australian
Cyber Security
Centre

NETWORK PARTNER

HealthIT
Connecting Health

THE ESSENTIAL EIGHT

maturity levels

Zero

No protection

One

Protection from Opportunistic attacks

- "Drive by"
- "Script kiddies"
- (Bulk) Phishing
- Website compromise

Threat actor is using common tools to look for any victim

Two

Protection from Selective attacks

- Spear Phishing
- May be targeting health specifically
- May be looking for supply chain attacks

Threat actor is using common tools but spending more time and energy on potential targets

Three

Protection from Focused attacks

- Targeting you specifically
- Less reliant on common tools
- May be able to cover their tracks and dig deeper and for longer into your network

OTHER COMPLIANCE

THE PRIVACY ACT 1988

A data breach happens when personal information is accessed or disclosed without authorisation or is lost. You must notify affected individuals and the OAIC when a data breach is *likely* to result in serious harm.

No medical practice is exempt under the small business exception to the Privacy Act!

GP ACCREDITATION

C6.4 A Our practice has a team member who has primary responsibility for the electronic systems and computer security.
C6.4 B Our practice does not store or temporarily leave the personal health information of patients where members of the public could see or access that information.
C6.4 C Our practice's clinical software is accessible only via unique individual identification that gives access to information according to the person's level of authorisation.
C6.4 D Our practice has a business continuity and information recovery plan.
C6.4 E Our practice has appropriate procedures for the storage, retention, and destruction of records.
C6.4 F Our practice has a policy about the use of email.
C6.4 G Our practice has a policy about the use of social media.

HealthIT
Connecting Health

MY CYBER SECURITY CHECKLIST

What can I do to make my surgery more secure today?

People

❑ **Establish security training for all staff and ensure ongoing training happens**

Health IT customers receive free ongoing security training – ask IT if this is available.

Consider phishing simulations or inside email system security hints.

❑ **Review staff permissions and ensure administrative access is limited.**

Use the concept of least privilege to restrict potential damage – if you don't need access to something daily you don't need everyday access to it!

❑ **Improve staff onboarding / offboarding to include security**

Ensure access is appropriate and secure and promptly removed when necessary.

❑ **Do not trust by default, test by default**

Use more than one form of communication to test things, especially if they seem too good to be true. Build this sort of testing into your culture with training and reminders.

MY CYBER SECURITY CHECKLIST

What can I do to make my surgery more secure today?

Process

❑ **Understand your backup strategy and have it tested**

Where are your backups? What is backed up? What potential downtime exists? How are they tested?

❑ **Review and update your business continuity / information recovery plans**

Document what to do in the case of a disaster. Have a one sheet plan laminated and available. A free Data Breach Response template is available from HealthIT.com.au .

❑ **Review and update your Internet / Email / Social Media policy**

These policies are required for GP Accreditation. A free template is available from HealthIT.com.au .

❑ **What other process / policy do they need? What do you insurance policies say?**

HealthIT
Connecting Health

MY CYBER SECURITY CHECKLIST

What can I do to make my surgery more secure today?

Technology

❑ **Speak to IT about compliance with the Essential Eight or get an audit done**

Complying to a more complex framework may work for you but we suggest achieving Level 1 maturity in the Essential Eight as a starting point.

❑ **Turn on auto-update for everything**

Ensure operating systems and applications are kept up to date to minimise vulnerabilities.

❑ **Disable or lock down Office Macros**

If somebody really needs to use a macro it can be allowed, but they should be off by default.

❑ **Protect external access to everything with multi-factor authentication**

Access should be tested and reported on regularly. If exceptions are required find another way to secure each use case.

❑ **Improve your password posture**

Ensure external passwords are AT LEAST 12 characters long and are unique. Use a password manager.

HealthIT
Connecting Health

RESOURCES

Australian Cyber Security Organisations

https://www.cyber.gov.au/ - the Australian Cyber Security Centre – a wealth of information and the home of not just the Essential Eight but the Small Business Cyber Security Guide, and the Information Security Manual (ISM) for larger business, a Cyber incident reporting tool and much more.

https://www.oaic.gov.au/ - the Office of the Australian Information Commissioner – information and reporting of any Notifiable Data Breach.

Free DIY Cyber Security Resources

https://healthit.com.au/password-strength-checker/ - anonymously check the strength of your passwords.
https://passphrase.com.au/ - create strong and unique passphrases
https://haveibeenpwned.com/ - free Dark Web check – see if your email address or phone number has been leaked
https://emailsecuritytester.com/ - commercial product but offers a free email security scan
https://hostedscan.com/ - commercial product but offers a free web site / location scan
https://www.grc.com/ - Shields UP!! – check your firewall for open ports

Other Security Advisories

https://www.cisecurity.org/ - the Centre for Internet Security – home of the CIS framework and the MS-ISAC free security advisory service.

https://www.cisa.gov/ - the US Cybersecurity & Infrastructure Security Agency.

https://www.cert.govt.nz/ - CERT NZ – the New Zealand cyber security organisation.