Introduction to Cyber Security

What is Cyber Security?

Cyber Security, also known as information technology security or electronic information security, is the practice of defending digital information and data stored on computers, servers, devices, systems, and networks. It is a multifaceted practice which provides security to protect information stored digitally from malicious attacks which attempt to steal, leak, or corrupt your private information.

Why does Cyber Security matter?

Within healthcare, the privacy of patient information is vital and protected by several laws in Australia, including the Privacy Act, the Crimes Act (1914), the Security of Critical Infrastructure Act (2018), the Telecommunications (Interception and Access) Act (1979), and more. It is your duty as a healthcare practitioner, as well as the duty of the practice you work for, to protect the privacy of your patients. By utilising the tools, practices, systems, and habits which protect this information, you are protecting your patients and yourself from attempts to intercept this private information.

How does Cyber Security benefit me and my practice?

By protecting your patient's private information, you are meeting the legislative requirements laid out for medical professionals. You are also protecting yourself from heavy fines, legal action by patients whose information is breached, and protecting your practice's information and your own information as an individual. Hackers may also seek to breach privacy for financial gain – i.e. selling private information online or extorting businesses by holding private information 'hostage' until payment is received. If your practice has a cyber security breach, this may affect your organisation's profitability, access to critical business systems and its capacity to run business as usual.

Cyber Security Guide for General Practice

- ☐ Consult the Office of the Australian Information Commissioner's (OAIC) guidelines.
- ☐ Update all staff members log in information.
  Ensure all staff have strong, unique usernames and passwords.
- ☐ Wherever possible, use two-factor authentication for best protection during log in process.
- ☐ Ensure all operating systems/software are set to update automatically wherever possible.
- ☐ Install anti-virus software and an ad-blocking browser plug-in to help prevent malware.
- ☐ Be aware of obligations to report breaches of individual information and have a plan for accessing technical and legal advice for these situations.
- ☐ Ensure that all measures are compliant with the requirements of the RACGP.
  These can be found in the RACGP guidelines.
- ☐ Keep frequent back-ups for all critical information and systems.
  Have off-site back-ups that are not connected to the practice network to protect from loss due to fire, theft, or malware.
- ☐ Subscribe for alerts and updates.
  Subscribe for alerts from Stay Smart Online, ScamWatch, and your software vendors.
- ☐ Educate staff about Cyber Security and the measures in place.
  Also educate staff about risks to look out for, such as phishing/scam emails.

For ongoing support and education, please visit the Australian Digital Health Agency website, or contact the Capital Health Network's Digital Health Team (see contact page at back of this booklet).

<u>Websites to visit:</u>

Staysmartonline.gov.au
scamwatch.gov.au
racgp.org.au/running-a-practice/security
nist.gov
healthit.gov
cyber.gov.au