Digital Age Regulations & Cybersecurity

Reading time:
Donna Dalby

Date created: 28/07/2021

Tags: Article | Medico-Legal | Medical Practitioner | Dental Practitioner

Why are privacy and cyber security important to healthcare practitioners?

Cybersecurity in healthcare is of increasing concern. Healthcare organisations are attractive targets for cybercrime for two main reasons: they are a rich source of highly prized personal information and its defences are comparatively weak. Digital security is not just a technical problem, but rather a complex sociotechnical issue. Human behaviour proves to be one of the biggest contributors to cybersecurity vulnerability, and staff referred to as “cybersecurity’s weakest link”[1].

Behaviours that compromise cyber security[2]

- Poor computer and user account security
- Unsafe email use
- Use of USBs and personal devices
- Remote access and home working
- Lack of encryption, backups and updates
- Unsecured use of connected medical devices
- Social engineering
- Poor physical security.

Cyber hygiene principles

Focus on information security risks you experience across your critical domains of healthcare delivery

- Use a risk analysis framework to identify, prioritise and respond to risks and vulnerabilities.
- Ensure any third-party suppliers you use (such as cloud services, practice management software) undertake a similar exercise and are managing their information security risks.

Upskill yourself and your team with good cyber hygiene practices (strong passwords, using up-to-date software and not clicking on suspicious emails or links)

Cyber hygiene best practices[3,4]

- Encrypt and password-protect mobile devices, including cell phones, iPads, and laptops.
- Install and update anti-virus and malware software.
- Secure your wireless network
  - Turn off and update the default name and password the router came with from the manufacturer.
  - Turn off remote management and log out as the administrator once it's set up.
  - Ensure your router offers WPA2 or WPA3 encryption to maintain the highest level of privacy of information sent via your network.
- Create one Wi-Fi network for your practice and another for your patients (eg practice and practice guest).
- Create and enforce a workplace policy requiring strong passwords using a mixture of letters, numbers, and symbols.
- Use multi-factor authentication
  - Two-factor or multi-factor authentication offers an additional layer of protection
- Encrypt all devices and media that store personal and sensitive data — laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage.
- Audit software applications on each computer, maintaining a list of approved software applications and removing any unauthorised software as soon as it is detected.
- Develop, implement and exercise and implement backup and disaster recovery plans
- Ensure staff who leave your practice are 'offboarded' (accounts disabled, mobile phones wiped, and logins of key systems changed)
- Automate your practice's security practices reducing the impact of human error.

MIPS Membership

The benefits of membership include the MIPS indemnity insurance which relates to the provision of healthcare. It excludes and does not cover any claims associated with the loss of, damage to, or the failure to properly protect the security of, electronic or hard copy medical records. MIPS does not provide, a cyber cover or Practice Entity cover. Members need to make their own assessment and consider their risk in relation to this. MIPS has established a relationship with Aon to help facilitate MIPS members to enquire and obtain an estimate for practice entity and cyber cover - Practice entity and cyber cover referral

Missed the previous MIPS webinar on this topic?Catch up On-Demand here

This information is not intended to be legal advice and as such should not be relied on as a substitute. You may need to consider seeking legal or other professional advice about your individual circumstances as appropriate. Should you wish to obtain further information you can review our Member Handbook Combined PDS and FSG or contact MIPS on 1800 061 113. You may need to consider seeking legal or other professional advice about your individual circumstances as appropriate. Information is current as at the date published.

Useful resources

- RACGP Factsheet - Responding to a cybersecurity incident
- RACGP - Information security in general practice
- RACGP - Computer and information security standards
- Office of the Australian Information Commissioner - Privacy action plan for your health practiceMIPS Practice Notes
- Cyber: Legacy system letdown
- Cyber risk: The essential of online security
- Cyber security attacks – are you prepared?
- Why should I insure my clinic?

[1] Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. Intelligence and National Security, 35(4), 556-585.

[2] Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: a narrative review of trends, threats and ways forward.Maturitas, 113, 48-52.

[3] Checklist: Protecting office computers in medical practices against cyberattacks (2019)

[4] Good cyber hygiene habits to help stay safe online (2021)