Avant factsheet:
Cyber security checklist

This cyber security checklist can assist you in reviewing security measures in your practice. If the check reveals your security measures are not adequate, update them.

Establish a security culture

- □ Designated team members are responsible for championing and managing computer information security
- □ Checklists and policies for managing computer and information security are in place
- □ Checklists and policies for information transfer, storage and destruction are in place
- □ Education is kept up-to-date through regular training
- □ The practice has up-to-date security against threats

Maintain good computer habits

- □ Policies are in place specifying system maintenance procedures
- □ Computers are free of unnecessary software and data files
- □ Remote sharing and printing are disabled, unless security measures are in place
- □ Systems and applications are updated or patched regularly (automatically where possible), as recommended by the manufacturer
- □ Processes are in place to ensure safe and proper use of internet and email
- □ Consider advanced threat protection security services for email and internet (e.g. web proxies) to restrict access to known malicious internet sites and email hygiene – review email for cyber threats
- □ All staff log off the system(s) at the end of each day

Control physical access

- □ Policies are in place prescribing the physical safety and security of devices
- □ Computers are protected from environmental hazards, such as extreme temperatures
- □ Physical access to secure areas is limited to authorised individuals
- □ Equipment located in high traffic or less secure areas is physically secured
- □ Physical storage devices, including hard disks and documents containing patient information, are securely stored and accounted for

Protect mobile devices

- □ Policies are in place about the use of mobile devices
- □ Mobile devices are configured and password protected to prevent unauthorised access
- □ Patient health information on mobile devices is encrypted

Control access to health information

- □ All staff understand and agree to abide by the practice's access control policies
- □ Each user has an individual account and their activity can be monitored
- □ Users are only authorised to access information they need to know to perform their duties
- □ There are reliable and secure systems in place for electronic sharing of patient health information with other specialists, patients and, when authorised, third parties

Avant mutual
by doctors for doctors

☎ 1800 128 268
avant.org.au

Limit network access

- □ Access to the network is restricted to authorised users and devices
- □ Staff are prevented from installing software without prior approval
- □ Wireless networks use appropriate encryption
- □ Separate and isolate internal wi-fi from public wi-fi that is accessible for patients. Protect wi-fi hotspots by changing the pre-installed password
- □ Public instant messaging services that are not password protected are not used

Passwords and passphrases

- □ Policies are in place that specify password obligations for your practice
- □ Passwords/passphrases are at least eight characters in length, with a combination of upper and lower case, numbers and symbols
- □ Each staff member has their own username and password
- □ Login information is not shared between staff or with anyone outside the organisation
- □ Computers are set to automatically lock after a period of inactivity
- □ Where possible use two factor authentications

Antivirus software

- □ Policies are in place requiring antivirus software
- □ All staff know how to recognise symptoms of viruses or malware on their computer and what to do
- □ Antivirus software is set to allow automatic updates from the manufacturer

Firewalls

- □ All computers are protected by a properly configured firewall

Plan for the unexpected

- □ A data breach response plan is in place
- □ Policies are in place specifying back-up and recovery procedures
- □ Staff understand the recovery plan and their duties during recovery
- □ System restore procedures are known by more than one person within the practice and at least one trusted party outside the practice, such as your IT provider
- □ A copy of the recovery plan is stored safely off site

This publication is not comprehensive and does not constitute legal or medical advice. You should seek legal or other professional advice before relying on any content, and practice proper clinical decision making with regard to the individual circumstances. Persons implementing any recommendations contained in this publication must exercise their own independent skill or judgment or seek appropriate professional advice relevant to their own particular practice. Compliance with any recommendations will not in any way guarantee discharge of the duty of care owed to patients and others coming into contact with the health professional or practice. Avant is not responsible to you or anyone else for any loss suffered in connection with the use of this information. Information is only current at the date initially published. © Avant Mutual Group Limited [July 2019] MJN53-2 07/19 (0983)

If you have an Avant practice policy you have automatic cyber insurance coverage.
If your practice policy is with another provider we suggest you check with them about your coverage.

Avant mutual
by doctors for doctors

☎ 1800 128 268
avant.org.au