Avant
By doctors for doctors

Cyber security Checklist

The 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
- [ ] Orientation/induction for new team members includes education on cyber security
- [ ] 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. Software is uninstalled when it is no longer used
- [ ] 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 thoroughly examine emails to identify and mitigate potential cyber threats (email hygiene)
- [ ] Implement policies and procedures requiring all staff to 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
- [ ] Mobile devices are configured and password protected to prevent unauthorised use
- [ ] Log off/lock computers when not attended

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 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

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 all users in your practice
- [ ] Passwords should not be displayed in clear text when entered
- [ ] Password length must be at least fourteen alphanumeric characters and include at least one special character (such as !, @, #, $, &, *, ?). Passphrases are encouraged as length and memorability are important security considerations
- [ ] Each staff member has their own username and password
- [ ] Passwords are never shared or written in an accessible place
- [ ] Login information is not shared between staff or with anyone outside the organisation
- [ ] Computers are set to automatically lock after a period of inactivity
- [ ] Temporary passwords are changed on a successful login
- [ ] Where possible use multi-factor authentication

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
- [ ] Staff can access recovery plans and contact numbers without using the computer system
- [ ] 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
- [ ] Test recoveries from backup drives are performed reasonably regularly
- [ ] A copy of the recovery plan is stored safely off site