Steps to protect your practice from a cyber security incident

Summary

Preparation is your best defence to minimise the chance of a cyber security incident. This fact sheet provides a quick guide on the following issues:

- the importance of policies and procedures
- implementing a business continuity plan
- updating contracts with third party providers
- how to use an IT service provider
- six steps to protect your IT system.

Policies and procedures

Your practice should have a policy that covers the expectations of staff in relation to cyber security, including:

- not sharing passwords
- using the internet
- downloading software to the practice system
- caution when opening unusual emails
- prohibiting use of personal email addresses in the workplace.

The policy should outline your protocol for backing up data and a recovery plan if an incident occurs. All staff should be trained and regularly updated on their responsibilities if an incident occurs.

Business Continuity Plan

It is essential to have a business continuity plan. The plan should outline your data back-up procedures and contain details on patient care management if there is major incident. For example, we recommend that you have a supply of paper prescription pads, a hard copy appointment diary and patient history forms, manual billing processes including manual Medicare forms for patients to sign, available to use if a cyber incident occurs.

Review and update contracts with third party providers

Ensure third party back-up providers (e.g. in the cloud) or outsourced back-up providers who store information have security measures in place to protect private information.

Contracts with IT software and hardware providers should include a clause that protects the practice if there is a security breach due to a system error or fault on the part of the provider.

Request regular reports from your IT provider on back-ups being tested for restorability & viability.

IT service provider

An external expert view can be helpful. Consider hiring an IT consultant to undertake a security audit or risk assessment to test the potential threat to the practice and to help implement mitigation strategies.

Talking to your IT service provider about cyber security protections

There is no one-size-fits-all IT solution for medical practices to reduce the risk of a cyber incident. For example, the risk profile and IT needs of a metropolitan practice with 30 doctors seeing hundreds of patients with an electronic health records system and online appointments will be different to a sole practitioner in a remote town with limited access to the internet who uses mostly paper-based records.

A risk assessment of your practice is vital to identify:

- how you use technology
- where the risks are
- the most likely staff to be a target for a cyber incident (e.g. staff with IT administration privileges)
- your staff's level of awareness and understanding of their role in risk mitigation.

An IT consultant should explain what they propose for your practice and why in plain language. They should be able to guide you through the requirements for your practice.

Six steps to protect your systems

The following six steps to protect your network and system can help you navigate discussions with your IT service provider:

Check your network security controls

Your IT consultant should check your network security controls including:

- remote desktop privileges (e.g. log-on from home or remote IT support)
- firewall (network and/or local computer)
- virtual local area networks (vLANs)
- intrusion detection and protection.

Ask the provider the following questions to help facilitate this process:

- How are these maintained?
- Is there a monitoring process in place?

- How are unusual behaviours tracked, reported and addressed?

Check how your network and computing systems can be accessed and who will have access.

- How are user IDs created and managed?
- Are certain users granted access to systems administration (more advanced than the usual staff role) and is this access regularly reviewed and managed?
- When a staff member moves to another role or leaves the practice, how is their access changed, deactivated or deleted?
- Do you have password standards (e.g. complexity, expiry, secure communication of passwords, etc) that leverage best practice? Are they being followed?
- How is compliance monitored and reported? If there is non-compliance, how is it managed?

Check that all personal computing devices i.e. laptops, desktops and mobile phones, are also secure.

Update your systems and software with patches

Alerts that pop up to advise a new software update is available to install can easily be ignored. However, regularly installing operating system (security) and software updates is one of the most effective ways to keep healthcare systems protected against cyber intrusions and viruses.

Known as patches, these updates resolve any issues in your operating system, applications, and programs. If there is a known security risk they should be applied immediately. If there is no security risk identified, they should be installed within 48 hours of the alert.

Keep applications (e.g. Adobe Flash, web browsers, Microsoft Office, Java, PDF viewers, etc) and operating systems up to date as some may no longer be supported by the manufacturers, increasing vulnerabilities to your systems. Your IT service provider should advise you when to change your systems.

Use anti-virus and ad-blocking software

Cyber criminals commonly use malicious software (malware) to target computers with viruses, spyware, trojans and worms. These can be delivered by email or while browsing the web. Some malware is also delivered through advertisements on the web.

To prevent these attacks compromising your systems, ensure anti-virus software and an ad-blocking browser plug-in is installed and up-to-date, and allow automatic updates from the manufacturer.

Use strong passwords

Strong passwords are vital to keep sensitive health information safe and to prevent cyber intrusions. Hackers can use automated methods to guess a password, so avoid using personal information in your password. This includes anything that can be found on social networking sites, even if the words are slightly altered. Consider implementing the following in your practice:

- Passwords should not be displayed in clear text when entered.
- Change passwords regularly and/or set a password expiry period.
- Staff must never share passwords.
- 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.
- Temporary passwords are changed on a successful login.
- The login account is locked after a set number (such as 3), unsuccessful attempts to log in.

Use two factor authentication

The primary purpose of two-factor authentication is to enhance security and mitigate the risks associated with password-based authentication alone. Even if hackers manage to obtain users passwords, they will need the second factor to gain access. In this way, two-factor authentication is a powerful security measure that provides an additional layer of protection for online accounts, reduces the risk of password-related breaches, and enhances overall security and privacy for users. Application based two factor authentication is recommended.

Backup your business systems and files

Backing up computer systems and files is crucial to protect against data loss, whether due to hardware failures, software issues, accidental deletion, or security breaches. Hackers may also use malware to deny access to files and can demand a ransom to regain access. Malware can usually only be removed by wiping the computer and reinstalling the operating systems, applications and data from backups. Some things to consider when backing up your business systems and files:

- Determine what to back up – identify the critical files and data that you need to back up regularly.
- Choose a back up method – external hard drives, Network Attached Storage, cloud storage or online back up storage.
- Implement the 3-2-1 backup rule.
  - Have at least three copies of your data.
  - Store the copies on two different types of media (e.g. local hard drive and cloud storage).
  - Keep one copy off-site (e.g. cloud storage or external drive stored at a different location).
  - Regularly schedule backups.
  - Encrypt your backups.
  - Test your backups.

Remember the key to effective backup practices is consistency and redundancy. By implementing a robust backup strategy, you can significantly reduce the risk of data loss in the event of a cyber security incident.

Further resources

Information security guide for small healthcare businesses (digitalhealth.gov.au)

Cyber security training and support | Australian Digital Health Agency

Computer and information security standards (Royal Australian College of General Practitioners)

Essential Eight | Cyber.gov.au

For more information or immediate medico-legal advice, call us on 1800 128 268, 24/7 in emergencies.
avant.org.au/mlas

Visit our **Insights & Resources** page for further educational content including webinars, eLearning courses, case studies, articles and checklists.