Avant factsheet:

Preventing data breaches

In the simplest form, a 'data breach' is a breach of a person's privacy or the security of information held by an organisation about a person. Data breaches can be many and varied, and can range from a malicious attack on computer systems (hacking and malware); the inadvertent disclosure of sensitive information due to an internal error or failure to follow information handling processes and procedures; through to damage of files (paper or electronic) because of a natural disaster such as a fire or flood.

Protecting the privacy and confidentiality of the personal information you hold is an important professional and legal obligation.

Not only can a data breach or breach of privacy leave you open to a complaint to the Office of the Australian Information Commissioner (OAIC) or disciplinary action by regulatory authorities. A data breach can also have a significant impact on your relationship with your patients, as well as causing reputational damage to you and your practice.

Steps you can take to prevent data breaches:

1. Ensure you and your staff are aware of your privacy obligations.
2. Review and update information handling practices, procedures and systems.
3. Review and update your contracts and arrangements with third party providers.
4. Implement mitigation strategies to prevent cybersecurity incidents.

Ensure you and your staff are aware of your privacy obligations

Your practice has an obligation under the *Commonwealth Privacy Act 1988* to take all reasonable steps to protect the personal information you hold from misuse, interference and loss, and from unauthorised access, modification or disclosure (APP 11).

- Train your staff and regularly update them about their privacy obligations, security of your systems and policies and procedures in your practice.
- Keep up to date with changes to privacy laws and obligations.
- Appoint a senior staff member to be responsible for privacy compliance in your practice.
- Talk about privacy and security at practice meetings, including any privacy incidents or near misses.

Resources:

Avant's Top 10 privacy tips, privacy essentials and Avant guide to privacy reforms are resources that can help to remind you of your privacy obligations.

Review and update information handling practices, procedures and systems

Reviewing your information handling practices, procedures and systems can help to ensure that your processes and systems are up to date, reduce the risk of a privacy or security breach in your practice and reduce the time and expense involved in addressing any breaches.

You should have the following in place at your practice:

- a privacy policy outlining how information is collected, used and disclosed in your practice
- documented privacy and security processes and procedures, including processes for managing staff authorisation, authentication and access to records
- a process for proactively detecting data breaches
- a data breach response plan to apply if a privacy or security breach is discovered
- a business continuity plan and disaster recovery plan, so that if there is a disruption to your systems you can continue to operate your practice.

Resource:

The RACGP Computer and information security standards provides detailed information and templates for ensuring computer and information security at medical practices.

Consider the security measures in place at your practice, and if they are not adequate, update them. Our cybersecurity checklist can assist you in reviewing the security measures in place at your practice.

Consider:

- protection from human error, natural disasters, power interruptions, malicious attacks – firewalls, encryption, password policies, anti-virus/antimalware protection
- where information is stored and if you have measures in place to ensure the security of information held on servers, back-ups (onsite or off-site), in the cloud (in Australia or overseas), on portable devices (memory sticks, flash drives, smart phones, laptops)
- If information can be accessed remotely, ensure it can be deleted remotely if necessary
- physical security of information you hold – where physical files are kept, and who has access to them, where you make telephone calls to patients or other healthcare providers and who has access to the premises during the day and after hours.

If documents need to be destroyed, ensure you use a secure document destruction company and that they have adequate security measures in place to guarantee safe transit and destruction.

Resources:

OAIC Guide to Securing personal information
RACGP Computer and information security standards

Review and update your contracts and arrangements with third party providers

- Ensure third party providers who store information (e.g. in the cloud; outsourced backup providers), have security measures in place to protect private information.
- Ensure your contracts with IT software and hardware providers include a clause that protects the practice if there is a breach due to a system error or fault.

Implement mitigation strategies to prevent cybersecurity incidents

The Australian Signals Directorate recommends that organisations implement eight essential strategies to mitigate the risk of a cybersecurity incident. These are:

1. Application whitelisting – only allows selected software to run on computers.
2. Patch applications – to fix security vulnerabilities in software.
3. Disable untrusted Microsoft office macros – macros can enable the download of malware.
4. User application hardening – to block access to browsers which can be ways to deliver malware.
5. Restrict administrator privileges.
6. Patching operating systems - to fix security vulnerabilities in operating systems.
7. Multi-factor authentication.
8. Daily backup of important data and store securely offline.

An external expert view can be helpful. Consider hiring an IT consultant to undertake a security audit, testing and threat or risk assessment, and to help implement these mitigation strategies.

Resources:

Australian Digital Health Agency Information Security Guide for small healthcare businesses

Australian Signals Directorate Essential Eight Explained

IMPORTANT: Professional indemnity insurance products available from Avant Mutual Group Limited ABN 58 123 154 898 are issued by Avant Insurance Limited, ABN 82 003 707 471, AFSL 238 765. The information provided here is general advice only. You should consider the appropriateness of the advice having regard to your own objectives, financial situation and needs before deciding to purchase or continuing to hold a policy with us. For full details including the terms, conditions, and exclusions that apply, please read and consider the policy wording and PDS, which is available at avant.org.au or by contacting us on 1800 128 268. While we endeavour to ensure that documents are as current as possible at the time of preparation, we take no responsibility for matters arising from changed circumstances or information or material which may have become available subsequently. Avant Mutual Group Limited and its subsidiaries will not be liable for any loss or damage, however caused (including through negligence), that may be directly or indirectly suffered by you or anyone else in connection with the use of information provided in this presentation. 2251 09/19 (0983)

Cyber security checklist

Establish a security culture

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

Maintain good computer habits

6. Policies are in place specifying system maintenance procedures
7. Computers are free of unnecessary software and data files
8. Remote sharing and printing are disabled, unless security measures are in place
9. Systems and applications are updated or patched regularly (automatically where possible), as recommended by the manufacturer
10. Processes are in place to ensure safe and proper use of internet and email
11. 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
12. All staff log off the system(s) at the end of each day

Control physical access

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

Protect mobile devices

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

Control access to health information

21. All staff understand and agree to abide by the practice's access control policies
22. Each user has an individual account and their activity can be monitored
23. Users are only authorised to access information they need to know to perform their duties
24. 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

25. Access to the network is restricted to authorised users and devices
26. Staff are prevented from installing software without prior approval
27. Wireless networks use appropriate encryption
28. 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
29. Public instant messaging services that are not password protected are not used

Passwords and passphrases

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

Antivirus software

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

Firewalls

39. All computers are protected by a properly configured firewall

Plan for the unexpected

40. A data breach response plan is in place
41. Policies are in place specifying back-up and recovery procedures
42. Staff understand the recovery plan and their duties during recovery
43. 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
44. A copy of the recovery plan is stored safely off site