Avant
By doctors for doctors

Preventing data breaches

Quick guide

- Educate your staff and colleagues about the necessary steps to prevent a data breach.
- Regularly review your systems and processes.
- Consider hiring an IT consultant to undertake a risk assessment.

Data breaches

In its simplest form, a 'data breach' occurs when personal information is accessed, disclosed without authorisation, or is lost. 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.

A data breach or a breach of privacy can leave you open to a complaint to the Office of the Australian Information Commissioner (OAIC) or disciplinary action by regulatory authorities. It 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 and security 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 Privacy Act 1988 (Cth) to take all reasonable steps to protect the personal information you hold from misuse, interference and loss, and from unauthorised access, modification or disclosure (Australian Privacy Principle (APP) 11).

It is important that you:

- 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 Privacy basics and data breaches and Responding to data breach 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, specifically points one and two which are obligations under the Commonwealth Privacy Act , APP 1:

- 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 Information security in general practice 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 cyber security checklist can assist you in reviewing the measures in place at your practice. Issues to consider include: 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 Information security in general practice

Review and update your procedures to respond to and report a data breach

In the unfortunate event of a data breach, it is important to be ready to respond quickly and to know your obligations. Privacy breaches can be traumatic and emotional, and the incident can escalate and move quite quickly and it is unlikely you will have enough time to research and understand your requirements when a breach is discovered.

Before a data breach occurs, it is important to develop a procedure outlining required actions for all staff and third parties and to make sure everyone is aware of this procedure and understand their roles and obligations. Handling communications and reporting a data breach to regulators, legal entities, third parties and customers can be an exhausting and time-consuming process, so it is important to be prepared for this and to understand who is going to be involved and responsible for these actions.

Resource:

ACSC Reporting Support
Report and recover | Cyber.gov.au

Review and update your contracts and arrangements with third party providers

It is important to regularly review your contracts and arrangements with third party providers to make sure that the terms and conditions under which they operate have not changed. When reviewing your contracts and arrangements with third party providers it is important to ensure:

- Third party providers who store information (e.g. in the cloud; outsourced backup providers), have security measures in place to protect private information.
- 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

Resources for business and government | 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.

Avant
By doctors *for* doctors

*IMPORTANT: 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 practise 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 judgement 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 2024 fact-104 Published and current as of: 24/01 (DT-3631)