FACT SHEET

FOR SPECIALIST PRACTICES

Digital Foundations

Data Privacy, Security and Social Media

WHY IS DATA PRIVACY AND SECURITY IMPORTANT?

Data privacy and security are critical considerations for specialist private practice. Attention to privacy and security ensures that patients can be confident that their health and personal information is being used for the purpose it was intended and their right to privacy is being upheld. This trust and confidentiality underpin the professional and privileged position of a medical practitioner.

There are legal and professional data privacy and security requirements that apply to medical professionals in private practice. As patients' health information is classed as sensitive information under the *Privacy Act 1988*, privacy and security are critical to practice management. Non-compliance can carry fines and other penalties.

Breaches of data security and privacy carry significant reputational risks and can have serious financial consequences for businesses. Research has shown that the impact of a data breach can have a large impact on healthcare businesses and the healthcare industry is often a target for malicious attacks.

WHAT ARE MY SPECIFIC DATA PRIVACY OBLIGATIONS AS A MEDICAL PROFESSIONAL IN PRIVATE PRACTICE?

Information privacy is a legal requirement for healthcare providers in Australia. Requirements are set out in federal, state and territory legislation and in Office of the Australian Information Commissioner (OAIC) directives. Your obligations as a medical practitioner are consistent across physical and digital domains.

The OAIC's Guide to Health Privacy outlines eight key steps to implement privacy in your medical practice.[1] These include:

- STEP 1 Develop and implement a privacy management plan
- STEP 2 Develop clear lines of accountability for privacy management
- STEP 3 Create a documented record of the types of personal information you handle
- STEP 4 Understand your privacy obligations and implement processes
- STEP 5 Staff training
- STEP 6 Create a privacy policy
- STEP 7 Take reasonable steps to protect and secure personal information
- STEP 8 Develop a data breach response plan

Australian Government
Australian Digital Health Agency

WHAT ARE MY OBLIGATIONS IN RELATION TO DATA BREACHES?

Under the *Privacy Act* 1988, a data breach is a **notifiable data breach** where there has been:

1. Unauthorised access to, unauthorised disclosure of, or loss of personal information that the organisation holds; and
2. The data breach is likely to result in serious harm to any individual to whom the information relates; and
3. The entity has not been able to prevent the likely risk of serious harm with remedial action.

In the event of a data breach there are specific obligations a specialist practice must address:

1	Contain the data breach
2	Assess the data breach
3	Notify the OAIC and affected individuals concerned if it is a **notifiable data breach**. If it is not practicable to notify affected individuals, the statement provided to the OAIC (see below) may be provided on the practice website and reasonable steps must be taken to publicise the contents of the statement
4	Review the incident and undertake preventive action to ensure this does not occur again.

STATEMENT CONTENT: The statement must include the name and contact details of your practice, a description of the data breach, the kind or kinds of information involved, and what steps your practice recommends that individuals at risk of serious harm take in response to the data breach.

Different data breach obligations apply in relation to the My Health Record system.

For more information about managing data breaches, refer to the Data Breach Action Plan for Health Service Providers.

WHAT ARE MY OBLIGATIONS IN RELATION TO USE OF SOCIAL MEDIA?

Social media and the internet have opened valuable new lines of communication between healthcare providers and patients. However, they pose risks regarding security, confidentiality, maintaining professional boundaries and professional reputation. In many cases website and social media content will be subject to the same requirements as advertising regulated health services. Any inappropriate use of social media may result in harm to patients, professional reputation and trust. It may include breaches of confidentiality, defamation, or violation of patient and healthcare provider boundaries. The Australian Medical Association have provided this guide for each specific type of social media.

The Australian Health Practitioner Regulation Agency has developed guidelines to assist in meeting your obligations. These obligations include:

- Complying with confidentiality and privacy obligations,
- Complying with your professional obligations (e.g. code of conduct),
- Maintaining professional boundaries,
- Communicating professionally and respectfully with or about patients, colleagues and employers, and
- Not presenting information that is false, misleading or deceptive, including advertising only claims that are supported by acceptable evidence.

Further information about your obligations may be able to be provided by your medical indemnity or practice indemnity insurer.

NEXT STEPS

Digital Foundations Learning module 1: An overview of digital health, including proven benefits, digital technologies, and the key concepts required to understand digital systems.

Digital Foundations Learning module 2: An overview of data privacy and security, including key steps to ensure compliance and keep your practice safe.

[1] OAIC, 'Guide to health privacy', 2019, accessed 10 September 2020.