Privacy basics and data breaches: what you need to know

There are privacy obligations for medical practitioners in Australia in relation to patient communication, patient records and health information. This is legislated at both a Commonwealth and state level. This factsheet provides an overview of the key issues.

Private medical practitioners and practices in all states and territories must comply with the Commonwealth's *Privacy Act 1988*.

The Privacy Act was significantly amended in 2014 by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* and from 22 February 2018, further amendments require you to report eligible data breaches that are likely to cause serious harm.

The privacy legislation outlines how personal information is handled. This includes how you collect and store information, how you share it with others and destroy it when no longer needed. It also outlines when personal information can be used for direct marketing purposes and sent overseas.

The Privacy Commissioner has the power to conduct privacy assessments or investigations. There is a civil penalty for privacy breaches of up to $1.8m for corporations and $360,000 for individuals.

Victoria, NSW and the ACT also have legislation governing privacy obligations with which medical practitioners and practices in those jurisdictions must also comply.

It is your responsibility to review your privacy obligations and ensure your information handling practices, procedures and systems are up to date. This includes having a privacy policy in your practice that is available to patients free of charge.

Dealing with requests from partners and spouses for information on each other

A patient is entitled to have his or her health information kept confidential. As long as a patient is competent to request access to health information, no other person – even if they are the patient's partner or spouse – is entitled to access information without the patient's authority.

Dealing with requests from a parent for information concerning their child

Parents cease to have a right of access to their child's health information when their child is of sufficient maturity to make decisions about their healthcare. The child at this point can provide informed consent for medical treatment and is competent to exercise their rights to the privacy of, and access to, their health information.

Before the child has a sufficient level of competence, both parents have the right to access health information about their child. It does not matter that the parents may be separated or divorced, unless a court has directed that a parent has no right of access to their child's health information.

If one parent asserts that the other is not to have access to their child's health information, you should verify this by asking for and sighting a copy of the court order.

Privacy issues when dealing with patients over the telephone

The duty of confidentiality requires caution in discussing a patient's health information over the telephone. You must be satisfied that you are speaking to the patient or the patient's authorised representative. Asking a person to confirm their personal details is a common approach for substantiating their identity. If you are not satisfied with the particulars exchanged over the telephone, you should not disclose any health information.

If a patient asks for information to be provided by telephone, email, fax or mail to a third party, you should request a signed authority from the patient, in the same manner as would be required to provide a medical report or information to any third party. If the matter is urgent, you should document the request in the medical records.

Practice staff obligations regarding privacy

Patients are entitled to have their privacy respected by all staff at the practice and they should be made aware of the privacy obligations you all work under.

Regularly review how practice staff interact with patients, to ensure they are complying with the privacy requirements. This includes the following:

- Determine whether telephone conversations conducted by staff can be heard by patients at the reception desk or while waiting to see a medical practitioner. If so, implement strategies to ensure that patients do not become aware of other patients' health information as a result of overhearing telephone conversations.
- Similar considerations apply to conversations practice staff have with patients at the reception desk. It is inappropriate for practice staff to triage patients where discussions may be overheard by other patients.
- Clinical records, whether in storage, or awaiting the attention of a medical practitioner, must not be in view of patients attending the practice.
- Place computer screens so they cannot be viewed by patients attending the practice.
- When sending an SMS or email, ensure that the phone number or email address is current.

Exceptions to the privacy principles

Privacy of patients' health information is not absolute. Circumstances may arise where it is necessary to balance the public interest in maintaining privacy of health information and the public interest in avoiding danger or harm to the community, or individuals in the community.

Sometimes, doctors are faced with the dilemma that they have information they are expected to keep confidential but that, if disclosed to an appropriate authority, may prevent harm or result in the apprehension of a person who has engaged in serious criminal activity.

If you are faced with this dilemma, it is unwise to make a decision to maintain privacy, or to provide information to an appropriate authority, without first obtaining advice. A college or the ethics committee of a college is one avenue of advice. The Australian Medical Association is another. Avant is also able to assist members in determining the appropriate course when practitioners are faced with the dilemma of competing public interests.

Data breaches

A data breach occurs when there is unauthorised access or disclosure, or loss of personal information held in your practice. This could be an email sent to the wrong person, a lost laptop containing patient information or your database being hacked. Prevention of data breaches is much better than dealing with them after the fact. Consider hiring an IT specialist to advise you on how to minimise your risks.

Notifiable data breach changes to the Privacy Act (from February 2018) require you to investigate a data breach or suspected data breach, and decide if it is likely to result in serious harm to one or more individuals. You may be able to remediate the negative impact of the breach, for example by retrieving an email sent incorrectly or by having good security in place on a missing laptop. If not, you are obliged to notify the affected patients and the Office of the Australian Information Commissioner (OAIC).

For more advice, call Avant's Medico-legal Advisory Service on **1800 128 268.**

Visit **avant.org.au/avant-learning-centre** for resources including webinars, eLearning courses, case studies and checklists.

 2197 (0936) 10/17