AUSTRALIAN MEDICAL ASSOCIATION VICTORIA

FACTSHEET

This article is intended to provide general advice only. The contents do not constitute legal advice and should not be relied upon as such. Readers should seek specific expert and legal advice in relation to the information provided in this article.

MANDATORY DATA BREACH NOTIFICATION REQUIREMENTS UNDER THE PRIVACY ACT

September 2024

Amendments to the *Privacy Act 1988 (Cth)* (***the Act***) *with effect from 23 February 2018* introduce mandatory data breach notification provisions which all health service providers must comply with. "Health service" is broadly defined under s 6FB of *the Act*, and includes any service to assess, diagnose, or treat an illness, disability, or injury.

Part IIIC of the Act requires providers to notify the Office of the Australian Information Commissioner (***the OAIC***) and affected individuals when an *eligible data breach* occurs, ie, when they *suspect* that a data breach has occurred and there is a *real risk* of *serious harm* to individuals as a result of the breach.

HOW WILL THIS IMPACT MEDICAL PRACTICES?

Practices are increasingly storing personal and sensitive patient information electronically. It is important to note that under *the Act* practices are under an obligation to take reasonable steps to protect personal and patient information from loss and unauthorized access or disclosure. This includes taking reasonable steps to protect against possible data breaches, and ensuring the clinic can adequately respond should a data breach occur.

To meet these obligations, practices should:

(a) Review their information handling processes and policies and their storage and security systems to ensure they are able to comply with the mandatory data breach notification requirements of the Act:

(b) Prepare a data breach response plan: and

(c) Ensure that staff training covers the risks associated with handling patient data and the damage that can be caused by mishandling.

ELIGIBLE DATA BREACH

Eligible Data Breach is given the meaning provided by s 26WE(2) of *the Act*. An eligible data breach occurs when:

(a) There is unauthorised access to, or unauthorised disclosure of, information in circumstances where a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates; or

(b) Information is lost and unauthorised access to, or unauthorised disclosure of, information is likely to occur, and assuming unauthorised access or disclosure of the information were to occur, the access or disclosure is likely to result in serious harm to any of the individuals to whom the information relates.

Breaches may occur through data theft, hacking or by accidental loss or disclosure of information through internal errors or failure to follow policies.

SERIOUS HARM

If a reasonable person would conclude that the data breach is likely to result in serious harm, it is an eligible breach. "Serious harm" is not defined, but the Explanatory Memorandum indicates that it could include serious physical, psychological, emotional, economic and financial harm, or serious harm to reputation.

An assessment of serious harm should be undertaken holistically with regard to the relevant factors set out in s 26WG of *the* Act. Serious harm will be "likely" if such harm is more probable that not, having regard to:

- The kinds of information accessed/disclosed/lost
- The sensitivity of the information
- Whether the information is protected by security measures
- The person(s) or kinds of persons who obtained or could obtain the information

- The likelihood the person(s) will use the information to cause harm (the intention)
- The nature of the harm that may result.

It is worth noting that the above factors are not exhaustive, and that the sensitive nature of health information will almost always mean its unauthorized access or disclosure will result in serious harm.

SUSPECTED ELIGIBLE DATA BREACH

If a provider has reasonable grounds to suspect an eligible data breach may have occurred but cannot confirm this is so at the time, the provider has 30 days to take all reasonable steps to carry out a reasonable and expeditious assessment as to whether there are reasonable grounds to believe that the circumstances amount to an eligible data breach.

NOTIFICATION

If a provider has reasonable grounds to believe there has been an eligible data breach, and any serious harm cannot be mitigated through remedial action, the provider must prepare a statement which complies with s 26WK of *the Act* setting out:

a. The identity and contact details of the provider;

b. A description of the data breach that the provider has reasonable grounds to believe has occurred;

c. The kinds of information concerned; and

d. Recommendations about the steps which individuals should take in response to the data breach.

The statement must be provided to the OAIC and, if practicable, the provider must also notify the individuals to whom the information relates, or each of the individuals who are at risk of serious harm as a consequence of the data breach, of the contents of the statement.

If it is not practicable to contact the individuals, the provider must take reasonable steps to publicise the contents of the statement and must publish a copy on its website (if it has one).

EXCEPTIONS

A mandatory notification is not required to be made if the breach is required to be, and is, reported pursuant to the *My Health Records Act* 2012.

A mandatory notification is not required to be made if effective remedial action is taken before any serious harm is caused by the breach.