HealthLEGAL

www.healthlegal.com.au

March 2017 Edition

New data breach notification laws

By Giovanni Marino, Senior Solicitor

Introduction

The Privacy Act 1988 (Cth) (**Act**) has been amended by the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) (the **amending Act**).

The amending Act introduces a mandatory data breach notification regime where an 'eligible data breach' occurs.

The amendments will commence on 23 February 2018, unless they are proclaimed to commence earlier.

Who is required to comply with the new laws?

The new reporting regime will apply to 'APP entities' that hold personal information (those entities that must comply with the Australian Privacy Principles under the Act). In general, private health care organisations, including community health centres, and other private health providers will be considered APP entities. Public hospitals and health services in Victoria will not be considered APP entities.

The regime will also apply to certain credit reporting bodies and credit providers that hold credit reporting or credit eligibility information, and recipients of tax file number information.

What is an 'eligible data breach'?

An 'eligible data breach' occurs where:

- there is:
  - unauthorised access to, or unauthorised disclosure of, the information; or
  - there is loss of the information where unauthorised access or disclosure is likely; and
- a reasonable person would conclude that the access or disclosure would likely result in serious harm to any of the individuals to who the information relates.

These individuals to whom the serious harm would likely result are defined as being '**at risk**'.

'Serious harm' is not defined in the Act, but the Explanatory Memorandum to the amendments states that serious harm could include:

> … serious physical, psychological, emotional, economic and financial harm, as well as serious harm to reputation and other forms of serious harm that a reasonable person in the entity's position would identify as a possible outcome of the data breach.

What are the notification requirements?

If an organisation has reasonable grounds to believe that there has been an eligible data breach, then it must provide a statement to the Australian Information Commissioner (the **Commissioner**) which sets out matters including:

- the identity and contact details of the organisation;
- a description of the eligible data breach;
- the kind or kinds of information concerned; and
- recommendations about the steps that individuals should take in response to the eligible data breach.

As soon as practicable after preparing the statement for the Commissioner, the organisation must also take reasonable steps to notify the statement information to either:

- each individual to whom the information relates; **or**
- if not all these individuals are deemed to be 'at risk', only those affected individuals who are deemed to be 'at risk'.

The Explanatory Memorandum explains that:

> This discretion is intended to provide flexibility to respond to different kinds of eligible data breaches. For example, in some cases it may be impracticable for an entity to consider the circumstances of each affected individual to determine which individuals are at risk from an eligible data breach and which are not. In these circumstances notifying the entire cohort of affected individuals may be appropriate. In other cases it may be practicable for an entity to determine with a high degree of confidence that only some individuals from a broader group of affected individuals are at risk, meaning that notification to the broader group may not be necessary from a harm mitigation perspective.

The Commissioner may also direct an organisation to prepare a statement where the Commissioner has reasonable grounds to believe that there has been an eligible data breach. Prior to the Commissioner giving such a direction, the organisation will be invited by the Commissioner to make submissions to the Commissioner within a specified period.

What is required where an eligible data breach is suspected?

If an organisation has reasonable grounds to *suspect* that there *may* have been an eligible data breach, then it must carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the circumstances amount to an eligible data breach. If this is the case, then the notification requirements described above will apply.

The organisation must take reasonable steps to complete the assessment of the suspected data breach within 30 days.

Are there any exceptions to the data breach notification requirements?

There are certain exceptions to the notification regime, including where an organisation takes remedial action to address any unauthorised access to or disclosure of information, or loss of information, and:

- in relation to unauthorised access or disclosure – the remedial action occurs before there is any serious harm to any affected individuals to whom the information relates, and a reasonable person would conclude the access or disclosure would not likely result in serious harm to any of those individuals; or
- in relation to loss of information – the remedial action occurs:
  - before there is any unauthorised access to or disclosure of the information, and as a result of the action there is no unauthorised access or disclosure; or
  - after there is any unauthorised access to or disclosure of the information, but before the access or disclosure results in serious harm to any individuals to whom the information relates, and a reasonable person would conclude the access or disclosure would not likely result in serious harm to any of those individuals.

If multiple entities are holding the same information, and a single eligible data breach incident affects more than one entity, only one of the entities needs to comply with the notification regime in respect of the data breach.

Determining when access or disclosure will result in serious harm

The amending Act sets out a list of factors to consider in order to determine whether a 'reasonable person' would conclude access or disclosure of information will likely result in serious harm to affected individuals. These include:

- the kind or kinds of information;
- the sensitivity of the information;
- whether the information is protected by one or more security measures, and the likelihood that any of those security measures could be overcome;
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information;
- the likelihood that the persons who have obtained, or who could obtain, the information have the intention of causing harm to any of the individuals to whom the information relates;
- the nature of the harm; and
- any other relevant matters.

What happens if an organisation does not comply with the requirements?

Breach of the data breach notification requirements or the requirement to assess suspected data breaches are taken to be acts that are 'an interference with the privacy of an individual'.

Section 13G of the Act provides that a civil penalty applies to serious or repeated interferences with the privacy of an individual. An individual penalty of $360,000 and a maximum corporate penalty of $1,800,000 currently applies for breach of this provision.

Conclusion

Organisations should review their policies and procedures regarding data breaches, and prepare data breach response plans in line with the requirements of the amending Act (if these are not in place already).

The data breach response plans should contemplate potential remedial action to prevent any serious harm occurring to any affected individuals.

Organisations that hold or share data in collaboration with other entities or service providers may wish to establish processes to enable a coordinated response to any data breach.

*If you have any questions arising out of this article, please contact **Giovanni Marino** on **(03) 9865 1339** or email **giovanni.marino@healthlegal.com.au**.*