Mandatory Reporting in Healthcare

Reading time:
Jayson Nagpiing
Date created: 03/12/2020

Tags: Article | Medico-Legal | Medical Practitioner | Practice Risk Management

The Privacy Amendment (Notifiable Data Breaches) Bill 2016 places further obligations on healthcare practitioners to report data breaches causing 'serious harm' to the Office of the Australian Information Commissioner (OAIC).

The key things that healthcare practitioners need to be aware of are:

Practices/practitioners need to notify patients and the Privacy Commissioner (OAIC) as soon they become aware of a data breach or lost data likely to result in serious harm.

Failure to make notifications may result in fines of up to $360,000 for individuals and $1.8 million for organisations.

Under the law, a data breach must be notified where there is a likely risk of serious harm to any of the affected individuals as a result of the breach, that is unauthorised access or disclosure, or the loss of data. For example, if hackers have acquired data records of patients that would be sufficient information to commit identity fraud.

Contemporary medical and dental practices and other businesses are holding large amounts of personal information in electronic form. This has raised the risk of security breaches and misuse of the data including identity theft. This has prompted the Government to seek to tighten regulation and reduce the risk of serious data breaches.

In prior submissions concerns about the nature of mandatory notifications for the healthcare sector and the potential burden this places on healthcare practitioners and their practices were raised.

The key obligations for practitioners and other individuals/businesses are:

- 'Eligible data breaches' must be notified to the Privacy Commissioner as soon as reasonably practicable
- A copy of the statement must be provided to the individuals affected (ie the individual's whose information was disclosed, accessed or lost), if practicable.
- If the above is not practicable then a statement must be published on the business's website and steps taken to publicise the content.

Practitioners will need to identify when a data breach could cause 'serious harm'. This is likely to be key in working out if a data breach is notifiable. For example, if a practitioner accidentally shared a patient's medical data with their spouse but neither the patient nor the spouse were concerned and it was known they readily shared medical information, it may be reasonable to assume that serious harm was unlikely therefore a breach report not required.

The new laws under the Privacy Amendment (Notifiable Data Breaches) Bill 2016 are in addition to the current Australia, mandatory data breach notification requirements which apply in the event of unauthorised access to certain eHealth information under the My Health Records Act 2012. Under the My Health Records Act, certain participants such as a registered healthcare provider (eg GP or dental practice) are required to report data breaches that occur in relation to the eHealth record system to the Office of the Australian Information Commissioner (OAIC) and the system operator.

Failure to report a data breach can result in penalties under the My Health Records Act including civil penalties of up $21,600 for individuals, $108,000 for corporations and potentially a criminal penalty of up to two year's imprisonment.

Under the new Act, penalties for failure to comply with obligations may increase to 360,000 for individuals or up to $1.8m for corporations.

Further reading