Mandatory data breach notification requirements for medical practice

Mandatory notification laws bring stiff penalties for failures to meet requirements of the notification scheme

The Australian Government has introduced new mandatory disclosure rules, which came into force in February 2018, requiring most health and medical providers to notify patients or others affected when there is a serious data breach that results in unauthorised access to personal information. With fines of up to $420,000 for individuals and far higher fines for businesses that fail to report serious data breaches, the mismanagement of a breach by a medical practice will potentially be very serious.

With the current scheme, early data show that health care organisations are responsible for almost one-quarter of data breach reports, while just over 50% of all reported breaches are due to human error. These results underscore the importance of the scheme for health care practitioners and practices, as well as the central role internal systems and staff play in combatting the risk of a data breach.

The new law: breaches and notification

There are a number of potential causes of a data breach; these include malware, disgruntled employees, lax systems, and human error. The costs of data breaches are significant, with the average cost of a data breach to an Australian organisation reaching $2.51 million or $139 per compromised record in 2017, and a survey by the Office of the Australian Information Commissioner (OAIC) indicating that six in ten (58%) Australians would avoid dealing with private enterprises because of privacy concerns.

The new law, the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) amends the Privacy Act 1988 (Cth) such that, when an entity that is subject to the Privacy Act believes that there may have been an eligible data breach, that entity must take steps to notify both the OAIC and the individuals who may suffer serious harm because of the breach. Private medical practices, health services and aged care providers are all subject to this new mandatory data breach notification regime.

The new law applies to electronic and to non-electronic data that contain personal information. This means that the notification requirements apply if electronic or hard copy medical records, diagnostic reports, financial or other records are compromised or disclosed in some way.

The new obligations: key features

The new law applies whenever there is unauthorised access, unauthorised disclosure, or a loss of information (section 26WE(2)(a)-(b)). Unauthorised access occurs when anyone accesses personal information without authorisation. Unauthorised disclosure occurs when personal information becomes accessible to others outside the practice and the information is removed from the effective control of the practice. A loss occurs when data are lost and unauthorised access to or unauthorised disclosure of the information is likely to occur.

The crux of the new law is its assessment and notification requirements. If a practice has reasonable grounds to suspect that there has been a breach, it must undertake an assessment of the potential breach (within 30 days). When a practice has reasonable grounds to believe (but may not necessarily know) that there has been a breach, it must notify the OAIC and all individuals affected by the breach when a reasonable person would conclude that a data breach is likely to cause serious harm to any of the affected individuals. Serious harm is not limited to physical harm but includes serious psychological, emotional, economic and financial harm, as well as serious harm to reputation.

In the case of a notification, a practice must compile a statement regarding the breach, which must contain particular pieces of information, including a description of the kinds of information that may have been accessed, disclosed or lost and recommendations regarding steps individuals should take in response to this breach. This statement must be provided to both the OAIC and the individuals affected by the breach as soon as practicable.

Implications of the new law

The new law requires practices to exercise vigilance, instituting proactive measures to ensure that they reduce the risk of a breach and can respond in a timely manner. Practices must now follow specific processes should they suspect a breach has occurred, with a failure to do so being the cause of possible reputational damage, the breakdown of established clinical relationships, risk to the business and potential fines.

As with many areas of practice management, ensuring that the fundamentals are in place will make a material difference to the practice’s risk of causing a breach and of
its ability to respond to it. On this front, there are two key areas of work. The first relates to the practice itself, while the second relates to patient relationships.

Within the practice, reasonable steps must be taken to prevent employees from disclosing information to unauthorised third parties or from accessing information they do not have authorisation to access. Being clear about roles and responsibilities for information management in the practice, supported by clear policies and procedures, remains the foundation of good information security, which includes:

- managing access within the practice;
- ensuring that only those who are trained and authorised have access to clinical and financial information;
- using and updating effective passwords;
- establishing clear protocols for the use of email and transmission of information; and
- managing storage and destruction of hard copy and electronic records.

The same applies to third parties (eg, IT support), with contracts and confidentiality agreements needed to govern access and responsibilities. The Royal Australian College of General Practitioners’ computer and information security standards provide well established processes and templates for review and implementation of these practices.7

As to patients, forming and maintaining good information management relationships with patients is an often overlooked strategy. Ensuring that patients are informed about the practice’s information management efforts, that they can see those efforts in evidence when they visit and consent to the collection and use of information, and that agreement is reached about the use of their information will provide an excellent foundation for managing a data breach should one occur. Explicit conversations play a role here. For example, discussing the use of email communication between the practice and patients and explicitly recording their consent to the use of this mode of communication at the outset sets realistic expectations for patients surrounding security, informs them of practice staff who have access to their email correspondence and sets boundaries about what the practice is prepared to use unsecured email correspondence for and in what circumstances based on information security, clinical and business priorities.

Case after case of data breach in health care is caused by violation of these most basic good practices, which often result in minor breaches related to a single person, rather than large scale, catastrophic breaches. However, minor breaches can still cause serious harm and, thus, may still require notification to the OAIC and patients concerned. In light of the significant damage that data breaches can cause to practices and patients, if a practice suspects or believes a breach may have taken place, it should promptly engage relevant assistance.

Legal advice, cybersecurity providers, indemnity insurers, related entities (eg, diagnostic services providers or health services that may be also affected) and the OAIC itself will likely be suitable avenues for notification and collaboration.

Importantly, the new law encourages rapid action in the event of a breach. An exception to the notification requirement has been built into the new law so that rectifying a breach when it occurs — so that it is unlikely to cause serious harm — will mean that a breach is deemed never to have occurred and no notification is required. This is a clear signal to practices that the law aims to ensure information remains secure, rather than punishing breaches. However, this also reinforces the need for well established systems: only practices with systems already in place will be able to rapidly rectify a breach and to achieve this reduction of clinical and business risk in the process.

Limitations and challenges for medical practice

There are some advantages to the new law. For one, it assists in understanding a medical practitioner’s existing duty found in section 3.4 of the Good Medical Practice code of conduct to safeguard the confidentiality and privacy of patient information.9 However, there will be time and training costs for practices that are yet to establish suitable systems for data management and breach. Over time, the law will also change the expectations of patients, as breaches that are unable to be rectified will be made public. Health services providers are currently the organisations most trusted to look after personal information in Australia — a status that will have to be maintained by diligent and proactive work.

A major challenge remains the effective control of information that is legitimately transmitted outside of the practice. The high profile case of the 1600 letters found dumped in an apartment complex rubbish bin demonstrates this issue.10 They were dumped there by an employee of a subcontractor who was to provide transcription and mailing services for the health service concerned. This breach was caused by someone over whom the health service had very little effective control, and who was quite unrelated to the practitioners who had dictated those letters. And yet, it was the health service itself that had to work to rectify the issue and it was the clinical relationships of those practitioners that were placed at risk. The law cannot prevent every breach. However, by establishing well functioning internal procedures — such as those described in the Royal Australian College of General Practitioners’ computer and information security standards — and by informing patient expectations as to how their information is treated and by whom, the aftermath of a breach such as this might well be reduced in severity, especially as regards patient–doctor relationships.

Competing interests: Samuel Hartridge is an in-house counsel to ParaFlare, a cybersecurity company.

Provenance: Not commissioned; externally peer reviewed.

© 2018 AMPCo Pty Ltd. Produced with Elsevier B.V. All rights reserved.

References are available online at www.mja.com.au.
1 Privacy Act 1988 (Cth); “Notification of Eligible Data Breaches” Part III C (ss 26WA-26WT); “Civil Penalties” ss 80W, 15G; “Enforcement powers of the Office of the Australian Information Commissioner” ss 33E, 33F, 52, 55A, 62, 98, 80W.


