Notifiable data breach scheme

Reading time:
Jayson Nagpiing
Last Modified on 30/05/2024

Tags: Article | Medico-Legal | Medical Practitioner | Dental Practitioner | Risk Education

When running your own practice or working in a dental or medical practice, it is important to ensure you are using secure electronic communication to protect the data of your patients. As technology progresses, the need for strong data management has become essential in the running of a practice.

The Law has changed

As of 22 February 2018, new legislative requirements under the Federal Government's Notifiable Breaches scheme came into effect. The aim of this was to outline new standards of accountability and transparency to protect individuals'; personal information. As a practice you have access to patient records and private information and this information must be protected.

The scheme stipulates that any entity subject to the Privacy Act 1988 with an annual turnover of more than $3 million is required to notify individuals if their personal data has been involved in a serious breach. For those who don't comply, the fines are up to $420,000 for individuals (serious or repeated interference with privacy) and up to $2.1 million for corporations.

As with any personal data and information breaches, the accidental release of people's health records and Medicare card information can cause ‘serious harm’, ruin reputations and cause distrust of that organisation.

Harm can include psychological, emotional, physical, reputational or other forms of harm and ‘requires an objective assessment, determined from the viewpoint of a reasonable person in the entity's position.

Here are some key points from the Office of the Australian Information Commissioner - OAIC on the Notifiable Data Breaches Scheme

What is a data breach?

A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. An individual has the potential to be placed under serious harm as a result of a data breach or your practice has not been able (or has not acted swiftly) to prevent this serious harm.

Examples of a data breach include when:

- a device containing customers personal information is lost or stolen
- a database containing personal information is hacked
- personal information is mistakenly provided to the wrong person

The type or types of personal information involved in the data breach

Some kinds of personal information may be more likely to cause an individual serious harm if compromised. Examples of the kinds of information that may increase the risk of serious harm if there is a data breach include:

- sensitive information such as information about an individual's health
- documents commonly used for identity fraud (including Medicare card, driver licence, and passport details)
- financial information

- a combination of types of personal information (rather than a single piece of personal information) that allows more to be known about the individuals the information is about.

Steps to take if a data breach occurs

There are three options for notifying affected individuals:

- Notify all individuals whose personal information was involved
- Notify only those who are at likely risk of serious harm; or
- If direct notification is not practicable: publish the notification, and take reasonable steps to publicise it.

Notification can be via your normal methods of communication.

The faster an entity responds to a data breach, the more likely it is to effectively limit any negative consequences. A data breach response plan is essential to facilitate a swift response and ensure that any legal obligations are met following a data breach.

An effective data breach response generally follows a four-step process — contain, assess, notify, and review.

My Health Record system data breaches

Certain participants in the My Health Record system (such as the System Operator, a registered healthcare provider organisation, a registered repository operator, a registered portal operator or a registered contracted service provider), are required to report data breaches that occur in relation to the My Health Record system to either the System Operator or the Commissioner, or both, depending on the entity reporting the data breach (s 75 of the My Health Records Act). If a data breach has been, or is required to be, notified under s 75 of the My Health Records Act, the NDB scheme does not apply (s 26WD). This exception is intended to avoid duplication of notices under the NDB scheme and the data breach notification requirements in the My Health Record system.

Information about data breach notification requirements of the My Health Records Act is available in the OAIC's Guide to mandatory data breach notification in the My Health Record system.

Only notifications under s 75 of the My Health Records Act fall within this exception. Notifications under other schemes such as that within the National Cancer Screening Register Act are not excluded from the NDB scheme.

Example

A practice manager who has access to the My Health Record system for administrative purposes only, accesses a patient's My Health Record clinical information without authorisation. The GP discovers this incident and immediately notifies the System Operator and the Commissioner as required under s 75 of the My Health Records Act. There is no need to also notify this data breach under the Privacy Act.

At or about the same time, the practice manager also accesses the GP's clinical database (not part of the My Health Record system), and downloads their ex-partner's health information without authorisation. Upon discovering this incident, the GP takes immediate steps to contain the breach and, due to the nature of the relationship between the practice manager and the patient, decides there is a likelihood of serious harm to the patient in the circumstances. The GP notifies the patient and the Commissioner about the data breach, as required under the Privacy Act's NDB scheme.

Maintain information governance and security — APP 1 and 11

Entities have an ongoing obligation to take reasonable steps to handle personal information in accordance with the APPs. This includes protecting personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

Suspected or known data breach

A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that an entity holds.

Contain

An entity's first step should be to **contain** a suspected or known breach where possible. This means taking immediate steps to limit any further access or distribution of the affected personal information, or the possible compromise of other information.

Assess

Entities will need to consider **whether the data breach is likely to result in serious harm** to any of the individuals whose information was involved. If the entity has reasonable grounds to believe this is the case, then it must notify. If it only has grounds to suspect that this is the case, then it must conduct an **assessment** process. As part of the assessment, entities should consider whether **remedial action** is possible.

Organisations can develop their own procedures for conducting an assessment. OAIC suggests a three-stage process:

- **Initiate:** plan the assessment and assign a team or person
- **Investigate:** gather relevant information about the incident to determine what has occurred
- **Evaluate:** make an evidence-based decision about whether serious harm is likely. OAIC recommends that this be documented.

Entities should conduct this assessment expeditiously and, where possible, within 30 days.

If it can't be done within 30 days, document why this is the case.

Take remedial action

Where possible, an entity should take steps to reduce any potential harm to individuals.

This might involve taking action to recover lost information before it is accessed or changing access controls on compromised customer accounts before unauthorised transactions can occur.

If remedial action is successful in making serious harm no longer likely, then notification is not required and entities can progress to the review stage.

NO — Is serious harm still likely? — **YES**

Notify

Where **serious harm is likely**, an entity must prepare a statement for the Commissioner (a form is available on the Commissioner's website) that contains:

- the entity's identity and contact details
- a description of the breach
- the kind/s of information concerned
- recommended steps for individuals

Entities must also notify affected individuals, and inform them of the contents of this statement. There are three options for notifying:

- **Option 1:** Notify all individuals
- **Option 2:** Notify only those individuals at risk of serious harm

If neither of these options are practicable:

- **Option 3:** publish the statement on the entity's website and publicise it

Entities can provide further information in their notification, such as an apology and an explanation of what they are doing about the breach.

In some limited circumstances, an exception to the obligation to notify the Commissioner or individuals may apply.

Review

Review the incident and take action to prevent future breaches. This may include:

- Fully investigating the cause of the breach
- Developing a prevention plan
- Conducting audits to ensure the plan is implemented
- Updating security/response plan
- Considering changes to policies and procedures
- Revising staff training practices

Entities should also consider reporting the incident to other relevant bodies, such as:

- police or law enforcement
- ASIC, APRA or the ATO
- The Australian Cyber Security Centre
- professional bodies
- your financial services provider

Entities that operate in multiple jurisdictions may have notification obligations under other breach notification schemes, such as the EU General Data Protection Regulation.

Notifiable data breaches flowchart

Related articles

CAREER LEADERSHIP PROGRAM >