Avant factsheet:

Notifying a data breach under the Notifiable Data Breach Scheme

Data breach notification under the Notifiable Data Breaches Scheme

From 22 February 2018, organisations covered by the *Privacy Act 1988* are required to notify individuals likely to be at risk of serious harm because of a data breach, and to notify the Office of the Australian Information Commissioner (OAIC).

Notification is one part of the process of responding to a data breach. For more information, see Avant's privacy and data breach guides.

If you have:

1. identified that a data breach has occurred in your practice; and
2. determined that it needs to be notified under the Notifiable Data Breaches Scheme [see Avant's notifiable data breach scheme decision-making flowchart]

you must provide a statement to the OAIC and notify individuals at risk of serious harm from the breach about the contents of the statement.

Why do I need to notify about a data breach?

The aim of notifying individuals about the data breach is to ensure they can take steps to protect themselves from harm, including identity theft and fraud. For example, this might include cancelling and replacing credit cards or Medicare cards if these have been compromised. Individuals may also need to protect themselves if their address details were disclosed.

What information does the statement need to contain?

The OAIC has a form on its website that you can complete. The form is also a good prompt for assessing the data breach and considering the steps affected individuals should take in response to the breach. You can complete and submit the form online. If you are unable to do this, for example because your IT systems have been compromised by a breach, there is also a Word version of the form available. Alternatively, you can contact the OAIC (details below).

The OAIC also provides guidance on what to include. The details of what is required are not included in the form, so check you understand what each field requires:

Identity and contact details for your organisation	Include the name most familiar to your patients (e.g. your practice is owned by Smith Pty Limited but is called City Medical Practice – include both names in the notification).
Description of the data breach	Provide enough information to allow individuals to properly assess the possible consequences of the data breach for them and to take action in response. This might include the date of the breach, when it was detected, what happened (e.g. known causes of the breach), who is likely to have obtained or accessed the information and what steps you have taken to contain the breach.
Kind or kinds of information involved in the breach	Consider whether the information is sensitive information, for example personal health information, patient contact information, Medicare numbers or financial information.
What steps you recommend individuals should take in response to the data breach	Consider what practical steps individuals could take. For example, if Medicare numbers are involved, advise individuals how they can cancel their card and obtain a new one.

Who needs to notify?

If more than one organisation is involved in the breach, only one organisation needs to prepare the statement and notify individuals about the breach. The statement may include the name and contact details of the other organisation(s) involved if that would help affected individuals.

When do I notify?

You need to notify individuals and the OAIC 'as soon as practicable' after becoming aware of the breach. What is considered practicable will depend on the type and extent of the breach, but it should not be more than 30 days as this is the maximum time allowed to assess a suspected breach to determine if it is notifiable.

The Commissioner can also direct you to prepare a statement and notify individuals if the Commissioner becomes aware there has been an eligible data breach. You must comply with such a direction.

How do I notify affected individuals?

You have three options:

- notifying all individuals to whom the information relates
- notifying only those individuals likely to experience serious harm as a result of the breach
- if neither of these two options is practicable, publish the notification.

You will need to make a prompt decision about which option you will use. You can notify individuals before or at the same time you notify the OAIC.

You should notify the individual in the way you usually communicate with them, or by any reasonable method. This might include a telephone call, SMS, physical mail, social media post or in person.

If it is not practicable to notify individuals directly, you must publish your statement on your website and take active steps to publicise its contents. You could do this by:

- announcing it on your practice's website and social media channels (if you have any)
- ensuring your website can be located via search engines
- placing a print or online advertisement in a publication likely to reach affected individuals.

What happens when the OAIC receives my statement?

While the primary aim of the data breach notification regime is to ensure affected individuals are notified so they can take steps to prevent harm, one consequence of the regime is the OAIC will be alerted to a breach that may be an interference of privacy under the Privacy Act, and for which action can be taken.

The Commissioner will decide whether or not to take any action when they receive a data breach notification.

If the notification suggests a possible breach of the privacy legislation, the Commissioner may:

- make preliminary inquiries to determine whether to investigate the breach
- offer advice and guidance in response to a notification, including how best to respond to the breach and prevent similar incidents in the future.

In exceptional cases, the Commissioner may make a declaration that an organisation does not need to comply with notification requirements in certain circumstances – if it is in the public interest.

What happens if I don't comply with the data breach notification requirements?

The OAIC has stated it will take an educative approach to compliance with this and other privacy obligations. Nevertheless, the OAIC can take enforcement action against you if you do not do any of the following:

- carry out an assessment of a suspected breach
- prepare a statement about an eligible data breach and give it to the OAIC
- notify affected individuals of the contents of the statement
- comply with a direction of the Commissioner to notify the eligible data breach.

Are there any circumstances in which I don't need to notify?

There are some situations in which you don't need to notify a breach that would otherwise be notifiable. These include:

- enforcement-related activities – where notification by an enforcement body such as the police, a crime commission or other enforcement agency would be likely to prejudice an enforcement-related activity
- inconsistency with secrecy provisions (where a Commonwealth law prohibits or regulates the use or disclosure of information)
- declarations by the Australian Information Commissioner that an entity does not need to comply with the legislative requirements. This is only likely to be done in exceptional circumstances when the risks outweigh the benefits of notifying individuals at risk of serious harm

What if the breach involves My Health Record information?

There are separate requirements for data breaches involving My Health Record. See the OAIC's Guide to mandatory data breach notification in the My Health Record.

Resources

Avant notifiable data breach flowchart (downloadable pdf)

Notifying individuals about an eligible data breach (December 2017)

What to include in an eligible data breach statement (December 2017)

Notifiable data breach form (complete this form online)

Guide to OAIC Privacy Regulatory Action – Chapter 9: Data breach incidents (currently in draft)

Office of the Australian Information Commissioner

Phone: 1300 363 992

enquiries@oaic.gov.au