



Navigating the New Data Breach Management Requirements

May 2018

Magali De Castro
Clinical Director, HotDoc

Navigating the New Data Breach Management Requirements

This session will cover:

- What constitutes a data breach
 - What are the responsibilities of the practice in terms of data breach management
 - How to prepare a response plan and create a practice policy that complies with the Notifiable Data Breach Scheme
-



What is the new notifiable data breach scheme?

- On 22 February 2018, new privacy laws came into effect to regulate reporting and notification of *eligible data breaches*.
- The scheme includes *non-compliance fines* of up to \$420,000 for individuals and up to \$2.1 million for corporations.
- Practices will need to develop their own *procedures for assessing and dealing with a suspected data breach*.
- This means reviewing procedures and systems for *securing personal information and training staff* on how to comply with these new requirements.

What is a Notifiable Data Breach (NDB)?

An eligible data breach arises when the following three criteria occur:

1. There is **unauthorised access** or unauthorised **disclosure** of personal information, or a **loss** of personal information that a practice holds
2. This is **likely to result in serious harm** to one or more individuals
3. The practice has **not been able to prevent the likely risk of serious harm with remedial action**



What is serious harm?

Issues to consider when deciding if the data breach could result in serious harm:

- **Type of information:** information about an individual's health is considered to be 'sensitive information' that may increase the risk of serious harm
- **Circumstances** of the data breach – whose information was involved, the number of individuals, whether the information was encrypted
- **Nature of the harm** that may result– such as humiliation, damage to reputation or relationships, threats to an individual's safety



Data breach examples



Data breach instances may include:

- A database containing medical records is hacked (e.g. cyber-attack)
- Health information is mistakenly provided to the wrong person (e.g. test results being sent to the wrong patient)
- A device containing patients' medical records, such as a laptop or hard drive, is lost or stolen
- Inappropriate disclosure of health information to a family member or friend
- Viewing of health records by unauthorised practice staff members or contractors
- Inadequate steps to 'cleanse' or destroy information on computer hardware before it is disposed of
- Inadvertently placing health or other personal information on a publicly accessible website.



Consequences of a data breach

Data breaches can cause harm in multiple ways:

- Harm to the affected person's physical or mental well-being
- Financial loss or fraud
- Identity theft causing financial loss or emotional and psychological harm
- Family violence
- Physical harm or intimidation (e.g. blackmail, discrimination, etc.)

Consequences of a data breach

Harm to the practice

A data breach can also negatively impact a practice's reputation which can have short and long-term implications on the practice's business viability.

To minimise the risk of harm to affected individuals:

- Demonstrate accountability (transparency) in your data breach response
- Act quickly so individuals may take steps to reduce their risk of harm
- Make changes to prevent data breaches from occurring in the future and communicate these changes

Preparing the practice

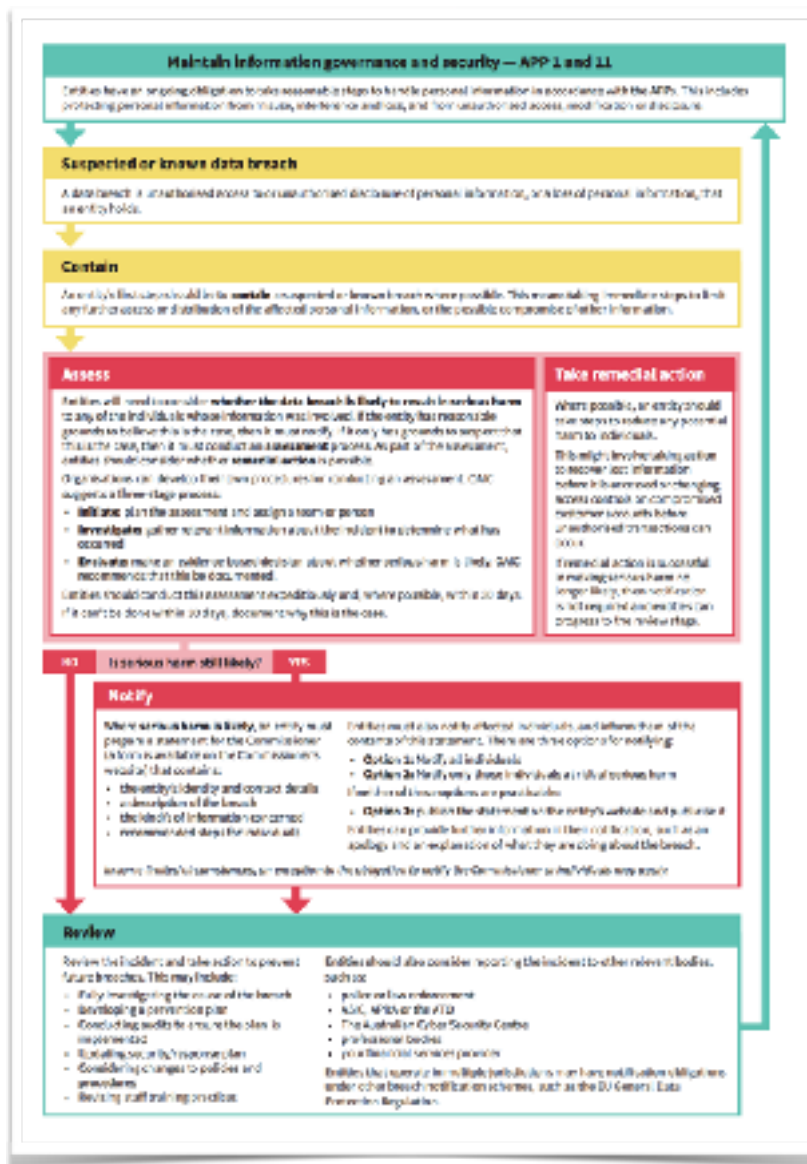
- Review current information security practices, procedures and systems:
 - Ensure all **security software and controls are up to date**
 - **Remove accesses from people who no longer require high level access to sensitive information**
- **Prepare a data breach response plan** so your team can respond quickly to suspected data breaches
- Provide **training to staff** so they are able to identify and respond to data breaches.



Creating a data breach response plan

- A data breach response plan *sets out the roles, responsibilities and steps* involved in managing a data breach.
- Should be *in writing* and include:
 - Clear explanation of **what constitutes a data breach**
 - Strategy for **containing, assessing and managing** data breaches
 - **Immediate communications strategy** for the prompt notification of affected individuals and other relevant entities
 - **Who staff should inform** immediately if they suspect a data breach
 - **How your practice will record** data breach incidents
 - **Your review process** to identify and address any weaknesses in data handling that contributed to the breach

What to do in the event of a data breach:



The One-page flowchart available from OAIC (Office of the Australian Information Commissioner):

<https://www.oaic.gov.au/resources/privacy-law/privacy-act/notifiable-data-breaches-scheme/flowchart.pdf>



Responding to data breaches

There is no single way of responding to a data breach. Each breach will need to be dealt with on a case-by-case basis,

Generally, you should follow four key steps after a data breach:

- Step 1: **Contain the data breach to prevent any further compromise** of personal information.
- Step 2: **Assess** the data breach by gathering the facts and **evaluating the risks**, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.
- Step 3: **Notify individuals and the Commissioner** if required. If the breach is an 'eligible data breach' under the NDB scheme, it may be mandatory for the entity to notify.
- Step 4: **Review** the incident and consider **what actions** can be taken to **prevent future breaches**.

Notifying affected individuals

If there are reasonable grounds to believe an *eligible data breach has occurred*, you must *notify the individuals* at risk of serious harm *and the OAIC* (Office of the Australian Information Commissioner) as soon as practicable.

The notification must set out:

- Name and contact details of the practice
- A description of the data breach
- The kind of information involved in the data breach
- Recommendations about the steps that individuals should take in response to the data breach.



Insurance

Does your insurance protect against privacy/data breaches?

- Check with your insurance provided to make sure you are protected against unintentional privacy breaches.
- As well as cover for fines and penalties related to data breaches.



Case study 1



Unauthorised data access

A practice manager accesses the GP's clinical database, 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.

Outcome:

The GP notifies the patient and the Commissioner about the data breach, as required under the Privacy Act's NDB scheme.

Scenario source: <https://www.oaic.gov.au/resources/agencies-and-organisations/guides/data-breach-preparation-and-response.pdf>

Case study 2

Unintentional disclosure



A clinic introduces a new reminder system for appointments that includes sending a short text message to patients

The clinic has two patients with the same name and an appointment reminder is sent to the wrong patient

Outcome:

The patient's GP contacts their insurance provider and is advised to ***let the patient know*** that a reminder was sent to the wrong number and that this was an administrative error.

Because this is not likely to result in serious harm, this data breach ***does not require notification to the OAIC.***

Scenario source: <https://www.avant.org.au/news/mandatory-data-breach-notification/>

Case study 3



Theft of sensitive information

A GP downloads patient data to a laptop ready for a visit to a nursing home the following morning.

The data includes personal information about each patient including identification details such as Medicare numbers, contact details of family members, and personal medical details.

The GP makes a stop on the way to the nursing home and leaves the laptop locked in the car, however the laptop is not password protected.

The car is broken into and the laptop stolen.

Outcome:

Mandatory notification is required by the GP to the nursing home and all patients whose details were downloaded to the laptop about the theft.

This data breach would also require notification to the OAIC.

Scenario source: <https://www.avant.org.au/news/mandatory-data-breach-notification/>

Case study 3-B



Theft of sensitive information

A GP downloads patient data to a laptop ready for a visit to a nursing home the following morning.

The data includes personal information about each patient including identification details such as Medicare numbers, contact details of family members, and personal medical details.

The GP makes a stop on the way to the nursing home and leaves the laptop locked in the car, however the laptop *is password protected and the information is kept in a secure cloud-based service.*

The car is broken into and the laptop stolen. The GP immediately contacts their IT support service who is able to remotely revoke access to any sensitive information from that device and is able to confirm the data has not been accessed in the meantime.

Outcome:

Mandatory notification is not required because remedial action has successfully prevented unauthorised access of sensitive information.

Resources



Australian Government
Office of the Australian
Information Commissioner

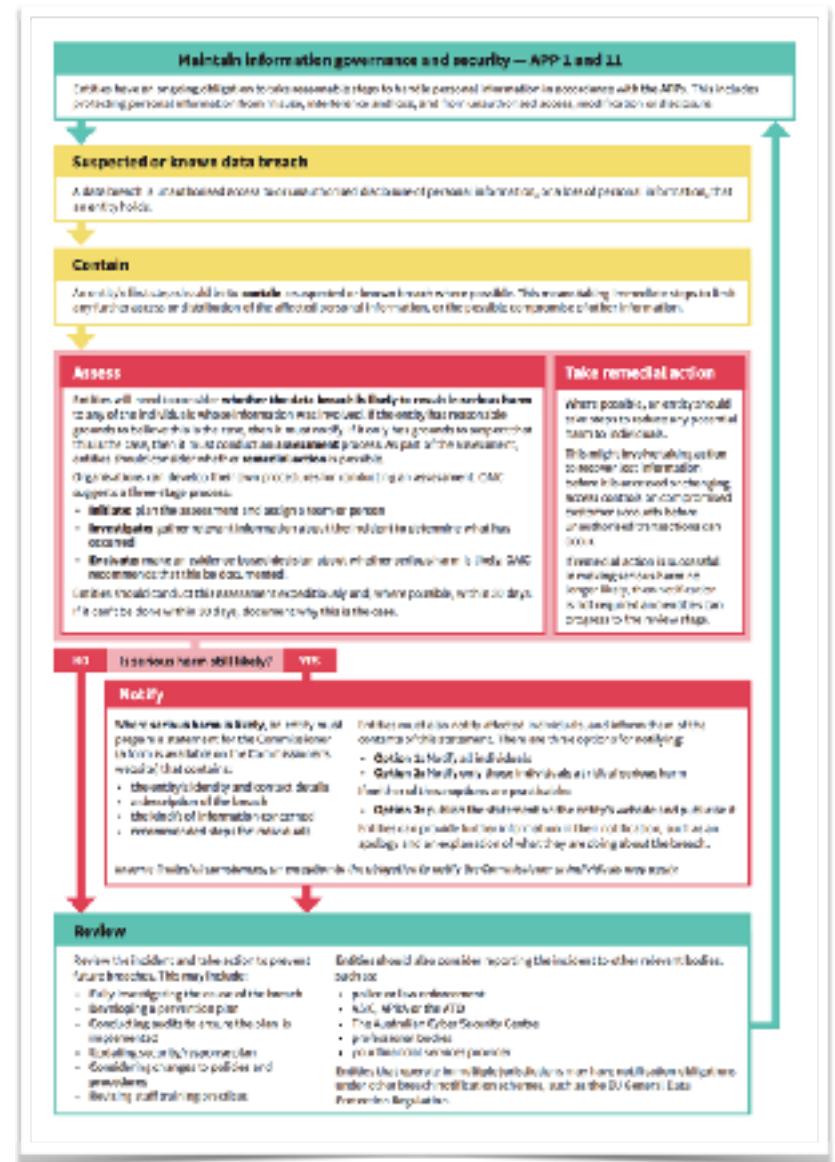
Data breach preparation and response

A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)


oaic.gov.au



February 2018



Resources



Australian Government

Business

business.gov.au

Form: Notifiable Data Breach Form

Description

You can use this form to notify the Office of the Australian Information Commissioner (OAIC) of an eligible data breach.

If you are unsure whether your entity has experienced an eligible data breach, you may wish to review the 'Identifying eligible data breaches' resource.

About this form

The OAIC uses the Australian Government's SmartForm service, which enables our forms to be lodged online using a personal computer or tablet. When you save or submit a form using this service, it is encrypted and stored on a secure server located in Australia and controlled by the Department of Industry, Innovation and Science (DIIS). Once you have submitted your completed form, we will download and decrypt it. Your form will then be permanently erased from the DIIS secure server.

Your personal information

For guidance on the personal information we collect and how we will handle your information, please contact the OAIC enquiries line on 1300 363 992 or see the OAIC [privacy policy](#).

You can view the DIIS privacy statement on the SmartForm service [here](#). Only the information under the heading 'SmartForm Service' applies to SmartForms.


Click the Complete Form button to access the notifiable data breach form.

[Complete Form](#)

Open a previously saved form

[Open Saved Form](#)

Service Provided By



Australian Government

Office of the Australian Information Commissioner

Office of the Australian Information Commissioner

Website: <https://www.oaic.gov.au>

Phone: 1300 363 992

Email: enquiries@oaic.gov.au

Notify via: <https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB>

Thank you for participating!

Got a question?
Email: md@hotdoc.com.au