# Data Breach Management Plan

Entities, including medical practices, have an ongoing obligation to take reasonable steps to handle personal information in accordance with the Australian Privacy Principles. 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.

The OAIC suggests organisations use the following 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.

These steps should be documented.

Our organisation 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.

## Is serious harm still likely?

### If yes: Notify

Where **serious harm is likely**, we must prepare a statement for the Commissioner (a form is available on the Commissioner’s website: <https://forms.business.gov.au/smartforms/landing.htm?formCode=OAIC-NDB> ) that contains:

• Our identity and contact details

• a description of the breach

• the kind/s of information concerned

• recommended steps for individuals

We 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

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

### If no: 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

We 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

## Key staff and contact details in the event of a suspected data breach:

Team leader/Data and privacy leader:

Supporting staff with data breach assessment responsibilities:

IT support and security provider: