Australian Government

Office of the Australian Information Commissioner

My Health Record data breach form

*Fields marked with * are required*

This form is used to notify the Australian Information Commissioner of a data breach where required under section 75 of the *My Health Records Act 2012 (Cth)* (**My Health Records Act**). For further information, reporting entities should review the Guide to mandatory data breach notification in the My Health Record system.

Who should use this form?

Entities with mandatory data breach notification obligations under the My Health Records Act:

- the My Health Record System Operator, the Australian Digital Health Agency (**ADHA**)
- registered healthcare provider organisations
- registered repository operators (**RROs**)
- registered portal operators (**RPOs**)
- registered contracted service providers.

What is a My Health Record data breach?

An entity must make a notification if it becomes aware that:

1. a person has, or may have, contravened the My Health Records Act in a manner involving an unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record; or
2. an event has, or may have, occurred (whether or not involving a contravention of the My Health Records Act) that compromises, may compromise, has compromised or may have compromised, the security or integrity of the My Health Record system; or
3. circumstances have, or may have, arisen (whether or not involving a contravention of the My Health Records Act) that compromise, may compromise, have compromised or may have compromised, the security or integrity of the My Health Record system.

When does a report need to be made?

A reporting entity must notify a data breach under the My Health Records Act when:

- it becomes aware that such a data breach has, or may have, occurred; **and**
- the data breach directly involved, may have involved or may involve the entity.

The reporting entity must make a notification as soon as practicable after becoming aware that a data breach has, or may have, occurred.

Who should the My Health Record data breach be reported to?

This will depend on the kind of entity:

- The System Operator must report a My Health Record data breach to the Information Commissioner.
- For other reporting entities, notification requirements differ depending on whether they are:
    - a state or territory authority or instrumentality of a state or territory. These entities may include public hospitals and health clinics wholly administered and funded by a state or territory:
        - these entities must report a My Health Record data breach to the System Operator but not the Information Commissioner. State and territory entities may also be required to comply with their local mandatory reporting schemes or choose to voluntarily report data breaches to their local privacy regulator in addition to reporting to the System Operator.
    - are **NOT** a state or territory authority or instrumentality of a state or territory. These entities may, for example, include private hospitals, general practitioner clinics and retail pharmacists:
        - these entities must report a My Health Record data breach to the Information Commissioner **and** the System Operator.

Completing the form

The appropriate amount of detail to include in the form will depend on the nature of the data breach. Where an entity identifies that a breach is minor, isolated or contained, it may be appropriate for the entity to focus on providing a brief overview of the breach, the consequences (if any) of the breach and the follow-up actions taken by the entity.

In contrast, where an entity identifies that a breach is serious, widespread or ongoing (for example, because the breach affects or potentially affects a large number of healthcare recipients, the effect of the breach is or is likely to be significant for the healthcare recipients, or the factors leading to the breach have not yet been identified or addressed), more detailed information will be required in the notification. The OAIC may need to contact you to seek further information.

Once completed, please send the form via email to MHR.Notifications@oaic.gov.au.

Your personal information

We will handle personal information collected in this form (usually only your name and contact details) in accordance with the Australian Privacy Principles.

We collect this information to consider and respond to your breach notification. We may use it to contact you.

More information about how the OAIC handles personal information is available in our privacy policy.

Entity details

You must complete this section

Entity name*

Phone *

Email *

Address Line 1 *

Address Line 2

Suburb *

State *

Postcode *

Other contact details (e.g. fax or international phone number or address)

Description of the potential or actual My Health Record data breach

You must complete this section

A description of the data breach outlining the confirmed or potential unauthorised collection, use or disclosure or threat to the security or integrity of the My Health Record system: *

Information involved in the potential or actual My Health Record data breach

You must complete this section

List the particular kind or kind(s) of personal information involved in the data breach: *

In addition, please select any categories that apply:

- ☐ Identity information
  (e.g. date of birth, Medicare number)
- ☐ Contact information
  (e.g. home address, phone number, email address)
- ☐ Health information
- ☐ Other sensitive information
  (e.g. Individual Healthcare Identifier, sexual orientation, genetic information, biometric information)

Breach details

Number of healthcare recipients whose personal information is involved in the potential or actual data breach:

Date the data breach occurred (or may have occurred):

You may provide your best estimate if the exact date is not known:

Date the entity became aware of the potential or actual data breach:

You may provide your best estimate if the exact date is not known:

Date the incident was assessed as a potential or actual data breach:

Best estimate if the exact date is not known:

What caused, or may have caused, the potential or actual data breach (including whether the breach was inadvertent or intentional and whether the data breach appears to stem from a systemic issue or an isolated trigger):

Are there any risks to individuals because of the data breach? If yes, advise the kind(s) of risks and whether any of these might be serious for any individual.

Has the data breach been contained?

☐ Yes ☐ No

Advise the steps that were or will be taken to contain the breach.

What action has been taken or is being taken to mitigate the effect of the data breach and/or prevent further breaches?

Other involved entities

If the data breach described above was also a data breach involving another entity, you may provide their identity and contact details.

Was another entity involved?

☐ Yes ☐ No

Please provide contact details for the entity:

Entity name

Phone

Email

Address Line 1

Address Line 2

Suburb

State

Postcode

Other contact details *(eg fax or international phone number or address)*

Notification

If the reporting entity is **not** the System Operator, has the reporting entity requested the System Operator notify all healthcare recipients that have, or may have, been affected?[1] Please note, if a significant number of healthcare recipients have been affected by the breach, the reporting entity must request that the System Operator also notify the general public.[2]

☐ Yes ☐ No ☐ N/A

If the reporting entity **is** the System Operator, have all healthcare recipients that have, or may have, been affected been notified?[3] Please note, if a significant number of healthcare recipients have been affected by the breach, the System Operator must also notify the general public.[4]

☐ Yes ☐ No ☐ N/A

[1] See section 75(5)(c)(i) and 75(6)(d)(i) of the My Health Records Act.
[2] See section 75(6)(d)(ii) of the My Health Records Act.
[3] See section 75(5)(c)(ii) and 75(6)(c)(i) of the My Health Records Act.
[4] See section 75(6)(c)(ii) of the My Health Records Act.

Additional information

Is there any other information you wish to provide at this stage, or any matters that you wish to draw to the OAIC's attention?

You can provide additional information below or attach supporting documents when you submit this form.

If you wish to provide further information or documents after you submit the form, you may email them to MHR.Notifications@oaic.gov.au.

Your contact details

Title

First name

Last name

Position title

Phone

Email

Review and submit

Please review the information that you have provided about the data breach.

Once you are ready to submit, please send the completed form by email to MHR.Notifications@oaic.gov.au.