



# My Health Record Data Breach Notification

## ABOUT THIS FORM

This form is intended for use by **reporting entities**, including organisations that are registered to participate in My Health Record as a healthcare provider organisation, contracted service provider, portal operator or repository operator.

Reporting entities must notify the Australian Digital Health Agency (the Agency), as system operator for My Health Record, of any actual or potential data breach. Data breach notifications must be submitted as soon as practicable after the reporting entity becomes aware that the breach has, or may have, occurred (regardless of whether or not the data breach has been confirmed).

A My Health Record **data breach** involves either (or both) of the following:

- unauthorised collection, use or disclosure of information in a person's My Health Record
- an event or circumstance that has (or may) compromise the security or integrity of the My Health Record system.

My Health Record data breach notification requirements are outlined in the *My Health Records Act 2012*. Further information is available on the [Australian Digital Health Agency website](#).

**i** Note: Data breaches that do not involve My Health Record may need to be handled in accordance with the Privacy Act 1988 [Notifiable data breaches scheme](#).

## ASKING THE AGENCY TO INFORM AFFECTED INDIVIDUALS

If a data breach **has** occurred, section 75(6)(d) of the *My Health Records Act 2012* requires the reporting entity to ask the Agency to notify all healthcare recipients affected by the data breach (and the general public if a significant number of healthcare recipients are affected).

If a data breach **may have** occurred, section 75(5)(c) of the *My Health Records Act 2012* requires the reporting entity to ask the Agency to notify all healthcare recipients that would be affected by the data breach, if there is a reasonable likelihood that the data breach has occurred and the effects might be serious for at least one healthcare recipient.

## NOTIFYING THE OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER

With some exceptions (see note below), reporting entities are also required to notify the Office of the Australian Information Commissioner (OAIC) of an actual or potential data breach. The OAIC will issue a data breach reference number, and a copy of this reference number should be provided to the Agency. For further information, and instructions on how to notify the OAIC, please visit the OAIC's [Report a My Health Record data breach](#) webpage and refer to the [Guide to mandatory data breach notification in the My Health Record system](#).

**i** Note: The requirement to notify the OAIC does not apply if the organisation is a state or territory authority or instrumentality, which are only required to notify the Agency (see sections 75(2)(c) and 75(2)(d)) of the *My Health Records Act 2012*). State and territory bodies may also be required to comply with mandatory reporting schemes for their jurisdiction or may choose to voluntarily report data breaches to their local privacy regulator in addition to reporting to the Agency.

## SUBMITTING THIS FORM

Please send the completed form by email to [MyHealthRecord.Compliance@digitalhealth.gov.au](mailto:MyHealthRecord.Compliance@digitalhealth.gov.au).

**i** Note: If some information is not yet available (for example, because your organisation has not yet concluded its investigations), you will need to provide this information once it becomes available.

## MY HEALTH RECORD DATA BREACH NOTIFICATION

## 1. ORGANISATION DETAILS

**Organisation Name****Health Provider Identifier–Organisation (HPI-O) Number**  
(if applicable and known)**Contact Name****Position****Address****Phone Number****Email Address**

## 2. DETAILS OF MY HEALTH RECORD DATA BREACH

**I am reporting that:** a data breach **has** occurred a data breach **may have** occurred**Description of the actual or potential data breach**

Please include details of any:

- contravention of the *My Health Records Act 2012*, involving suspected/actual unauthorised collection, use or disclosure of health information included in a healthcare recipient's My Health Record
- events/circumstances that compromise (or may compromise) the security or integrity of the My Health Record System.

**Date and time of the actual or potential data breach****Date:****Time:****Outline when and how you became aware of the actual or potential data breach**

<p><b>Type of information that was, or may have been, involved in the data breach</b></p>	
<p><b>Number of healthcare recipients that were (or may have been) impacted by the data breach</b> Please do not include personal details.</p>	
<p><b>Cause, or suspected cause, of the data breach</b> Please include details of whether the data breach was deliberate, malicious, inadvertent or intentional and whether it was caused by a systemic issue or an isolated situation.</p>	
<p><b>Any measures that were already in place to prevent the breach</b> For example, policies and procedures, user account management measures, training programs, cyber security controls etc...</p>	
<p><b>Steps taken to contain the data breach, and whether the breach has been contained</b></p>	

<p><b>Steps taken to mitigate the effects of the data breach and prevent similar breaches occurring in the future</b></p>	
<p><b>Any other entities involved in the data breach (where applicable)</b> Please provide details, including entity name(s) and outline how they are involved in the breach</p>	
<p><b>Any similar data breaches experienced by your organisation (where applicable)</b> Please provide details, including date(s), reference numbers and other relevant information</p>	
<p><b>Any other relevant information</b></p>	

**3. OAIC NOTIFICATION (PLEASE REFER TO OAIC NOTIFICATION REQUIREMENTS ON PAGE 1)**

<b>Has the OAIC been notified of the data breach?</b>	<input type="checkbox"/> <b>Yes</b> <input type="checkbox"/> <b>No</b> <input type="checkbox"/> <b>N/A</b> (The requirement to notify the OAIC does not apply if the organisation is a state or territory authority or instrumentality (see sections 75(2)(c) and 75(2)(d) of the <i>My Health Records Act 2012</i> ).
<b>OAIC data breach reference number</b> (if applicable)	
<b>Notification Date</b>	

**4. REQUEST TO NOTIFY AFFECTED INDIVIDUALS**

**i** Note: Only one option should be selected (A or B). Refer to the explanatory notes on page 1 for further information.

**A. Where a data breach has occurred:**

**Please confirm**

<input type="checkbox"/> <b>Confirm</b>	<p>A data breach has occurred, and in accordance with section 75(6)(d) of the Act, _____ requests that the Australian Digital Health Agency notify all healthcare recipients affected by the data breach.</p> <p>In addition to the above, if a significant number of healthcare recipients are affected, _____ that the Australian Digital Health Agency notify the general public.</p>
--	--

**i** Note: Where a data breach **has** occurred, it is a legislative requirement that the organisation must request the Agency (system operator) to notify affected healthcare recipients.

**B. Where a data breach may have occurred:**

**Please confirm**

Is it reasonably likely that a data breach has occurred and the effects might be serious for at least one healthcare recipient?

<input type="checkbox"/> <b>Yes</b> Therefore, in accordance with section 75(5) (c) of the Act, _____ requests that the Australian Digital Health Agency notify all healthcare recipients that would be affected by the data breach.	<input type="checkbox"/> <b>No</b> Therefore, no healthcare recipients are required to be notified (as section 75(5) does not apply).
--	---

**Contact details for provision to individuals affected by the data breach**

Please provide the contact details (name, position title, email address and/or phone number) of a person that affected individuals can contact if they wish to discuss the matter with your organisation. If this is another individual, please obtain consent before providing personal information.

**Where healthcare recipients are contacted, please note that these details will be provided to the healthcare recipient(s)**

**i** *Note: If details are the same as what is listed in section 1, above, write 'as above'.*

<b>Contact Name</b>	
<b>Position</b>	
<b>Phone Number</b>	
<b>Email Address</b>	

**Please sign and date this form on behalf of your organisation.**

I confirm that the information in this form is accurate and correct, based on information currently available. Where additional information comes to light through the course of managing this matter, I confirm that this information will also be provided to the Agency.

**Name:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**- END OF FORM -**

**Save the filled form.**



**Print the form.**

