# **Data Notification Guidance**

**Notification requirements**

There is an onus on a Healthcare Provider Organisation (HPO) or Organisation Maintenance Officer to notify the data breach related to My Health Record (MHR) to the Australian Digital Health Agency (ADHA) and the Office of the Australian Information Commissioner (OAIC). Notification should occur as soon as practicable after they have been notified or become aware of the breach.

**Examples of Privacy Breaches**

The misuse or unauthorised disclosure of information from a healthcare recipient’s MHR by persons authorised to access the MHR system via or on behalf of the HPO

Accidental disclosure of information contained in a healthcare recipient’s MHR

Possible or actual loss, destruction, theft or compromise of the HPO’s NASH PKI Certificate

Unauthorised access to the MHR system using the HPO’s clinical information systems

**Notifications Required**

Notification to ADHA and OAIC

‘Eligible data breach’ that leads to a ‘likely risk of serious harm’ requires HPO to notify ADHA and OAIC

Notification to the HPO’s insurer

Notification to the involved practitioner’s insurer by the practitioner

Additional notification requirements for practices may include:

* the HPO’s insurer
* the involved practitioner
* the practitioner’s insurer; and
* the OAIC.

If an HPO becomes aware that a data breach has occurred, it must undertake a preliminary assessment of the causer of the data breach, evaluate any risks related to the data breach, and take steps to prevent further similar data breaches.

To notify the relevant organisation(s) complete the [Data Breach Notification form](https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB) and submit the information to the Australian Digital Health Agency and/or the OAIC.

**Data Breach Notifications**

**Office of the Australian Information Commissioner**

To notify the OAIC of a data breach, complete the [Notifiable Data Breach form](https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB) available on the OIAC website.

For enquiries, phone 1300 363 992.

**The Australian Digital Health Agency**

To notify the My Health Record System Operator (the Australian Digital Health Agency), email [myhealthrecord.compliance@digitalhealth.gov.au](about:blank) with the details below.

|  |  |
| --- | --- |
| Description of the breach | *Outline the suspected unauthorised collection, use or disclosure, or the event or circumstance* |
| Date and time of the breach | *When was the breach? When was the breach discovered?* |
| Cause of the data breach |  |
| Type of information involved in the data breach |  |
| Number of healthcare recipients that were or may have been affected |  |
| Has the data breach been contained? |  |
| What action has been taken or is being taken to mitigate the effects of the data breach and/or prevent further data breaches? |  |
| Name and contact details of appropriate person within the entity |  |
| Other relevant factors or comments |  |