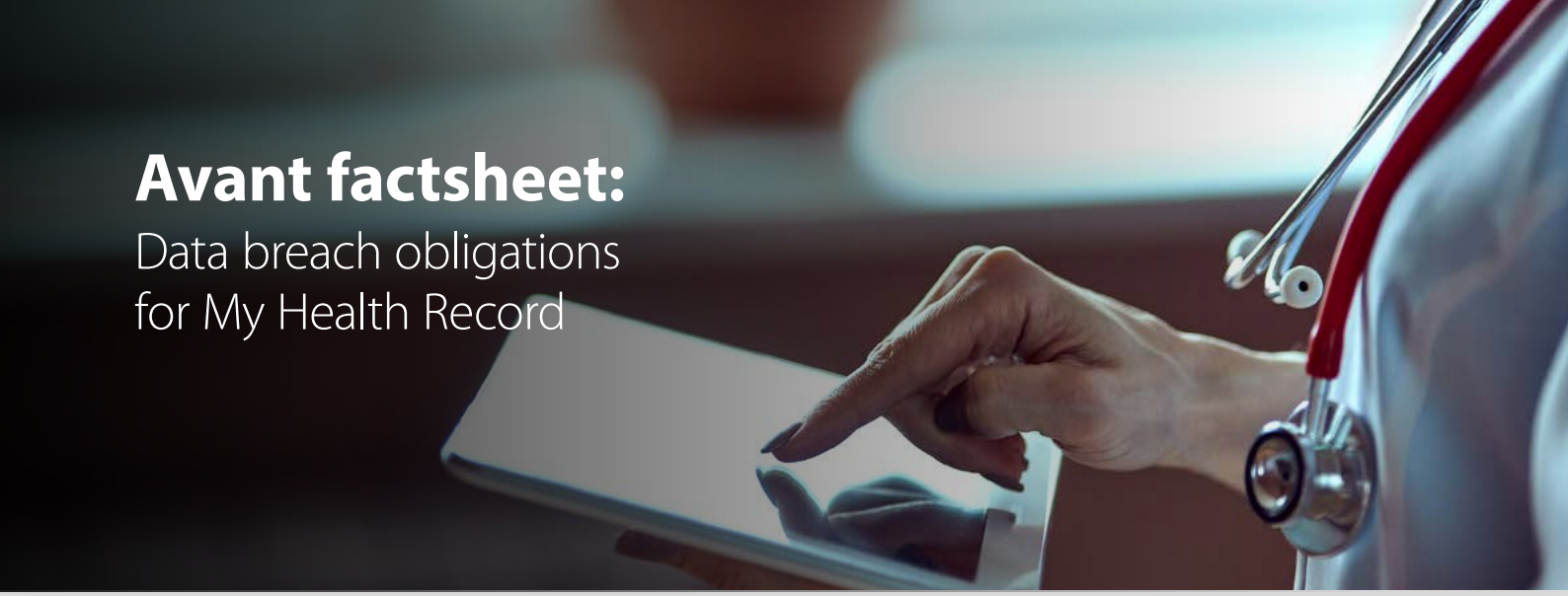

Avant factsheet:
Data breach obligations for My Health Record

If you are using the My Health Record (MHR) in your practice, your practice must notify the Australian Digital Health Agency (the MHR system operator) and the Office of the Australian Information Commissioner (OAIC) of certain data breaches relating to the MHR.

This is separate from your obligations under the Privacy Act. Your obligations under the My Health Record Act 2012 (section 75) are stricter than those under the Privacy Act. If you make a notification under the My Health Records Act, you do not have to also make a notification under the Privacy Act's Notifiable Data Breaches Scheme.

The MHR obligation applies only to information contained within the MHR. The types of breaches that need to be reported are:

- Actual or suspected unauthorised collection, use or disclosure of health care information in an individual's MHR.
- Events or circumstances that have compromised or have the potential to compromise the security or integrity of the MHR system.

The obligation does not apply to information that has been downloaded from the MHR and incorporated into your local practice records. If you download information to your practice records, that information becomes part of your practice record. Any breach related to your practice records would need to be considered under the Privacy Act's Notifiable Data Breaches Scheme.

1. What breaches do I have to notify?

A MHR data breach is:

a. The actual or suspected unauthorised collection, use or disclosure of health information in an individual's My Health Record.

Example

Dr Smith is a GP who is authorised by her registered healthcare provider organisation to use the My Health Record system. One evening, Dr Smith searches the system to see if her neighbour, a high-profile sports star who is a patient at the clinic, has a record. She finds the neighbour's record and – as her neighbour has not set access controls – views the information in it, including his MBS data and a file uploaded by a psychologist.

Viewing information in an individual's My Health Record is considered a 'use' of information. As Dr Smith used the information in her neighbour's record and it was not for the purposes of providing healthcare to her neighbour, she has breached s 59 of the My Health Records Act.

When Dr Smith's neighbour next logs on to his My Health Record, he notices that the audit log shows that a doctor at the healthcare provider organisation has accessed his record. He calls up the healthcare provider organisation to ask why someone has accessed his record. As soon as the healthcare provider organisation becomes aware that a doctor has accessed the patient'sr's record for purposes unrelated to providing healthcare, it is required to comply with the data breach notification requirements of s 75 of the My Health Records Act.

In addition, Dr Smith may be subject to a civil or criminal penalty under the My Health Records Act.

Adapted from: OAIC Guide to mandatory data breach notification in the My Health Record system

b. An event or circumstance that has or may have occurred and that has or may have compromised or may in the future compromise the security and integrity of the MHR (this includes past, current and potential compromises of the system).

Example

A registered healthcare provider organisation discovers that an external party has hacked into its IT system. As its IT system connects to the My Health Record system, there is a possibility that the hacker was able to use the organisation's credentials to log in to the My Health Record system and access information in the system.

This would be considered a circumstance that has arisen that may compromise the security and integrity of the My Health Record system. As such, the healthcare provider organisation would be required to comply with s 75 of the My Health Records Act when reporting and responding to the potential breach.

Source: OAIC Guide to mandatory data breach notification in the My Health Record system

The organisation is required to notify suspected breaches as well as actual breaches.

If you do not comply with the notification requirements, you may be liable to a penalty of up to 100 penalty units.

If you make a notification under the MHR Act, you do not have to also make a notification under the Privacy Act's Notifiable Data Breaches Scheme.

2. When do I have to notify?

You must notify a data breach promptly and as soon as practicable after you become aware of the breach or a suspected breach.

You must notify a data breach involving the MHR system even if the breach has been rectified or remedial action taken.

If you are uncertain about whether to report a breach, the OAIC recommends that you report it. You may wish to contact Avant for advice if you have any doubt about whether to report.

3. Who do I notify?

You have to notify the Australian Digital Health Agency (as the MHR System Operator) and the Office of Australian Information Commissioner.

You must also ask the Australian Digital Health Agency to notify affected patients if there is a confirmed breach, or in the case of a potential breach, if it is reasonably likely that the potential breach might be serious for at least one of your patients. This will require an assessment of the number of patients affected, the potential seriousness for your patient/s and an evaluation of the breach and risks associated with it.

If a significant number of individuals are affected you must ask the Australian Digital Health Agency to notify the general public.

You are not required to advise your patients – the Australian Digital Health Agency is responsible for notifying affected individuals of the breach. The aim of this is to ensure there is a coordinated approach to informing healthcare recipients of breaches and to avoid over-notification and inconsistent messaging.

Nevertheless there may be situations where it is appropriate to inform your affected patients to allow them to take steps to mitigate or remedy the breach and to assist them to regain control of their personal information. We suggest that you discuss this with the Australian Digital Health Agency and take their advice. The best contact is via the My Health Record Health line 1800 723 471 (option 2).

4. How do I notify?

The notification should be in writing and should include the following:

- a description of the breach outlining the suspected unauthorised collection, use or disclosure, or threat to the security and integrity of the MHR system
- the date and time of the data breach
- the cause of the data breach and whether it was inadvertent or intentional
- the type of information involved
- when and how you became aware of the breach
- how many healthcare recipients were or may have been affected
- whether the data breach has 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
- the name and contact details of an appropriate person within your practice
- any other relevant factors.

You should notify the Australian Digital Health Agency at MyHealthRecord.Compliance@digitalhealth.com.au Include information about the identities of affected individuals. This does not require specific patient consent as notification is required under the My Health Records Act.

The OAIC plans to have a notification form on its website. Notifications can also be made to enquiries@oaic.gov.au. Do not include information about the identities of affected individuals to the OAIC, only to the Australian Digital Health Agency.

5. Is there anything else I need to do?

As soon as you become aware of a breach or potential breach you must also:

a. Take appropriate steps to contain the breach eg changing access privileges

b. Undertake a preliminary assessment of the cause or causes and extent of breach

c. Evaluate the risks that may arise from the breach. Consider:
   - The type of information involved, how it could be used and who is affected by it
   - The context of the breach – some information may be more sensitive than others
   - The cause and extent of the breach
   - Risk of harm to affected individuals – who received the information, what harm could result

d. Take steps to prevent or mitigate the risks, and set up an action plan to prevent further breaches.

You should have a data breach response plan in place that reflects and implements these steps in the context of your practice.

You should document the steps you have taken to assess, contain, notify and rectify a breach.

6. What is the difference between my obligations under the MHR Act and my obligations under the Privacy Act?

The MHR notification scheme only applies to:

- Actual or suspected unauthorised collection, use or disclosure of health care information in an individual's MHR.
- Events or circumstances that have compromised or have the potential to compromise the security or integrity of the MHR system.

The obligation under the MHR Act is stricter than the obligation under the Privacy Act's Notifiable Data Breaches Scheme.

Under the Privacy Act a data breach is notifiable to affected individuals and the OAIC if the breach is likely to result in serious harm to an individuals or individuals, remedial action can be taken to prevent the likelihood of serious harm.

By contrast, all breaches or potential breaches are notifiable under the MHR Act. There is no need for serious harm, and even a breach that has been rectified or where remedial action has been taken must still be notified.

If you make a notification under the MHR Act, you **do not** have to also make a notification under the Privacy Act's Notifiable Data Breaches Scheme.

	My Health Record	Notifiable data breach
What type of breach?	• Actual or suspected unauthorised collection, use or disclosure of health information in an individual's MHR. • Events or circumstances that have compromised or have the potential to compromise the security or integrity of the MHR system.	• Unauthorised access to or unauthorised disclosure of personal information. • Loss of personal information where unauthorised disclosure likely.
When to notify?	• Must be notified even if the breach has been rectified or remedial action has been taken.	• Not required to report if remedial action prevents likelihood of serious harm.
Who to notify?	• Notify ADHA and OAIC • ADHA to notify affected individuals.	• Notify OAIC and affected individuals.

Resources and further information

Australian Digital Health Agency

My Health Record Manage a data breach

Information security guide for small healthcare businesses

Office of the Australian Information Commissioner

OAIC My Health Records material, including:

- Privacy business resource 23: Handling personal information in the My Health Record system
- Privacy business resource 22: Ways you can protect patient privacy when using the My Health Record system
- My Health Record Data Breach Response Plan
- FAQ: Using the My Health Record system