RACGP
Royal Australian College *of* General Practitioners

Managing notifiable data breaches in general practice

1

Maintain information governance and security

To reduce the risk of data breaches, make sure your privacy and data security practices, procedures and systems are up to date and reviewed regularly.

Go to step 2.

2

Identify suspected or actual data breach

A data breach involving personal information or compromising the security or integrity of the My Health Record system has occurred or is suspected.

Go to step 3.

3

Contain the suspected or actual data breach

Take immediate steps to contain the suspected or actual data breach.

Go to step 4.

4

Evaluate the risks

Assign to a data breach response team/person who promptly:

- investigates the incident
- evaluates the risks arising from the incident.

Go to step 5.

5

Is the suspected or actual data breach related to the My Health Record system?

Consider whether the breach or suspected breach is a data breach under the *My Health Records Act 2012*.

Data breaches under this Act arise from:

- unauthorised collection, use or disclosure of health information in an individual's My Health Record or
- events or circumstances that may compromise the security or integrity of the My Health Records system.

Yes. Go to step 6. **No. Go to step 7.**

6

Notify the data breach to the Office of the Australian Information Commissioner (OAIC) and the My Health Record system operator (Australian Digital Health Agency)

Notify the OAIC and Australian Digital Health Agency as soon as practicable after becoming aware of the data breach.

In some circumstances, you must also ask the system operator to notify affected healthcare recipients about the breach.

Go to step 11.

7

Does the suspected or actual data breach fall within the Notifiable Data Breaches scheme under the *Privacy Act 1988*?

Has personal information been (or is it suspected to have been) accessed by or disclosed to unauthorised parties, or lost?

Is the data breach likely to cause serious harm to individuals?

Yes. Go to step 8. **No. Go to step 11.**

8

Is there remedial action that can be taken to reduce the likelihood of serious harm?

Yes. Go to step 9. **No. Go to step 10.**

9

Despite the remedial action taken, is serious harm still likely?

Yes. Go to step 10. **No. Go to step 11.**

10

As soon as practicable, notify the data breach to the OAIC and inform all individual/s at risk of serious harm.

Go to step 11.

11

Review the incident

Review and evaluate the incident and take action to prevent or mitigate the effects of future data breaches.

For more information, consult the OAIC's *Guide to mandatory data breach notification in the My Health Record system* and *Data breach preparation and response – A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth).*