Australian Government

DATA BREACH ACTION PLAN

FOR HEALTH SERVICE PROVIDERS

A data breach occurs when information held by an organisation is compromised or lost, or is accessed or disclosed without authorisation. For example, unauthorised access to health records, or lost client data.

1 CONTAIN

Take action to contain the breach

Take immediate steps to limit further access to, or distribution of, the affected information and to reduce the possible compromise of other information. Activate your organisation's data breach response plan, and seek professional assistance if required.

For example, stop the unauthorised practice, recover the records, or disconnect the system that was breached. Additional steps may include setting or changing passwords on client databases, turning on two factor authentication, attempting to recall unread emails, changing computer access privileges, and disconnecting internet connectivity.

Does the data breach relate to the **My Health Record system?**

No

2 EVALUATE

Assess any risks associated with the breach

Consider whether the data breach involves personal information and is likely to result in serious harm to any individuals (such as physical, psychological, emotional, financial or reputational harm). Can remedial action remove the likelihood of serious harm?

If remedial action is successful, a provider should progress to the review stage. If not, this may be an *eligible* data breach under the **Notifiable Data Breaches scheme** regulated by the **Office of the Australian Information Commissioner**. Assessment guidelines can be found on their website (see reverse).

3 NOTIFY

Contact all relevant parties

When an organisation believes an *eligible data breach* has occurred, they must promptly **notify affected individuals.**

The organisation must also **notify the Office of the Australian Information Commissioner** as soon as practicable using the form that is available on their website (see reverse).

Yes

All data breaches related to the **My Health Record system** must be reported!

This includes situations that have (or may have) resulted in **unauthorised collection, use or disclosure** of information in a My Health Record and events or circumstances that have (or may have) compromised the **security or integrity** of the My Health Record system.

When a data breach relates to the My Health Record system, organisations must **notify the Australian Digital Health Agency** as soon as practicable (see reverse).
In most cases you will also need to ask the Agency to contact affected individuals. Organisations must also **notify the Office of the Australian Information Commissioner*** as soon as practicable (see reverse).

* Public hospitals and health services are only required to notify the Australian Digital Health Agency.

Does the affected data contain **Centrelink**, **Child Support** or **Medicare** (customer and/or provider) information? Contact **Services Australia** (see reverse).

4 REVIEW

Minimise the likelihood and effects of future data breaches

- Thoroughly investigate the cause of the breach.
- Develop a prevention and response plan and conduct audits to ensure the plan is implemented.
- Review and strengthen security practices, consider changing organisational policies and procedures for maintaining data, and revise staff training practices.
- Refer to the **Office of the Australian Information Commissioner's** *Guide to health privacy* and other resources to identify additional steps that may be required (see reverse).
- Advice from the **Australian Cyber Security Centre** is also available to assist organisations with developing a cyber incident response plan (see reverse).

CONTACT INFORMATION

Office of the Australian Information Commissioner (OAIC)

The OAIC oversees the Notifiable Data Breaches scheme and privacy aspects of the My Health Record system. For more information on notifiable data breaches:

Web: oaic.gov.au/data-breach-preparation-and-response

Assessing an eligible data breach
Web: oaic.gov.au/data-breach-response-steps

Report a notifiable data breach
Web: oaic.gov.au/report-a-data-breach

Report a My Health Record data breach
Web: oaic.gov.au/my-health-record-data-breach

Guide to health privacy
Web: oaic.gov.au/guide-to-health-privacy

Enquiries
Web: oaic.gov.au/contact-us
Phone: 1300 363 992

Services Australia (Medicare)

You may wish to contact Services Australia to discuss options for protecting customers' **Medicare**, **Centrelink** or **Child Support** records. If there is a risk of compromise to these records, Services Australia may place additional security measures on records.

As a provider you may email us for assistance and support on protecting your customers' Medicare information and your provider credentials used for Medicare. Please note, this mailbox is for providers only.
Email: protectyouridentity@servicesaustralia.gov.au

Impacted customers can discuss these options by contacting Services Australia's Scams and Identity Theft Helpdesk between 8:00am-5:00pm Australian Eastern Time, Monday to Friday.
Phone: 1800 941 126

Australian Digital Health Agency (My Health Record system)

All data breaches related to the My Health Record system must be reported to the Australian Digital Health Agency. The Agency will contact affected healthcare recipients, when this is required under the *My Health Records Act 2012*. Where a significant number of people are affected, the general public will be notified.

Web:
myhealthrecord.gov.au/for-healthcare-professionals/howtos/manage-data-breach

Email: MyHealthRecord.Compliance@digitalhealth.gov.au

Phone: 1800 723 471

Australian Cyber Security Centre (ACSC)

The ACSC leads the Australian Government's efforts to improve cyber security, with the role of helping to make Australia the safest place to connect online. For advice on what to consider in developing an incident response plan:

Web: cyber.gov.au/advice/developing-an-incident-response-plan

Report a cyber security incident
Web: cyber.gov.au/report

Alert service: Sign up to the ACSC's Stay Smart Online free alert service on the latest online threats and how to respond at staysmartonline.gov.au

*You can also seek support from Australia's national identity and cyber support service, **IDCARE** by calling **1300 432 273***