Australian Government
National Office of Cyber Security

National Office of Cyber Security

Advice to Healthcare Professionals | Medisecure Cyber Security Incident

18 July 2024

The Australian Government has been advised by MediSecure that approximately 12.9 million individuals may have had their personal and health information relating to prescriptions, as well as healthcare provider information exposed by a cyber security incident.

MediSecure has published a public notice on the nature and extent of the incident. This can be found at: https://medisecurenotification.wordpress.com/

The affected data relates to prescriptions distributed by MediSecure's systems up until November 2023.

This service enabled prescriptions to be delivered from prescribers to a pharmacy of an individual's choice (for paper and electronic prescriptions). Until late 2023, MediSecure was one of two prescription delivery services operating nationally.

This data breach has not impacted the current national prescription delivery service.

Both paper and electronic prescriptions continue to operate as normal. People can continue to access medicines, doctors can still prescribe, and pharmacists can still dispense as usual.

People should keep accessing their medications and filling their prescriptions.

The National Office of Cyber Security and the Australian Government Department of Health and Aged Care have prepared this document to support you, should any of your customers enquire about the Medisecure cyber security incident.

Further information can be found at a dedicated website hosted on the Department of Home Affairs website at www.homeaffairs.gov.au/cyberincident

What happened?

- A MediSecure database containing personal and health information of individuals and healthcare provider information has been affected by this cyber security incident.
- Information on the data impacted by this breach can be found on MediSecure's public notice at: https://medisecurenotification.com.au/

What should I be aware of as a result of this incident?

- Patients and healthcare professionals should be alert for scams, including those that reference the MediSecure data breach. We do not recommend responding to unsolicited contact about this matter.
- Patients and healthcare professionals should also be wary of any unsolicited contact purporting to be a medical or financial service provider seeking payment or banking information.
    - It is recommended that if an individual receives unsolicited contact: hang up and call back on a phone number you have sourced independently.
    - Individuals can learn how to protect yourself from scams by visiting the National Anti-Scam Centre's ScamWatch site at: www.scamwatch.gov.au

How can I access information and support services following this data breach?

- We understand some people may feel distressed following a data breach.
- This is why we are particularly focused on ensuring Australians can access the support services they need.
- All the relevant information regarding support services is available at the Department of Home Affairs website: www.homeaffairs.gov.au/cyberincident

Do I need to replace my Medicare card?

- Services Australia advises that individuals do not need to take any action related to their Pensioner Concession, Healthcare Concession, and Commonwealth Seniors cards.
- While your Medicare account cannot be accessed with your Medicare card details alone, if you're concerned about your Medicare card details, the easiest way to replace your Medicare card is by using your Medicare online account through myGov.
- You can visit https://www.servicesaustralia.gov.au/medicare-card for helpful information about the steps you can take to replace your card.
- If you want more information about the security of your Medicare, Centrelink and myGov accounts, please visit www.servicesaustralia.gov.au/databreach for advice on how you can protect your personal information after a data breach.

Do I need to replace my Veteran, Pernsioner Concession or Commonwealth Seniors Card?

- The Department of Veterans' Affairs (DVA) advises that personal information cannot be accessed with a DVA file number alone, or be used as a proof of identity.
- DVA advises that individuals do not need to take any action related to their Veteran, Pensioner Concession, and Commonwealth Seniors cards.
- DVA is examining other potential impacts to individual identity security associated with breached card numbers.
- More information about how DVA protects information in the event of data breaches is available on the DVA website.

What should I do to keep my identity safe?

- If you believe your information has been misused as a result of this incident, report this to ReportCyber at cyber.gov.au.
- We can all take simple steps to protect ourselves online, including setting up multi-factor authentication, creating strong and unique passphrases and installing software updates regularly. More advice on protecting yourself online is available at: www.cyber.gov.au