Mead Medical Group Pty Ltd – Cyber Incident Notification

On 9 August 2023, Mead Medical discovered that an unauthorised third party had gained access to Mead Medical's administration mailbox (**Mailbox Incident**) and sent spam emails to some of our valued patients. Specialist forensic IT experts were immediately engaged to remove the unauthorised access and to investigate what happened. The investigation revealed that limited personal information for some patients was contained in the mailbox was *capable* of being accessed by the unauthorised third party. We reached out directly to those patients we deemed as having been impacted in late 2023. As some potentially impacted patients may not have received notice of the Mailbox Incident, this website notice about the Mailbox Incident is made out of an abundance of caution and only intended for patients of Mead Medical between March to August 2023, who have not been contacted by us.

The impacted mailbox is used for exchanging emails about consultations and appointments, and to exchange patient information with other health service providers where necessary. To date, we have no evidence that personal information from the Impacted Mailbox has been published, downloaded or used maliciously. The following categories of personal information were *capable* of being accessed, *only* where this information was contained in emails:

- Contact details
- Health information
- Government reference numbers, e.g. Medicare number, Centrelink reference number
- ID documents, e.g. license numbers

What has Mead Medical done in response?

In response to the Incident, we have implemented a number of measures to prevent reoccurrence including:

1. upgrading our security protections to our email environments;
2. enhancing our security frameworks and policies; and
3. following the advice of specialist forensic IT experts to improve security based on the latest trends.

What should patients do?

We set out below some recommendations to limit the potential impact of the breach:

- In order to protect yourself from potential scams, please be alert for suspicious calls, email and text messages purporting to come from Mead Medical.
- regularly change your passwords and security questions & answers for accounts containing personal information;
- do not click on links or download file attachments when an email or text message appears suspicious;

- do not reply to email or text messages requesting your personal information;
- beware of cold callers falsely claiming to be from authorities or businesses that ask you for your personal information;
- If concerned about the security of your Medicare or Centrelink account, please visit servicesaustralia.gov.au/databreach for more information on how you can protect your personal information after a data breach.
- If concerned about identity information, contact the issuer (e.g. for licenses, contact the department of transport)
- obtain a free credit report to identify whether there is any suspicious activity against your credit history (for example, Equifax credit reports are available at https://www.equifax.com.au/personal/products/credit-and-identity-products); and
- you can find further information about online safety, cyber security and helpful tips to protect yourself at the Australian Cyber Security Centre or the ACCC's Scam watch website.

We apologise for any distress the Incident may cause you. If you require any further information, please do not hesitate to contact Collean Guest on collean@meadmedical.com.au.