Geelong Anaesthetic Group – Cyber Incident

On 16 October 2023, we discovered that Geelong Anaesthetic Group had been the victim of an email security incident involving unauthorised access to one of our employee mailboxes, which was used to send spam emails to addresses contained in that account.

Following discovery of the attack, we immediately engaged an IT consultant to remove the unauthorised access to the email account and investigate the scope of the incident. Geelong Anaesthetic Group's system has since been secured and notifications have been issued to the Office of the Australian Information Commissioner and any individuals likely to have been affected.

We would like to reassure all patients that Geelong Anaesthetic Group does not transfer medical records via email and all patient records are secured within a secure patient management system. Access to this patient management system is separate to the email accounts and there was no unauthorised access to the patient management system.

Queries

If you have any queries, please contact us at fiona@gag.com.au. Geelong Anaesthetic Group takes cyber security and privacy of personal information seriously, and we remain highly alert and continue to monitor our systems for signs of any suspicious activity.

Protection against theft of personal information

Although there is no evidence that any personal data has been accessed apart from the email addresses used in the spam attack, we have outlined some simple steps below that you can take if you have any concerns:

1. Check your bank account statements for suspicious activity and contact your bank if you see any unusual activity. If necessary, discuss options with your bank regarding replacement cards as required.

2. Contact IDCARE - Australia's national identity and cyber support community service. They have expert Case Managers who can work with you in addressing concerns in relation to personal information risks and any instances where you think your information may have been misused. IDCARE's services are at no cost to you. If you wish to speak with one of their expert Case Managers, please complete an online 'Get Help' form at https://www.idcare.org/contact/get-help, or call 1800 595 160 (Monday to Friday 8am – 5pm AEST excluding public holidays).

3. Obtain a free credit report to identify whether there is any suspicious activity on your bank accounts (for example, Equifax credit reports are available at https://www.equifax.com.au/personal/products/credit-and-identity-products).

4. Ensure that you have sufficiently complex passwords on your computer systems, your email and your social media accounts.

5. Ensure that you have up-to-date anti-virus software and any recommended software patches installed on your computer systems.

6. Visit Scamwatch (at https://www.scamwatch.gov.au/) to keep up with current scam trends.