Cyber Security Incident

We are writing to inform you that on 25 August 2025, Dr Sze Yeap Gastroenterology (**SYG**) experienced a cyber security incident (**Incident**) that may have resulted in you receiving an unsolicited SMS.

On discovery of the Incident, SYG immediately engaged a forensic cyber security firm to stop and investigate the Incident. Importantly, our cyber expert has determined, following its initial investigations, that:

1. an unknown third party accessed your contact information (name and mobile number) to send you the unsolicited SMS on 25 August 2025. The SMS was an attempt at 'phishing' by pretending to be a message from DHL for you to pay import duties;
2. your contact information (name and mobile number) was not exported or sent elsewhere;
3. your clinical records, Medicare information, and financial information (such as bank card details) were not affected by the Incident; and
4. the root cause of the Incident was likely due to the unknown third party using a compromised credential used by a legitimate external service provider (to SYG) to access our electronic appointment and booking system.

SYG has advised the external service provider of the Incident and adopted new cyber security measures to prevent a repeat of the Incident.

SYG takes your privacy seriously and recommends you consider taking the following additional steps to protect your privacy.

We assure you that we take the security of your information very seriously. Dr Sze Yeap and SYG apologise for the Incident.

Yours Sincerely,

The Management Team at Dr Sze Yeap Gastroenterology.

What actions has Dr Sze Yeap Gastroenterology taken?

Once aware of the Incident, we worked urgently to contain the threat and investigate what occurred. We also engaged external cyber security experts to assist with our response to the Incident and we have worked with these experts to ensure the ongoing safety and security of our systems.

What do you need to do now?

The investigation has not identified evidence that any personal information has been taken or stolen, such that any third party would have ongoing access to such information.

However, given some of your personal information may have been subject of unauthorised access, we encourage you to remain vigilant to potential scams and to exercise care when providing personal information to other parties.

Please refer to the annexed Fact Sheet which provides recommended steps you can take to further protect your personal information from misuse.

Conclusion

We regret that this incident has occurred and we sincerely apologise for any concern or inconvenience this may cause you.

If you have any questions or would like more information about the Incident, please contact us at contact@yeapgastro.com.au or (08) 8375 5247.

FACT SHEET

Recommendations to further protect your personal information

We recommend that individuals take the following steps to reduce the risk of harm associated with access to their personal information.

General recommendations

1. Remain alert to increased scam activity, especially email, SMS or telephone phishing scams (i.e., fraudulent communications disguised as if to look like they come from an organisation you trust). In particular, any such scam activity purporting to come from Dr Sze Yeap's rooms.
2. Do not click on any suspicious links or provide your passwords or any personal information. Always refuse any unprompted request from an individual to access to your computer even if they say they are from a credible organisation.
3. If your identification ("ID") documents have been impacted, this does not affect its validity and you can still use it for its intended purpose, and as proof of identity. ID information can provide credentials which can potentially be used, for example, to obtain a line of credit, or conduct other fraudulent transactions. As such, we recommend contacting the issuing authority to let them know that a copy of your ID may have been accessed by an unauthorised third party, and request that they put an alert or restriction on your file.
4. Consider changing your online account passwords. The Australian Cyber Security Centre provides guidance around good password practices: https://www.cyber.gov.au/protect-yourself
5. Enable multi-factor authentication for your accounts wherever possible.
6. Install up-to-date anti-virus software on any device you use to access your online accounts.
7. To monitor your financial records, you can apply for an annual free credit report or credit report ban from each of the consumer credit reporting agencies below:

- Equifax
- Illion
- Experian

Recommendations as to medical information

8. Please note that your Medicare account cannot be accessed with your Medicare card number alone. Unlike a scan or copy of a Medicare card, a Medicare card number by itself cannot be used as proof of identity.
9. However, if you are concerned about the security of your Medicare account, please visit servicesaustralia.gov.au/databreach for more information on how you can protect your personal information.
10. You may also choose to contact Medicare to obtain a replacement card free of charge. You can do this by using your Medicare online account through myGov, the Express Plus Medicare mobile app or calling the Medicare program.
11. If you have concerns about securing your confidential information with organisations such as MyHealth Record, MyGov or your health fund, you may wish to contact them and discuss additional security measures they can put on your account.
12. Otherwise, if you suffer any distress in connection to any impact to your medical information, we suggest that you contact your doctor, a support service, or your family or friends.

Additional resources

You can find further information about online safety, cyber security and helpful tips to protect yourself at the following websites:

a. Waysto protect your privacy | OAIC
b. ACCC's Scam watch website
c. Protect yourself | Cyber.gov.au