24 March 2025

Dear patients and valued colleagues

ADELAIDE SKIN AND EYE CENTRE AND ADELAIDE SURGICENTRE
NOTICE OF ELIGIBLE DATA BREACH

We are writing to inform you of a cyber incident affecting the *Adelaide Skin and Eye Centre* and *Adelaide Surgicentre*, which are operated by Adelaide Surgicentre Pty Ltd ACN 119 882 254. We are sorry to report that our practice has become one of many Australian organisations affected by a cyber-attack.

We engaged our information technology services provider (**IT Provider**) to understand, as best we can, the circumstances surrounding this data breach. Based on the information available to us, we have reason to believe that your personal information may have been accessed by an unknown person or persons.

This notice provides you with further details of what happened, what kinds of personal information was potentially accessed and what steps you can take to protect yourself.

1. What happened?

1.1 On the morning of 7 March 2025:

(a) our information technology services provider (**IT Provider**) detected that an unknown person or persons had gained access to our network, with a cyber ransom attack from one of our network servers (**Ransomware Server**); and

(b) our staff were unable to log into the Centre's network system, with a ransomware notice displayed on several printers (**Ransom Notice**).

1.2 The author(s) of the Ransom Notice identified themselves as "Inc. Ransom" (**Attacker**), with a link to access further details of their demands. We did not engage with the Attacker, whether by clicking on the link in the Ransom Notice or otherwise seeking to correspond with the Attacker. As at the date of this notification, no further correspondence has been received from the Attacker.

1.3 To contain the data breach, the IT Provider (amongst other matters):

(a) scanned all workstations and network servers (including the Ransomware Server), for malware and other malicious code;

Tel: (08) 8211 0000 | Fax: (08) 8211 0001
89 King William St, Kent Town SA 5067
www.asec.net.au

Provider Number 999771L
ABN 97 019 456 110
Fully accredited by HDAA Australia Pty Ltd

(b) restored data and files stored within the network servers (including the Ransomware Server) from the backups;

(c) isolated, and completely shut down the Ransomware Server; and

(d) deleted the administration accounts created by the Attacker,

that same day.

1.4 Our investigations and those of our IT Provider:

(a) found no evidence of data (including personal information) being copied, downloaded, exported, modified or transferred from the Ransomware Server or any other network servers by the Attacker; and

(b) confirm that data (including personal information) in the patient administration database, My Health Record and email accounts have not been accessed by the Attacker.

1.5 We have also notified the Australian Signals Directorate (who in turn notified the South Australian Police), Australian Cyber Security Centre and the Office of the Australian Information Commissioner of this incident.

2. What was accessed?

2.1 For patients, it is possible that the Attacker accessed some or all of the following personal information which was contained in the network servers:

(a) the user reference number that we have allocated to them for internal purposes;

(b) demographics information (being names, dates of birth and age);

(c) contact details (being email addresses, street/PO Box addresses and telephone numbers);

(d) government related identifiers (being Medicare card numbers, reference number and expiry dates and Department of Veterans' Affairs Numbers); and

(e) health information (including private health insurance information).

2.2 For other individuals, it is possible that the Attacker accessed some or all of the following personal information which was contained in the network servers:

(a) demographics information (being names, dates of birth and age);

(b) contact details (being email addresses, street/PO Box addresses and telephone numbers);

(c) superannuation account numbers and bank account details (i.e. BSB and account number but not credit card details or CCV numbers on those credit cards);

(d) results from Department for Communities and Social Inclusion Screening, Working with Children and National Police Checks; and

(e) government related identifiers (Medicare issued provider and prescribed numbers, Australian Business Numbers for individuals, Tax File Numbers and Australian Health Practitioner Regulation Agency numbers).

3. What can I do?

3.1 We acknowledge and apologise for the distress this data breach may cause you.

We suggest that you consider taking the precautions outlined below to safeguard your identity and to minimise the impact this data breach may have on you:

(a) contact Services Australia on 132 011. They can assist you with:

(i) getting a replacement Medicare card, which will have a new number and expiry date. This means your old card will no longer be valid;

(ii) adding a secret password to your Medicare records. This will provide an extra level of authentication;

(iii) locking access to your online Medicare account, the Express Plus mobile apps or phone self-service functionality;

(iv) cancelling your Medicare online account and Express Plus mobile apps; and

(v) placing additional authentication measures in place (e.g. additional security questions which must be answered) if your Medicare number has been compromised;

(b) contact the Australian Taxation Office if you suspect that your Tax File Number has been compromised, by calling the Australian Taxation Office on 1800 467 033. The Australian Taxation Office may investigate and place extra protection on your account;

(c) check for suspicious activity on your myGov account. The myGov website at https://my.gov.au contains details on how to view your myGov account history. If you find anything suspicious, you can call Services Australia's Scams and Identity Theft Help Desk on 1800 941 126;

(c) ask for a credit report from agencies such as Equifax, illion and Experian, to see whether someone has attempted to apply for credit in your name. Further information on how to do this is available at: https://www.idcare.org/fact-sheets/credit-reports-australia;

(d) call the Australian Cyber Security Hotline on 1300 292 371. This is run by the Australian Cyber Security Centre (a Commonwealth government agency), whose website at https://www.cyber.gov.au also contains useful tips on how you might protect yourself, whether online or with your devices;

(e) call ID Care on 1800 595 160. ID Care is a not-for-profit organisation which helps people with identity and cybersecurity concerns, and their website at https://www.idcare.org also contains useful tips on how you can further protect yourself against scams, fake texts and phishing exercises;

(f) visit the website of the Office of the Australian Information Commissioner, at https://www.oaic.gov.au for helpful 'Data breach support and resources' (including links to mental health support services);

(g) visit the website of the Australian Government's ScamWatch at https://www.scamwatch.gov.au for helpful tips on how to spot a scam. You can also subscribe to receive email alerts about new scams and scam trends;

(h) maintain vigilance for suspicious texts, emails or phone calls you may receive, including by:

  (i) being alert for any phishing scams that may come to you by phone, post or email;

  (ii) carefully reviewing any communications you receive to ensure they are legitimate;

  (iii) being careful when opening or responding to texts from unknown or suspicious numbers; and

  (iv) regularly updating your passwords with 'strong' passwords, not re-using passwords and activating multi-factor authentication on any online accounts, where available;

(i) contact Beyond Blue for support if this data breach has caused you distress, on either https://www.beyondblue.org.au/about-us/contact-us or 1300 22 4636.

Please contact the practice on patientenquiries@asec.net.au or 08 8211 0000 if you have any queries in connection with this notice.

Thank you for your understanding and co-operation on this matter.

Yours sincerely

Ms Susan Stuart
Practice Manager