

10th September 2024

## **Public Notice - Data Incident at GP Central**

GP Central suffered a data incident earlier this year. Since the incident, we have been working with technical specialists and advisors to secure the impacted account and investigate the scope and nature of the compromise.

This notice sets out what happened, steps patients may wish to take in response, and how patients can obtain further information.

We are obviously deeply disappointed that this has happened and apologise fully for any concern caused.

### **What happened?**

In May 2024 a third party appears to have accessed the email account of a GP Central staff member. This staff member is a member of our support team.

Our investigation into the incident has identified evidence that the third party may have sought to exfiltrate information from the account. While we cannot confirm exactly what information may have been impacted, it appears that all the information held in the account may have been at risk. With that in mind, GP Central has reviewed the content of the impacted account in its entirety.

Given the nature of the individual's role, which includes liaising with various external clinical contacts and stakeholders, the account held a range of information at the time. This included patient and clinical information. In a handful of very limited cases this also included IDs provided by patients.

### **What should I do?**

If you wish to know whether your information was implicated in the incident please contact us at [dataprotection@gpcentral.co.nz](mailto:dataprotection@gpcentral.co.nz) and we will be able to confirm what, if any, information of yours may have been impacted.

We note that the vast majority of the information potentially implicated would not appear to expose patients to an immediate risk of fraud or identified theft. However, you may wish to consider the below points as matters of general good practice:

- Stay alert to the prospects of fraud. We are mindful that scammers do take advantage of organisations through impersonation in order to elicit further details and access the

affected community. Further information about common scams and frauds and what to look out for can be found on the CERT NZ website [here](#).

- CERT NZ also provide a range of further material about securing your data more generally. Material for individuals can be found [here](#).
- Regularly check your credit report for any suspicious entries. Information on how to check your credit report for free can be found [here](#).
- If you are concerned that your personal information may be misused, you may also want to consider a temporary suppression of your credit file. This will prevent individuals from using your personal information to imitate you and, for example, open new lines of credit in your name. Further information about seeking a temporary suppression of your credit file can be found [here](#).
- Be wary of any correspondence, texts or phone calls purporting to be from either Stoddard, or any other entity you may engage with (such as law enforcement or your bank), that is asking to change bank accounts details or requesting funds. Always call the sender using an independently sourced number to confirm the legitimacy of any request.
- If you receive a text message or email that you think is spam, Te Tari Taiwhenua (Department of Internal Affairs) has a complaint service for spam text and email, [here](#).
- If you believe you are the victim of an online crime, then please report the matter to the Police dialling 105 (non-emergency reporting) in the first instance.

## Next steps

We are deeply sorry that this has happened and apologise fully for the concern this incident may have caused.

If you have any queries or concerns, please contact us on [dataprotection@gpcentral.co.nz](mailto:dataprotection@gpcentral.co.nz)  
We can confirm GP Central has notified this incident to the Office of the Privacy Commissioner.  
You can also raise any complaints directly with the Office of the Privacy Commissioner.

Ngā mihi

GP Central  
[dataprotection@gpcentral.co.nz](mailto:dataprotection@gpcentral.co.nz)