Fairfield Medical FAQs

**What happened?**

Fairfield Medical uses a data storage platform provided by a third-party provider. That third-party provider suffered a ransomware attack which impacted many of their customers.

The impacted data storage platform is not used to host our patient management and clinical notes systems. However, these systems were used to host a range of other data, including limited personal, clinical, and commercial data.

**What information was breached?**

The compromise did not affect our patient management and clinical notes system. However, limited personal, clinical and commercial information was affected by the compromise. We have notified the individuals at most risk.

**Why has it taken so long for me to be notified?**

It took some time for our IT provider to confirm precisely what information had been compromised, following their forensic investigations. We then embarked on a thorough review of the compromised data to identify all personal information and impacted individuals. We have been keeping the Office of the Privacy Commissioner updated with both our assessment process, and conclusions regarding notification obligations.

**Has my information been impacted?**

A range of information has been impacted. We have individually notified patients who are at most risk of harm as a result of the breach. If you suspect that you have been impacted and have not been contacted directly, please contact us at cyberincident@fairfieldmed.co.nz

**How are you responding?**

Along with our third-party provider we have worked with the relevant authorities, including the Office of the Privacy Commissioner. Steps have been taken to ensure the platform is secure, and we have sought advice on our obligations under the Privacy Act 2020.

**Who did this?**

We were unsure who did this but believe the ransomware attack was carried out by malicious third party actors.

**Is the platform now secure?**

Yes, further security measures have been taken to ensure that this does not happen again.

**What steps do I need to take?**

The ongoing risk appears to be low. However, we recommend the keeping an eye for the following:

* 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 : [Home | CERT NZ](https://www.cert.govt.nz/)
* CERT NZ also provide a range of further material about securing your data more generally. Material for individuals can be found here : [Individuals | CERT NZ](https://www.cert.govt.nz/individuals/)
* Regularly check your credit report for any suspicious entries. Information on how to check your credit report for free can be found here : <https://www.govt.nz/browse/consumer-rights-and-complaints/debt-and-credit>
* 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 : <https://www.centrix.co.nz/>
* Be wary of any correspondence, texts or phone calls purporting to be from either Fairfield Medical Centre, Pinnacle Health, 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, the following information may be of use:
	+ Te Tari Taiwhenua (Department of Internal Affairs) has a complaint service for spam text and email, here : <https://www.dia.govt.nz/>
* 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.

**If my information is affected, can I get a copy of my data?**

Yes, we can provide you of your information. Please send your request to cyberincident@fairfieldmed.co.nz

**What if I have any further issues or want to complain?**

We have notified the Office of the Privacy Commissioner of this incident. If you have any further concerns, please email us at cyberincident@fairfieldmed.co.nz. Otherwise you can complain to the Office of the Privacy Commissioner here :

**Any further questions?**

We appreciate that you may have further questions, please send them to cyberincident@fairfieldmed.co.nz