IN THE HIGH COURT OF NEW ZEALAND
WELLINGTON REGISTRY

I TE KŌTI MATUA O AOTEAROA
TE WHANGANUI-A-TARA ROHE

CIV-2026-485-2
[2026] NZHC 2

BETWEEN	MANAGE MY HEALTH LTD Applicant
AND	UNKNOWN DEFENDANTS Defendants

Hearing:	On the papers (Teleconference held on 6 January 2026)
Counsel:	J M Fitzgerald and N V Sirisamphan for Applicant
Judgment:	5 January 2026
Reasons:	6 January 2026

REASONS JUDGMENT OF ISAC J
[Application for permanent or interim injunction]

Introduction

[1] The applicant, Manage My Health Ltd, applies for a without notice injunction restraining unknown defendants from using, publishing or otherwise distributing information unlawfully obtained during a cyber-attack. The information was exfiltrated through a website administered by the applicant. The site stores and manages sensitive health information on behalf of general practitioners and their patients.

[2] The application was referred to me as duty Judge in the afternoon of 5 January 2025. I was satisfied it was appropriate to grant modified orders on an urgent basis. This judgment sets out my reasons for granting the application and the orders made.

Background

[3] The following background is set out in the supporting affidavit of Mr Vinogopal Ramayah, the applicant's Chief Executive Officer and one of its directors.

[4] Manage My Health provides and administers an online patient portal. The portal helps patients and health care providers communicate information to one another through a website. The portal also enables patients to book appointments, request repeat prescriptions, message their practice and access personal health information such as medical records and test results. Manage My Health is one of the largest private health information platforms in New Zealand and it is widely used across primary health care services (or GP practices).

[5] On 30 December 2025 the applicant received a notification that a third party was claiming to have accessed sensitive health information on its portal. On receiving the notification, Manage My Health initiated a technical investigation. The investigation identified signs of unauthorised access to its site. These included:

(a) abnormally high-frequency login activity;

(b) repeated authentication attempts within compressed timeframes;

(c) rotating IP address usage to hide the source of attack;

(d) repeated access to document endpoints and internal application programming interfaces (or APIs).

[6] These access patterns are consistent with automated extraction methods used by hackers in other cyber-attacks.

[7] The intrusion was focused exclusively on a "health documents" module within the portal. The module contains digitised clinical documents relating to individual patients (as opposed to a database of a patient's health information).

[8] On 31 December 2025, Manage My Health received three anonymous emails in its general inbox from the hackers. The emails referred to a database "leak" from the portal and advised that sample data had been published on a data leak website. The hackers threatened further publication "on various hacker forums" unless a "confidentiality fee" of USD$60,000 (in bitcoin) was paid.

[9] On 1 January 2026, with the assistance of an external expert, Manage My Health obtained access to the data leak website referred to in the hackers' emails. The posting to the data leak website revealed the hackers had:

(a) posted a sample of the information they said had been taken from the portal. Further analysis has confirmed the sample information has been obtained from Manage My Health's portal;

(b) recorded the ransom demand they had made of $60,000; and

(c) noted that the posting "expires" on 15 January 2025. This implies the hackers intend to release the patient information if the ransom payment is not made before then.

[10] Over recent days the hackers have communicated a shortened "ultimatum" deadline. They have said that "[t]his is the final notice. If you do not pay the random [sic] within the next 48 hours, we will leak all information." The applicant has now received similar messages repeatedly, but it is unclear when the 48-hour period referred to commenced or will end.

[11] Takedown requests have since been issued to the provider hosting the sample of the data leak website. At the time proceedings were filed the sample was no longer available.

[12] Manage My Health's analysis has also now concluded that there has been unauthorised access to the health documents module within the portal and that data was exfiltrated from it. Unauthorised access was gained through the exploitation of an

API "endpoint" (which has now been addressed by the applicant).[1] The hackers' claims are also consistent with the applicant's findings. There is no indication to date of further exploitation of or interference with other data on the portal.

[13] Based on the applicant's preliminary analysis:

(a) in the order of 430,000 patient documents have been exfiltrated from the portal (the "stolen data");

(b) the number of potentially affected patients is in the order of 127,000;

(c) documents in the stolen data include:

(i) clinical discharge summaries, referrals, and related files relating to patients;

(ii) historical clinical referral records (between 2017–2019) relating to patients;

(iii) personal health information uploaded by patients; and

(iv) clinical referral requests relating to patients.

(d) The stolen data relates to a range of medical practices, including:

(i) approximately 45 Northland-based GP practices;

(ii) approximately 355 "referral-originating" GP practices across a number of regions in New Zealand;

---

1 Mr Ramayah deposes that "The issue with the API that allowed the threat actor to access the MMH portal has been addressed. At this stage we do not believe there to be an ongoing risk to data held on the MMH Portal. This is being verified by the investigation currently being conducted by the engaged digital forensic experts."

(iii) patient-uploaded files. This is a subset of the stolen data and is not limited to Northland patients.

(e) The evidence in support of the application also records that much of the stolen data contains "sensitive personal health information". By way of example the documents include:

(i) highly sensitive and confidential descriptions of patients' ailments, injuries, health conditions, investigations, procedures, and diagnoses;

(ii) personal information, such as patient contact details, dates of birth and addresses; and

(iii) highly sensitive and confidential health information such as patient medical histories (physical and mental), diagnoses, medications, and health care plans.

[14] The media has since reported that Manage My Health has been a victim of a cyber-attack. The hack has also been reported by the applicant to Te Whatu Ora | Health New Zealand (Health NZ), the Privacy Commissioner, the Police, and the National Cyber Security Centre. The applicant has also convened an incident response team and is currently working through a process to ensure all affected individuals are notified in accordance with the requirements of the Privacy Act 2020. This process includes verifying the information contained in the stolen data, liaising with relevant stakeholders (including Te Whatu Ora, the Office of the Privacy Commissioner, Primary Health Organisations and GP practices), and setting up the necessary support resources for affected individuals.

[15] An ongoing concern identified by the applicant is the risk that patients' health information might be obtained by third parties if it is published online and further misused or disclosed, including using it to target patients directly or disclosing patient contact information to individuals who should not have access to it.

Why is the action brought against unnamed defendants?

[16] Other than the hackers mentioning they are known as the "Kazu Group", Manage My Health does not know who the hackers are or where they are based (although they are likely to be overseas). Similarly, the applicant is not aware if any third parties have downloaded the stolen data or any part of it, including the sample available on the data leak site. It is also unclear if the complete set of stolen data will be made available by the hackers following the "expiry" of the time frame for compliance with the ransom demand, on 15 January 2026.

[17] Accordingly the applicant says it is not practical nor possible to name any respondent to this proceeding. As in previous similar cases, Manage My Health seeks a general injunction against anyone who has or who might obtain the stolen data.

The causes of action

[18] The statement of claim sets out two causes of action. The first is for breach of confidence. The elements of the cause of action are:[2]

(a) that the information in question has the necessary quality of confidence about it;

(b) it has been imparted or obtained in circumstances importing an obligation of confidence; and

(c) there has been an unauthorised use, or threatened use, of that information.

[19] The second cause of action is for breach of privacy. The elements of the cause of action are:[3]

---

2 *Henderson v Walker* [2019] NZHC 2184, [2021] 2 NZLR 630. At [144]-[160], citing *Coco v AN Clarke (Engineers) Ltd* [1969] RPC 41 (Ch) at 46. *HWL Ebsworth Lawyers v Persons Unknown* [2024] NSWSC 71 at [29], citing *Corrs Pavey Whiting & Byrne v Collector of Customers (Vic)* (1987) 14 FCR 434, at 443; [1987] FCA 266 per Gummow J.

3 *Hosking v Runting* [2004] 1 NZLR 1 (CA) at [117].

(a) the existence of facts in respect of which there is a reasonable expectation of privacy; and

(b) publicity given to (or in this case threatened) in relation to those private facts that would be considered highly offensive to an objective reasonable person.

Principles

[20] The principles are well settled. On an application for an interim injunction, the Court will generally address itself to three issues:[4]

(a) Is there a serious issue to be tried?

(b) Where does the balance of convenience lie?

(c) What is the overall justice of the case?

[21] The last two issues require the Court to consider the adequacy of damages, preservation of the status quo, disadvantages to either party and the relative strengths of their cases.[5] At the interlocutory stage the Court is not required to resolve conflicts of evidence or resolve difficult questions of law requiring detailed argument and mature considerations.[6]

Consideration

[22] In light of the evidence in support of the application I was clearly satisfied that the requirements for the grant of an interim injunction were made out.

---

4 *Klissers Farmhouse Bakeries v Harvest Bakeries Ltd* [1985] 2 NZLR 129 (HC); and *NZ Tax Refunds Ltd v Brooks Homes Ltd* [2013] NZCA 90 at [12].

5 *Wellington International Airport Ltd v Air New Zealand Ltd* HC Wellington CIV-2007-485-1476, 30 July 2008 at [6]-[14].

6 *American Cyanamid Co v Ethicon Ltd* [1975] AC 396 (HL) at 407; *Villa Maria Wines Ltd v Montana* Wines *Ltd* [1984] NZLR 4 22 (CA) at 425; and *Health Club Brands Ltd v Colven* [2013] NZHC 428 at [9].

[23] First, there is no doubt that sensitive patient information has been unlawfully obtained by unknown parties in a cyber-attack. The individuals responsible for obtaining the data clearly have no entitlement to it.

[24] Second, there is also no doubt that the purpose of the data hack is to use the threat of further disclosure as a means to extort payment from the applicant. Those responsible have sought to make plain the seriousness of their threat by publishing a small sample of the stolen data.

[25] Third, if the ransom is not paid or the stolen data is published or otherwise made available, there is a risk of further harm to third parties, namely the patients whose sensitive health information has been compromised.

[26] Finally, given the hackers have concealed their identity, it is not possible or practicable for the applicant to name individual parties as respondents, as would normally be required.[7] Similarly, it is not possible (or necessary) to identify third parties who have or may come into the stolen data in order to enjoin them.

[27] For these reasons I concluded the applicant had made out a strong case and the overall justice of the case favours protection of the real victims of the cyber-attack, namely patients and their GP practices.

[28] I was not prepared to grant a permanent injunction as the primary relief sought by the applicant. Counsel acknowledged that a without notice urgent injunction would ordinarily issue on an interim basis only, to provide those affected by the orders an opportunity to be heard before they were made final. However, counsel submitted the right to be heard would be protected by the reservation of leave to apply, which could be "actioned by any person affected by the orders". A permanent injunction was therefore sought with that condition, with an interim order sought in the alternative if the Court was not satisfied it was appropriate to grant final relief.

---

[7] See the principles set out by Gault J in the leading decision on the question of injunctions issued against unknown parties in *Kennedy Point Boatharbour Ltd v Barton* [2022] NZHC 257, [2022] 2 NZLR 696

[29] While it is unlikely any party potentially restrained by the injunction would apply to modify or be released from the orders, there may be consequences that are not immediately evident. In addition, in the absence of argument and submissions, I was not satisfied that it is possible to grant final relief on a conditional basis. Either the Court would be functus and appeal would be the only recourse for affected parties, or the conditional order would not in fact amount to a permanent injunction.

[30] Finally, I was not satisfied that the terms of the orders as set out in the notice of interlocutory application and draft orders were entirely efficacious as originally framed. For that reason, I made modifications to the orders but reserved leave to the applicant to apply.

Conclusion and result

[31] For the foregoing reasons, I granted an interim injunction on the application at 4.46 pm on 5 January 2025 on the terms set out in the schedule to this judgment.

[32] In issuing this judgment I have modified the terms of the orders following a teleconference with counsel. They are now an order:

(a) subject to (b), (c) and (d) below, restraining all persons from accessing or in any way dealing with the stolen data, including storing, broadcasting, publishing, sharing, disclosing, or using any information taken from the stolen data;

(b) requiring all persons to immediately and permanently delete the stolen data in their possession or control, or any information obtained from it;

(c) requiring all persons to immediately and permanently delete and take down any and all publications of or links to the stolen data, or information obtained from it;

(d) for the avoidance of doubt, these orders do not restrain the lawful use of the stolen data by Te Whatu Ora, the New Zealand Police, the National Cyber Security Centre, affected GP practices or their patients;

(e) reserving leave to any person affected by these orders to apply to the Court for variation on 48 hours' notice; and

(f) that the Court file is to be sealed and is not to be searched by any person who is not a party to the proceeding without leave of the Court.

Isac J

Solicitors:
Wooton Kearney, Wellington for Applicant

Schedule 1

The original orders issued at 4.46 pm on 5 January 2025 were:

(a) subject to orders (b) and (c) below, restraining all unknown defendants from accessing or in any way dealing with the Affected Dataset obtained as a result of the December 2025 cyber-attack on the Manage My Health patient portal platform (MMH portal), including creating any derivation of, or using, accessing, collecting, searching, reviewing, copying, structuring, organising, adapting, retrieving, inputting, storing, broadcasting, publishing, sharing, making available to any other person, transferring, or disclosing any information, data or documentation, whether by manual or automated means, from the Affected Dataset;

(b) requiring all unknown defendants to immediately and permanently delete any and all copies of the Affected Dataset in their possession or control or information obtained from it, and provide an undertaking at the request of the applicant or the true owners of the information that they have done so;

(c) requiring all unknown defendants to permanently delete and take down any and all publications of or links to copies of the Affected Dataset of information obtained from it;

(d) reserving leave to any person affected by these orders to apply to the Court for variation on 48 hours' notice;

(e) that if any application to search the court file is made, the applicant is to be given notice and an opportunity to be heard;

(f) for the purposes of these orders, the "Affected Dataset" is those parts of the MMH portal that was exfiltrated as a result of the cyber-attack on the applicant in December 2025.