

[NEW ZEALAND \(/NEWS/NATIONAL\)](/NEWS/NATIONAL) / [TECHNOLOGY \(/TAGS/TECHNOLOGY\)](/TAGS/TECHNOLOGY)

Manage My Health data breach: A timeline of what happened, and everything we know so far

6:50 pm on 14 January 2026

[Dan Satherley \(/authors/dan-satherley\)](/authors/dan-satherley), Digital journalist



Photo: RNZ / Finn Blackwell

In one of the biggest privacy breaches in New Zealand history, at the end of 2025 hackers got access to health data being held by privately owned patient portal Manage My Health.

The cyber criminal(s) demanded thousands of dollars as a ransom, threatening to otherwise release the data on the dark web, potentially exposing more than 120,000 New Zealanders' medical details.

Here is a recap of what has happened, and what we know, so far.

2020

Patient portal Manage My Health, founded in 2008, was spun out of Medtech Global into founder Vino Ramayah's Cereus Holdings (<https://www.rnz.co.nz/news/business/419901/nz-ideal-for-new-health-tech-cereus-investment-company-head>). It had 700,000 users at this stage - a number that would grow to more than 1.8 million over the next five years.

Earlier in 2025

In July, a digital forensics and cyber security company in Nepal reported a hacker going by the name 'Kazu' (<https://www.rnz.co.nz/news/national/583417/who-are-the-hackers-behind-manage-my-health-s-cyber-attack>) allegedly stole 1.4TB of data from the Nepali Ministry of Education, Science, and Technology, including student information and academic transcripts.

Similar claims were made about attacks on a doctors group in Texas, the Colombian Ombudsman, the Thai Department of Agricultural Extension, the Kuwait Ministry of Public Works, the Bolivian Navy and more.

30 December, 2025 (NZ time)

A hacker (or group) calling themselves Kazu posted online they had breached Manage My Health, claiming to have 108GB of data, made up of 428,337 files including names, medical records, test results, prescription details and more. A small sample of data was published as proof.

Kazu demanded US\$60,000 (NZ\$104,000) as a ransom, giving a deadline of 15 January.

31 December

Manage My Health confirmed it had been breached (<https://www.rnz.co.nz/news/national/582969/managemyhealth-confirms-cyber-breach>). Ramayah said the incident was being investigated by the company alongside authorities and independent cybersecurity specialists.

1 January, 2026

The company revealed

(<https://www.rnz.co.nz/news/national/583030/managemyhealth-reveals-scope-of-data-breach>) between 6 and 7 percent of the approximately 1.8 million registered users may have been impacted by the breach, and it expected to start notifying affected patients within 48 hours.

Ramayah said the Office of the Privacy Commissioner, Health NZ police had been notified and the breach had been "contained".

Duty minister Karen Chhour said the breach was "incredibly concerning" for patients



Simoen Brown. Photo: RNZ / Marika Khabazi

(<https://www.rnz.co.nz/news/national/582996/gps-worried-by-lack-of-information-on-managemyhealth-data-breach>). Health NZ said it was working "closely" with the app's operators, and its own systems were not affected (<https://www.rnz.co.nz/news/national/583067/health-nz-says-systems-unaffected-by-managemyhealth-app-breach>).

Health Minister Simeon Brown later that day said

(<https://www.rnz.co.nz/news/national/583047/managemyhealth-data-breach-concerning-but-no-clinical-impact-health-minister>) the breach was concerning, but would have no clinical impact on patient care.

The president of the College of GPs said he only learned about the potential breach through the media, calling it "terribly disappointing", while the chair of General Practice NZ said it was an urgent situation.

3 January

The Public Service Association said the security breach highlighted the risk of cutting IT experts in public health (<https://www.rnz.co.nz/news/national/583088/psa-says-the-privacy-breach-exposes-risk-of-cutting-it-experts-in-public-health>). (While used by practices in the public system, Manage My Health is privately owned.)

Manage My Health said it had fixed the flaws in its code which allowed the breach (<https://www.rnz.co.nz/news/national/583112/managemyhealth-says-code-fixed-security-tightened-after-hack>). Just one part of the app had been accessed - Health Documents - and the company now had a list of everyone affected.

The company urged (<https://managemyhealth.co.nz/mmh-cyber-breach-update-3-january-2026/>) users to enable two- or multi-factor authentication if they had not already, to improve security. It also said users should "keep an eye out for anything unusual, such as medical bills or insurance claims you don't recognise, or unexpected letters from healthcare providers".

4 January

Kazu brought forward the deadline (<https://www.stuff.co.nz/nz-news/360920634/hackers-drastically-shorten-deadline-manage-my-health-pay-ransom>) for Manage My Health to pay, from 15 January to Tuesday, 6 January.

Manage My Health said it had identified which general practices were affected (<https://www.rnz.co.nz/news/national/583156/manage-my-health-cybersecurity-hack-gps-whose-patients-data-was-stolen-identified>) and set up an 0800 number people could contact them on. The company was yet to start contacting patients, despite promising on New Year's Day to do so within 48 hours.

Health NZ established an incident management team and was co-ordinating with other government agencies, including the National Cyber Security Centre and the Police Cyber Crime Unit, on the breach.

5 January

Health Minister Simeon Brown announced a review (<https://www.rnz.co.nz/news/political/583207/government-orders-review-into-managemyhealth-data-breach>) by the Ministry of Health into the response to the breach.

ManageMyHealth said it had filed papers in court seeking an injunction on publication of the stolen files. Brown said ManageMyHealth was "ultimately responsible" for managing the breach.

The National Cyber Security Centre said it was "working with Health NZ and other government agencies".

Manage My Health CEO Vino Ramayah. Photo: SCREENSHOT / RNZ



6 January

The revised deadline (<https://www.rnz.co.nz/news/national/583248/manage-my-health-data-breach-ransom-deadline-arrives>) passed without any data being released. There were later reports it had been moved to Friday, 9 December (<https://www.rnz.co.nz/news/national/583309/deadline-for-manage-my-health-ransom-moves-to-friday-reports>).

Manage My Health said it received an injunction from the High Court.

Brown said he had told the company to improve its communications with patients.

A group representing GPs said (<https://www.rnz.co.nz/news/national/583285/manage-my-health-breach-a-lot-of-queries-from-patients-as-anxiety-about-stolen-data-grows>) they still did not know which practices had been affected.

A person claiming to be Kazu (<https://www.nzherald.co.nz/nz/hacker-claiming-to-be-behind-managemyhealth-breach-i-do-it-for-the-money-and-im-in-negotiations-to-get-it/premium/FC2PYCTFXVEOXN4Q27ONTQIDKA/>) told the *NZ Herald* they were motivated by profit and notoriety.

"Most companies do pay the ransom. In fact, even if the government does not allow it, they pay privately without disclosing it."

The person described ManageMyHealth's security as lacking "basic security protocols".

7 January

Ramayah revealed the hacker "got in through the front door" of the website by simply using a "valid user password".

The CEO said he was open to standing down if required after his company "dropped the ball", but said Manage My Health itself was also the victim of a crime (<https://www.rnz.co.nz/news/national/583336/one-part-terrified-one-part-really-angry-assault-victim-s-anger-over-manage-my-health-hack>).

Mysteriously, Kazu removed all references to the Manage My Health data breach from its online presence (<https://www.rnz.co.nz/news/political/583383/manage-my-health-hackers-removes-information-about-data-online>).

It was revealed data belonging to people who had closed their Manage My Health accounts was still available on the portal.

Manage My Health began the process (<https://www.rnz.co.nz/news/national/583438/manage-my-health-patients-start-to-be-notified-after-massive-leak>) of telling general practices and individual patients if they had been affected.

Lawyers called for tougher penalties (<https://www.rnz.co.nz/news/national/583449/lawyers-say-privacy-rules-need-more-teeth-following-manage-my-health-hack>) for companies who fail to protect clients' data.

8 January

It was revealed patients who stopped using Manage My Data in the past were still having their new medical information added to its database (<https://www.rnz.co.nz/news/national/583486/patient-data-still-being-uploaded-to-manage-my-health-two-years-after-contract-ended>).

Manage My Health's website struggled with the number of people trying to find more information about the hack (<https://www.rnz.co.nz/news/political/583535/patients-ask-gps-for-info-on-health-records-after-manage-my-health-security-breach>).

9 January

Some patients reported (<https://www.rnz.co.nz/news/political/583547/criticism-of-manage-my-health-cyber-attack-response-mounts-as-another-deadline-passes>) receiving conflicting information from the company on whether their data had been

stolen.

The 0800 struggled with the volume of calls, while New Zealanders overseas were told they could no longer use the app due to security reasons

(<https://www.rnz.co.nz/news/business/583637/manage-my-health-patients-draw-blanks-in-quest-for-information-on-cybersecurity-breach>). Others received confusingly blank emails from the company

(<https://www.rnz.co.nz/news/business/583637/manage-my-health-patients-draw-blanks-in-quest-for-information-on-cybersecurity-breach>).

10 January

It was revealed most of the affected patients were based in Northland

(<https://www.rnz.co.nz/news/national/583695/many-manage-my-health-security-breach-victims-in-northland>) - about 86,000, and nearly 50 practices.

Manage My Health had notified about half of the 125,000 whose data had been stolen.

12 January

Northland GPs expressed frustration

(<https://www.rnz.co.nz/news/national/583793/manage-my-health-breach-northland-doctors-frustrated-by-inconsistent-messaging>) at the conflicting information they were getting from Manage My Health.

A second health provider, CanopyHealth, revealed it had been targeted in a cyber attack in July, the delay infuriating clients

(<https://www.rnz.co.nz/news/national/583813/second-health-provider-canopy-health-hit-in-major-cyber-attack>).

The Office of the Privacy Commissioner issued guidance for affected patients on what to do if their data had been exposed (<https://www.privacy.org.nz/tuhono-connect/statements-media-releases/information-for-people-impacted-by-the-manage-my-health-data-breach/>).

'Kazu' said they were motivated by money. Photo: 123RF



13 January

An IT expert expressed surprise (<https://www.rnz.co.nz/news/national/583887/kfc-app-more-secure-than-manage-my-health-expert-claims>) the KFC app had stronger security protocols than Manage My Health.

Kazu claims to have stolen data from MyVete, a Spanish veterinary management system.

There had been no further mention of the Manage My Health data from the hackers since the last reported deadline passed (9 January).

14 January

Manage My Health admitted some people it told had been affected by the hack, had not (<https://www.thepost.co.nz/nz-news/360930551/manage-my-health-tells-people-they-were-hacked-some-werent>).

Two weeks after the breach was first reported, Prime Minister Christopher Luxon was yet to make any public statement about the matter (<https://www.rnz.co.nz/news/top/583521/christopher-luxon-working-from-home-as-year-gets-underway>).

Sign up for Ngā Pitopito Kōrero, a daily newsletter (<https://radionz.us6.list-manage.com/subscribe?u=211a938dcf3e634ba2427dde9&id=b3d362e693>) **curated by our editors and delivered straight to your inbox every weekday.**

JOIN & FOLLOW RNZ



Sign up to RNZ Newsletters

RNZ STATIONS

National

Concert

RNZ Pacific

Parliament - live stream

ON DEMAND

Latest on demand radio

Latest podcasts

Latest video

HOW TO WATCH & LISTEN

Audio help

Radio

Follow our podcasts

Sky, Freeview & Satellite

YouTube

RNZ apps for iPhone and Android

RNZ Flash Briefing for Amazon Alexa

RNZ News for Google Assistant

ABOUT RNZ

About

Contact

Audience Feedback and Complaints

Media Releases

Awards

Jobs