(Keall, C., 2026)
[30 Dec 2025]

Premium Home / Business

# Five ways to make patient portals like ManageMyHealth more secure

**Chris Keall**
Technology Editor/Senior Business Writer · NZ Herald · 18 Jan, 2026 09:00 AM 9 mins to read

The vulnerability of your medical information has been vividly illustrated over the past month with the ManageMyHealth ransomware attack, in which some 127,000 people's medical files were exposed, plus a separate attack on Canopy Healthcare that took place in mid-2025 but was only revealed to some of its patients six months later.

GPs use ManageMyHealth to manage appointments with around 1.8 million patients around New Zealand. The portal is also used to share medical records, test results, prescriptions and other health files. Others are on a rival system called MyIndici.

On December 30, a hacker calling themselves "Kazu" claimed to have copied 428,337 files from ManageMyHealth, posting a small sample as proof and demanding a US$60,000 ($104,000) ransom, for which the deadline was extended when it was not paid.

Security expert Brett Callow told the *Herald* it was common practice for ransomware thieves to seek a low ransom, hoping for a quick, no-fuss payment, while countdown clocks were frequently reset.

On January 5, Health Minister Simeon Brown ordered the Ministry of Health to begin a review of the ManageMyHealth cyberbreach by January 30, covering the causes, the adequacy of protections and recommended improvements to prevent similar incidents occurring. The ministry will consult with the National Cyber Security Centre on the terms of reference, Brown said.

There was no immediate timeline given for the review. In the meantime, the *Herald* asked five experts for five ideas to make patient portals like ManageMyHealth safer.

## 1. Make two-step security mandatory

Security experts universally recommend a two-step login process when a site holds sensitive data.

That means, as well as typing a username and password, you're sent a verification code by email, text or app, which you also have to enter.

In the jargon-crazed world of cybersecurity, this process is variously called two-factor authentication (often abbreviated to 2FA) or multifactor authentication (MFA).

ManageMyHealth has been criticised by multiple experts, including digital standards consultant Callum McMenamin and Auckland University digital infrastructure specialist Dr Abhinav Chopra, for not making two-step security its default.

Chopra says he warned the company about that vulnerability and others, two years ago. MFA remains optional on ManageMyHealth.

"In 2026, passwords are not enough to protect our accounts. Multi-factor authentication can ruin a hacker's day, as it makes certain attack methods almost impossible," McMenamin says.

One of the most popular lines of attack is "credential-stuffing", where hackers use giant lists of user names and (often weak, predictable and reused) passwords from previous attacks. MFA derails that.

McMenamin says: "KFC has multifactor authentication enabled across all its accounts by default. I dream of a future where my health data is as secure as my fried chicken order."

## 2. Get serious about penalties

“The highest fine under the Privacy Act is a measly $10,000. But that’s not even for poor security practices resulting in a data breach – it’s only for failing to notify one,” Simply Privacy principal Frith Tweedie says.

She adds that New Zealand has no civil penalty regime and the highest award of damages the Human Rights Review Tribunal can make is a fine of up to $350,000. (The Privacy Commissioner can refer cases to the tribunal.)

This is in stark contrast to the penalties in other countries. In Australia, maximum fines for serious breaches are the greater of A$50m ($58m), three times the benefit obtained from what happened, or 30% of the organisations’ annual turnover.

The higher penalties across the Tasman were inspired by two major data breaches in 2022, Tweedie says, involving telco Optus, and Medibank, Australia’s largest health insurer.

Tweedie notes that in European Union countries, fines for being careless with data run up to €20m ($40m) or 20% of global annual turnover, whichever is greater.

“Our current approach means there are no real incentives for Kiwi organisations to protect personal information and respect people’s privacy rights,” Tweedie says.

“This has been a problem for years and one that successive Privacy Commissioners have called out. Maybe this time the Government might listen?”

Lowndes Jordan partner Rick Shera backs Tweedie’s sentiments.

He adds: “We need to allow people who have had their privacy seriously breached to bring their own proceedings, which would also open the way for direct class actions where multiple individuals are impacted, instead of having to first complain to the Privacy Commissioner and then undertake the lengthy Human Rights Review Tribunal process if dissatisfied.”

Privacy Commissioner Michael Webster has continued his predecessor John Edwards’ call for tougher penalties.

Webster told the *Herald:* “In my view, the Privacy Act 2020 doesn’t currently provide sufficient incentives for many organisations to ensure they understand or meet even the most basic privacy requirements.

“The act needs to include a reinforcing system of powers and penalties, including significant financial penalties, and real consequences. We see multimillion-dollar penalties in Australia for organisations which fail to protect personal information. But in New Zealand, there’s no civil penalty regime for privacy breaches – not even the ability to impose lower-level infringement fines.

“At the very least, I would want to see a civil penalty regime similar to that available to the New Zealand Commerce Commission.”

Justice Minister Paul Goldsmith says he’s taking advice on possible updates to the Privacy Act.

Software architect and data sovereignty campaigner Tamawera Owens (Ngāti Awa, Ngai Tuhoe, Te Arawa) says there’s a nuance that Goldsmith will have to take into account.

All-comers in the debate are aware of the legal advantage of data being stored within New Zealand’s borders, and ManageMyHealth has said its data resides at (unnamed) local data centres.

But Owens qualifies that, “Ownership matters more than location. US-owned servers in New Zealand still answer to US law. The Cloud Act allows American authorities to access data from AWS, Microsoft Azure, or Google globally - without New Zealand involvement.”

He explains, “Authentication is the gap most miss. Your credentials, login patterns, IP address, what you’re accessing, when you’re accessing it - may process offshore even when your records stay ‘local’.”

### 3. Don’t outsource the risk

If an Australian citizen wants to check a blood test result, they can access a government-held digital patient record system.

Here, we have a larger private component.

“Patient portals holding millions of health records shouldn’t be treated as ordinary commercial services that the Government can simply outsource and forget,” says Democracy Project director Dr Bryce Edwards.

“For 30 years, that’s exactly what happened – and ManageMyHealth is the result: a 21-person private company with near-monopoly status, minimal governance [the firm has just two directors, including its founder and chief executive, Vinogopal Ramayah] and no public accountability.

“When you outsource critical infrastructure to a private operator, you don’t transfer the risk – you just lose control of it.

“The market was supposed to drive standards through competition, but when patients are locked into whichever portal their GP uses, there is no competition.”

In Edwards’ view, security becomes a cost to be minimised, not a public duty.

“Real reform means rebuilding public capacity: completing the long-delayed national health information platform, enabling data portability so patients aren’t captive to a single provider and treating digital health as the critical infrastructure it is.”

### 4. Health NZ has good standards – not enforced

Health New Zealand has a set of guidelines for the health sector called the Information Security Framework (HISF), which cybersecurity expert Adam Voulstaker says is comprehensive and up-to-date.

Its guidance includes multifactor authentication for all user accounts, geolocation checks and real-time monitoring.

Voulstaker says ManageMyHealth’s (successful) application for an injunction against stolen files being published details how the company only launched an investigation that uncovered abnormally high login activity, from suspicious addresses after it was contacted with a ransomware threat by the apparent attacker.

“The problem isn’t the framework’s adequacy – it’s the complete absence of enforcement,” he says.

Audits could be on the way.

“As Health NZ progresses implementation of measures to increase the accessibility and security of health information, we are considering what further assurance of third-party providers against regulations and standards is required,” a Health NZ spokesperson said.

“This may include independent testing of third-party services such as patient portals.”

### 5. Make it illegal to pay a cyber ransom

Our Government has a policy of not paying a cyber ransom – which it reiterated during the major Waikato DHB data breach in 2022.

And police have a long-standing recommendation not to pay. They say there’s no guarantee you’ll get your data back, or that it won’t be used to blackmail your customers individually. Paying also incentivises further offending, and proceeds from cyber ransoms often fund other organised crime, including drugs and human trafficking.

Yet some individuals and organisations do pay cyber ransoms, according to cybersecurity firms. One survey, by Thales, found that one-third of New Zealand businesses would cough up a ransom in the hope of retrieving their data.

Cybersecurity expert Brett Callow and tech commentator Juha Saarinen are among those who say the only way to stop escalating cyberattacks is to make it illegal to pay a cyber ransom.

The previous Government, and the current one, have both told the *Herald* the same thing: they won’t consider the move because it would criminalise victims.

But during a 2023 trip to New Zealand, an Oxford academic said it might actually already be illegal to pay a cyber ransom in many cases, given the volume of cyberattacks that come out of Russia.

Professor Ciaran Martin – also chairman of the multinational security firm CyberCX – earlier noted that the invasion of Ukraine led New Zealand’s Parliament to pass the Russia Sanctions Act 2022.

That means paying a cyber ransom could constitute breaking sanctions and could result in criminal penalties of up to seven years in prison and/or a fine of $100,000 for individuals or up to $1m for organisations.

**Chris Keall is an Auckland-based member of the *Herald’s* business team. He joined the *Herald* in 2018 and is the technology editor and a senior business writer.**