New Zealand “ManageMyHealth” hack exposes thousands of patients’ medical records

John Braddock
18 January 2026

A ransomware attack on New Zealand’s “ManageMyHealth” (MMH) medical portal, disclosed on New Year’s Day, has exposed sensitive medical records of some 127,000 patients nationwide.

The cybercriminal group “Kazu” claimed responsibility for stealing up to 430,000 documents and demanding a ransom of $US60,000. The data breach affected 6-7 percent of the MMH platform’s 1.8 million registered users, who are locked into patient record systems of 60-75 percent of general practice (GP) clinics.

MMH, which is linked to the widely-used Medtech practice management system—owned by an Australian private equity firm—carries an array of patient information including test results, diagnoses, prescriptions, doctors’ notes and health histories. It has become NZ’s dominant tool for recording and managing interactions between health centres, GPs and patients. Intimate data threatened with exposure included mental health diagnoses, sexual assault documentation, medications and medical photographs.

The hackers claimed to have successfully extracted ransom money from healthcare companies in Asia and Africa. Samples of the NZ hacked data were initially published on the dark web but following the passing of a ransom deadline the information was removed from Kazu’s online presence after MMH obtained a High Court injunction preventing anyone from accessing or sharing the stolen data.

Thousands of patients still remain anxious that their privacy was breached. For nearly two weeks GPs didn’t know which practices had been affected, or what information was taken. There were reports of the portal’s website crashing amid the volume of requests for information, along with warnings that patients’ details might be used for identity theft. By January 10, MMH had notified only half the 127,000 patients whose data had been stolen.

On January 12 private health provider CanopyHealth, which specialises in breast cancer diagnosis and treatment, notified of a major cyber-attack on its systems. The company, which runs diagnostic and oncology clinics, breast surgical centres and a drug business, revealed that last July an unknown person had “temporarily obtained unauthorised access” to one of its servers. The company claimed the issue had been “contained” but kept the breach secret for six months.

Such incidents reveal far more than basic cybersecurity failures. They exemplify how decades of market-driven reforms, under governments of all stripes, have transformed essential health services into profit-making centres, placing working-class patients’ private medical information at the mercy of capitalist corporations which operate with impunity. The decades-long privatisation of the health “industry” is a key factor in the austerity-driven underfunding of the public health system itself.

MMH owner and CEO Vino Ramayah admitted that the hackers had accessed the system “through the front door” using valid credentials. The security failure could have been prevented with elementary protections like mandatory multi-factor authentication (MFA), but according to IT experts many health organisations have very poor security controls. Callum McMenamin, a web standards consultant, told RadioNZ he had called out MMH’s lax security six months earlier but the government was “failing to enforce what minimum standards it has.”

According to academic Bryce Edwards, MMH “skimped on security basics (no mandatory MFA, outdated software, apparent neglect of warnings) in order to maximise profit.” Ramayah, he added “chose to run his company on a shoestring and treat patient data as a private asset.”

Edwards further noted: “As a private limited liability company, Manage My Health operates in the shadows. No mandatory transparency reports, no public board meetings, no requirement to disclose security investments.”

Such environments are not confined to New Zealand. In September 2022, Australian telecommunications giant Optus suffered a cyberattack exposing the sensitive data of up to 10

million customers, potentially one-third of the population. Like MMH, the Optus breach involved basic preventable vulnerabilities. Both prioritized cost minimization over security while regulatory frameworks proved toothless. Their responses were characterized by opacity, delayed disclosure, and attempts to evade responsibility.

The National Party's Health Minister Simeon Brown commissioned a limited inquiry by the Ministry of Health (HNZ) into the breach but has washed the government's hands of the affair, declaring; "It is the agency that holds that data that has responsibility," adding that it was up to MMH to notify those affected.

But the MMH breach occurred within the context of blatant underfunding of New Zealand's public health system, which has been subject to some 2,000 job cuts over the past year, including many IT experts. In December, Brown ordered hospitals and public health services to find more than $NZ500 million in "efficiencies," on top of an existing $2 billion annual cost-saving target.

On January 14 a major IT outage hit hospitals across parts of the South Island, preventing clinicians from accessing medicinal dosage information, lab results and patient notes. A similar six-hour outage hit lower North Island hospitals the following day. HNZ officials have already warned of a "funding cliff" looming next June, with "no baseline funding forecast for National Cyber Security beyond 2026."

While healthcare is starved of funding, Defence Minister Judith Collins announced in November that the government is allocating $50 million to boost the Defence Force's (NZDF) protection from cyber threats, part of a $12 billion spend on new military equipment by 2029, in preparation for war with China. Three private NZ companies will be contracted to build the software, along with the NZDF hiring more military cyber specialists.

The crisis in public health is the product of decades of austerity measures under successive governments, including Labour. Thousands of nurses, doctors, ambulance personnel and lab technicians have over recent years taken industrial action over low pay, understaffing and deplorable conditions for both staff and patients in the hospitals. Their struggles have repeatedly been sold out by the trade union bureaucracy with no fundamental resolution.

Following a mass strike by more than 100,000 workers on October 23 last year—which included doctors, nurses, other healthcare workers and teachers as well as off-duty firefighters—the union leaders are seeking to isolate and demobilise their members, in order to push through more wage cuts or freezes.

Security breaches are just one of many class issues that define the country's two-tier health system. More than 20 percent of healthcare services are private with over 1.4 million people, just under a third of the population holding private health insurance. Meanwhile most working-class New Zealanders depend on poor public and semi-public health infrastructure. Worst affected by the MMH breach were 86,000 patients and nearly 50 practices in Northland, one of the country's most impoverished areas.

Governments have for years pursued policies of private sector de-regulation and removal of "red tape" which is deemed to be a burden on profitability. The Privacy Act 2020, like similar legislation internationally, places compliance obligations on organisations themselves, with minimal oversight. In a statement to *Stuff*, the Office of the Privacy Commissioner admitted it has "neither the statutory powers nor the resources to undertake proactive assurance audits of an agency's compliance with best practice security standards for its sector." The result has been open slather for corporations to self-regulate, or not, however they see fit.

The MMH scandal is not an aberration but the logical outcome of treating healthcare as a commodity and patients as profit sources. The solution to these systemic failures cannot come from within capitalism. Data systems must be removed from private hands.

As a basic social right all infrastructure including patient portals, electronic health records, and related systems must be operated by publicly accountable entities, determined by patient need and risk assessment, not profit calculations. That must form part of the socialist reorganisation of society as a whole.