

ManageMyHealth cyber breach exposes wider failures in medical records system - Cecilia Robinson

W

Home Latest news Herald NOW Video New Zealand



142 Herald • 29 Jan, 2026 03:00 PM 10 mins to read

Cecilia Robinson is a founder and co-chief executive of digi-physical primary care provider Tend Health.

THE FACTS

- The ManageMyHealth breach highlights vulnerabilities in how health records are managed and underscores privacy concerns.
- The health sector's handling of information is inconsistent, with both digital and physical systems carrying risks.
- A long-term digital health investment programme aims to improve system resilience and patient safety.

The recent breach involving ManageMyHealth is deeply unsettling. Health records sit at the very centre of our private lives. They contain information we would rarely share with anyone else. When that information is exposed, even indirectly, many experience it as a violation of personal privacy and trust.

This breach is serious. It matters. And it deserves scrutiny. But it also needs to be understood in context. Not as an unthinkable failure in an otherwise pristine system, but as an incident occurring within a health sector where information has long been handled inconsistently, imperfectly and sometimes in surprisingly fragile ways.

That context does not excuse failure. It does, however, make the breach easier to understand.

There is a widespread belief that health information, by its nature, is always treated with exceptional care. That because it is sensitive, it must be secure. That records are stored properly, transferred carefully and governed tightly as a matter of course.

In practice, that assumption has at times been misplaced.

As co-CEO of Tend Health, as we have built and scaled a modern primary care model, my team and I have had a rare window into how medical records are actually managed on the ground. The reality is often far removed from the idea that patient information is consistently stored securely, transferred carefully and governed tightly.

We have seen medical records stored in shipping containers. Filing rooms with no clear ownership or audit trail. Keys lost, shared or discarded because no one can quite remember who is responsible for them. Entire paper files physically mailed between clinics. Patient information photocopied, bundled and transported in ways that would shock people if they understood how routinely this still occurs.

These are not historical anecdotes from decades ago. They are recent, real examples from across the system. They reflect a health sector that has evolved over time, layering new expectations on top of old processes without always stopping to reconsider whether those processes remain appropriate for the scale and complexity of modern healthcare.

For me, this issue stopped being abstract very quickly.

For a period, almost monthly, patient files were sent to my home address instead of the business. Not digitally. Not encrypted. Physical medical records, sometimes thick folders, sometimes loose pages, simply arriving in the post because a provider had searched my name and assumed that was the appropriate destination.

There was no ill intent. These were well-meaning people doing what they believed was required to transfer care.

But intent does not change the outcome. Each envelope was confronting. Not because of what it contained, but because of what it represented: a system where the handling of deeply sensitive information often relies on assumption, habit and individual judgment rather than consistently applied safeguards.

If this can happen quietly and routinely to someone running a healthcare organisation, it is reasonable to assume similar things happen to patients every day without ever being noticed or reported.

Why digital breaches feel more alarming

When a digital platform experiences a breach, it is visible. There is a clear moment of failure. Logs exist. Timelines can be reconstructed. The incident is named, reported and scrutinised.

When paper-based systems fail, the mistakes often fade into the background. A file misfiled. A letter sent to the wrong address. A box left unlocked. A container forgotten behind a clinic. At scale, these failures can appear administrative. To the individual whose records are involved, they are anything but. Health information is deeply personal, and the consequences can be just as serious even if the failure itself is quieter and less likely to be recognised.

Digital systems feel risky because their failures are observable. Physical systems feel safer because their failures are often invisible. In practice, both carry risk. One is simply easier to see.

New Zealand has already experienced multiple information failures within the public system, including incidents involving Health New Zealand and its predecessor organisations. These were not fringe operations. They were central institutions operating under significant pressure, using infrastructure that has been asked to do far more than it was ever designed for.

Seen in that light, the ManageMyHealth breach does not sit outside the system. It sits squarely within it.

None of this removes responsibility from organisations that hold health data.

When a platform holds sensitive information at scale, expectations are rightly high. Patients expect strong security, careful access controls and responsible handling. When those expectations are not met, scrutiny is appropriate.

But it is also important not to oversimplify the narrative.

Blaming a single platform, or assuming that removing one system would meaningfully reduce risk, misunderstands how health information actually flows. Records move across hundreds of systems, formats and organisations. Weakness in one part of the chain rarely exists in isolation.

The breach deserves scrutiny on its own terms. It also exposes broader realities about how health information is handled across the system every day.

It is important to be honest about where the greater risk now sits.

The lack of digitisation in our health system is, in many respects, a much bigger threat to patient safety and equity than the existence of digital records themselves. Fragmented, paper-based and poorly connected systems make safe, co-ordinated care harder than it needs to be. They increase the likelihood of missing information, duplicated tests, medication errors and delayed treatment. They rely heavily on patients' memory at moments of stress, crisis or incapacity.

That reality is now increasingly acknowledged at a system level. In late 2025, Health Minister Simeon Brown set out a long-term digital health investment programme, signalling a shift away from the stop-start approach that has characterised the last decade. For the first time, digital health has been framed not as a series of isolated projects, but as core national infrastructure requiring sustained, multi-year investment and planning.

Importantly, this is work that cannot afford to become politically fragile. Health data systems take years to design, implement and embed, and decades to deliver their full value. If direction and funding shift with each change of government, risk and fragmentation increase rather than reduce. Treating digital health as true national infrastructure therefore requires a bipartisan commitment to continuity, funding stability and long-term stewardship across political cycles.

The programme outlines a 10-year horizon focused on stabilising existing systems, reducing fragmentation and progressively enabling a shared digital health record that can be accessed across settings. Early phases focus on shoring up ageing platforms, improving interoperability and addressing basic digital capability gaps that still exist where paper remains dominant. Later stages aim to support more connected models of care, including telehealth and improved data sharing across primary, secondary and emergency services.

While initial funding commitments remain modest compared to the scale of the challenge, the significance lies less in the dollar figure and more in the acknowledgement of risk. Much of the risk now emerging around health data is not the result of digitisation itself, but of prolonged underinvestment in it. Digital health has often been treated as an operational upgrade rather than essential national infrastructure, with funding prioritising immediate delivery pressures over long-term resilience.

As a result, many organisations are running highly sensitive systems on ageing foundations, with limited capacity for continuous security improvement. At the same time, cyber crime has evolved rapidly. Healthcare data is now one of the most targeted and valuable categories of information globally. Responding to that threat requires ongoing investment in security capability, governance, monitoring and skilled people.

When investment lags, risk does not disappear. It accumulates quietly. Manual workarounds increase. Fragmentation deepens. Complexity grows in ways that are often invisible until something fails. The risk is not that health information is digital. The risk is that too much of it still isn't, or that it sits in systems that cannot reliably talk to each other when it matters most.

Digital health records exist because access to the right information at the right time matters. When someone arrives at hospital unconscious, confused or critically unwell, immediate access to their medical history, medications, allergies and diagnoses can be the difference between life and death. It can prevent a fatal drug interaction. It can guide urgent clinical decisions. It can save precious minutes when minutes matter.

A physical file in a storage container cannot do that. A paper record sitting in a filing room across town cannot do that. A folder mailed days later cannot do that.

The absence of digitisation also has equity consequences. Communities that already experience poorer health outcomes are often the same communities most affected by fragmented records and manual processes. When information does not follow the patient, those with the least capacity to advocate for themselves are the ones most likely to fall through the gaps.

This is why digital health investment matters beyond efficiency or convenience. It shapes who gets timely care, who experiences continuity and who is left navigating a system that does not join up around them.

Digital systems are not inherently safe or unsafe. They are tools. When poorly governed or under-resourced, they introduce risk. When thoughtfully designed and properly supported, they reduce it.

Seen through that lens, the real danger is not that health data is digital. It is that too much of our system still isn't.

There is often an unspoken expectation that health data systems should be perfect. That breaches should never occur. That risk should be eliminated entirely.

That expectation is understandable. It is also unrealistic.

You can build an extraordinary house with reinforced doors, alarms, cameras and monitoring services, and still, one day, someone may break in. That does not mean the house was a mistake or poorly built. It means risk exists.

Healthcare data is no different. The presence of risk does not automatically imply negligence. What matters is how that risk is understood, managed and responded to when something goes wrong.

What patients can do

Patients should not be expected to compensate for system-level weaknesses in how health information is managed. That responsibility sits squarely with the system.

However, in the reality we are operating in today, there are practical steps individuals can take to better understand and protect how their information is handled.

It is reasonable to ask how your medical records are stored, who can access them and how they are transferred between providers. Maintaining a simple personal health summary, including diagnoses, medications and allergies, can be invaluable when care crosses organisational boundaries.

Using strong security on patient portals, including unique passwords and multi-factor authentication where available, and questioning unexpected communications are sensible precautions.

These actions are not solutions. They are simply ways individuals can navigate today's environment while broader change catches up.

The recent breach is uncomfortable because it challenges assumptions many of us would prefer not to examine. That health data is always safe. That systems are tighter than they really are. That risk lives somewhere else.

It is easier to be shocked than to be honest.

Digital records are not inherently dangerous. Physical records are not inherently safe. Both carry risk. Both require care.

Understanding that may not make breaches feel better. But it does make them make sense.

Catch up on the debates that dominated the week by signing up to our Opinion newsletter – a weekly round-up of our best commentary.

Catch up on the debates that dominated the week by signing up to our [Opinion newsletter](#) – a weekly round-up of our best commentary.
