16 January 2026

Dear Murray,

We are writing to you with a further update regarding the December 2025 cybersecurity incident and reaffirm our commitment to protecting patient and practice data and maintaining the trust you place in us.

Since the incident occurred, we activated our response plan and engaged the services of third-party cybersecurity specialists who focused on network security and containment.
We now provide an overview of these steps as we move to the next phase of the incident response process.

Our actions and status

- Containment – Investigations led by our advisors have found that the incident has been contained, and our systems continue to operate securely.
- Law Enforcement - We are working closely with New Zealand Police and relevant regulatory and sector agencies, providing full cooperation and assistance as part of the ongoing investigation.
- Privacy – We have been rolling out notifications in compliance with our privacy obligations and have engaged with the Office of the Privacy Commissioner to ensure we take appropriate steps.
- Injunction - We have taken formal legal action, including obtaining a High Court injunction, to prevent any unauthorised use, disclosure, or dissemination of the affected data.
- Security - Our environment remains under continuous 24/7 monitoring, with no evidence to date of compromise to the core Manage My Health patient portal or associated practice management systems. We now step through these assurances below.

Independent assurance and security governance

Managed My Health has an ongoing cybersecurity programme to ensure the continuous strengthening and resilience of our network. This includes the following:

- Certification - Our organisation operates under a fully implemented ISO 27001–certified Information Security Management System (ISMS), which governs our policies, controls, risk management, incident response, and continuous improvement processes.
- Validation - We have engaged independent forensic cybersecurity specialists to investigate the incident, validate containment measures, and review our environment.
- Testing - Independent Vulnerability Assessment and Penetration Testing (VAPT) of our production systems is currently underway to provide additional confirmatory assurance.

These independent reviews sit alongside our own internal security tooling, controls, and governance processes to ensure multiple layers of verification and accountability.

Our commitment to you

We recognise that incidents of this nature can understandably cause concern for practices, partners, and patients.

Please be assured that we care deeply about the responsibility entrusted to us. Every decision we have taken has been guided by the principles of patient safety, data protection, transparency, and long-term resilience.

We will continue to:

- Ensure dedicated support is made available to our community
- Work collaboratively with authorities and sector stakeholders
- Act on the findings of independent experts
- Strengthen our security controls and monitoring
- Keep you informed as independent verification activities are completed

General updates are provided on our website together with FAQs for any common questions users may have. These are available here: https://managemyhealth.co.nz/mmh-cyber-breach-update/

Thank you for your continued confidence and partnership. We remain committed to earning and upholding your trust, today and into the future.

Yours sincerely,

Vino Ramayah
Chief Executive Officer
Manage My Health

Level 1, Cereus Health House, 48 Market Place
Viaduct Harbour, Auckland 1010