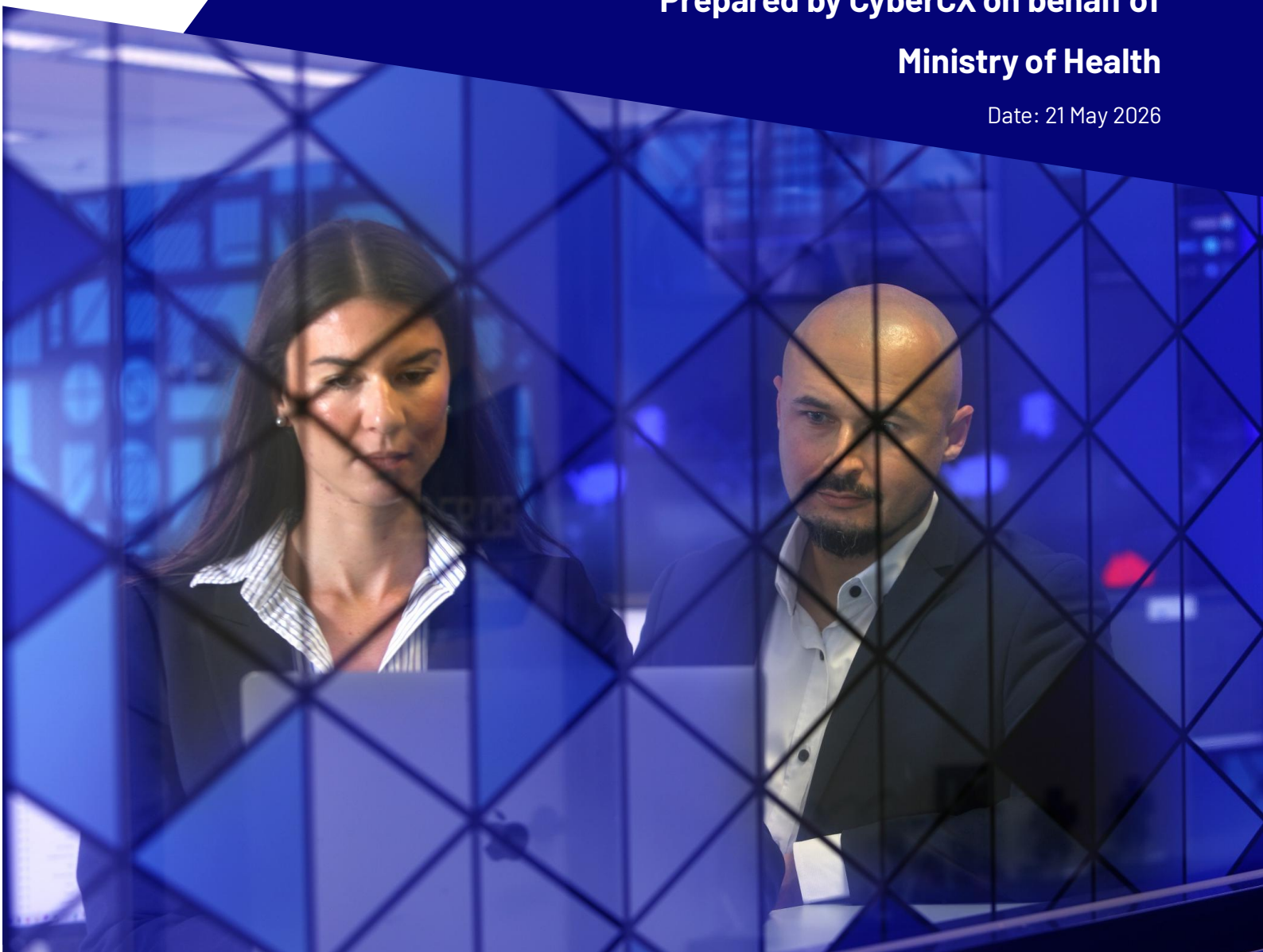
Manage My Health Cyber Security Review Phase 2

Prepared by CyberCX on behalf of Ministry of Health

Date: 21 May 2026



Document Control

Engagement Details

Report Details	
Document Title	Manage My Health Cyber Security Review Phase 2
CyberCX Reference	PR-023678
CyberCX Author(s)	Dan Richardson, Hayley Power, Mandy Elson
Client Contact	[name removed], [name removed], [name removed]

Version Control

Version	Details	Date	Author(s) / Reviewer(s)
0.1	Initial internal draft	15 April 2026	D. Richardson, H. Power, M. Elson
0.2	Amended draft	20 April 2026	D. Richardson, H. Power, M. Elson
0.3	Amended draft	24 April 2026	D. Richardson, H. Power, M. Elson
0.4	Quality assurance	24 April 2026	T. Sewell
0.5	Client draft issued for feedback	28 April 2026	D. Richardson, H. Power, M. Elson
0.6	Formatting amendments	29 April 2026	D. Richardson, H. Power, M. Elson
0.7	Inclusion of client feedback	30 April 2026	D. Richardson, H. Power, M. Elson
1.0	Final Version Released	06 May 2026	D. Richardson, H. Power, M. Elson
1.1	Updated following stakeholder feedback, formatting amendments	15 May 2026	D. Richardson, H. Power, M. Elson
1.1a	Abridged version	18 May 2026	D. Richardson, H. Power, M. Elson
1.2	Updated following stakeholder feedback	18 May 2026	D. Richardson, H. Power, M. Elson
1.2a	Abridged version	18 May 2026	D. Richardson, H. Power, M. Elson
1.3	Updated following additional stakeholder feedback	21 May 2026	D. Richardson, H. Power, M. Elson
1.3a	Abridged version	21 May 2026	D. Richardson, H. Power, M. Elson

Table of Contents

Executive Summary

On 30 December 2025, the privately-owned patient portal operator ManageMyHealth (MMH) became aware of unauthorised access to its systems. A significant number of portal users had data stolen by the threat actor, with claims of over 400,000 documents having been exfiltrated from one of MMH's systems.

The scale and scope of this incident represent one of the largest and most impactful cyber security incidents in New Zealand history, with the potential to cause significant downstream harm to individuals whose data was stolen.

In early 2026, CyberCX was engaged by the Ministry of Health (MoH) to undertake an independent assurance assessment of the MMH incident to:

- assess the cause(s) of the incident;
- review the adequacy of the data protections that were in place;
- review the response to the incident; and
- recommend any improvements required to prevent similar incidents occurring.

To complete this assessment, CyberCX conducted a comprehensive review of available documentation and other artefacts pertaining to the incident. CyberCX also interviewed key stakeholders involved in the incident response, including MMH, Health New Zealand (HNZ), the National Cyber Security Centre (NCSC) and New Zealand Police (NZ Police).

The key observations the CyberCX assessment team noted during the assessment are:

- MMH were unprepared for an incident of this nature, had significant control failings in their technology environment, and were likely not aligned with HISF requirements prior to the incident occurring.
- The management of the incident was generally appropriate to its criticality and impact of the incident; however, significant patient notification and communications issues were noted.
- Had more appropriate technical controls at MMH been in place prior to the incident, the incident may have been avoided, or the impact lessened.
- MMH has improved their technical controls following the incident, however only limited external technical assurance of these improvements has taken place at the time of writing (April 2026).
- As a supplier to HNZ and the broader health sector, and as holder of sensitive health data, a more stringent third-party cyber risk assessment process and governance should have been applied to MMH by entities that hold contracts with them.
- The interlocking HISO and HISF frameworks are the main vehicles to provide security and privacy guidance to third-party suppliers that hold personal health information, such as MMH. These frameworks lack any form of enforcement mechanisms, outside of contractual penalties.

This incident, alongside other cyber incidents in the health sector in early 2026, should serve as a call to action for the health sector, and New Zealand organisations more broadly, to improve cyber security controls and governance.

We thank all participants in the assessment for their time, transparency and willingness to engage as part of this process.

As part of this assessment activity, the assessment team has provided twelve recommendations aimed at both preventing similar incidents in the health sector and minimising the impact of future incidents within the sector. Ratings below are assigned based on potential to reduce risk; and timeframes are estimated recommended timeframes to address each recommendation.

The recommendations are summarised below, ordered by rating:

Reference	Recommendation	Recommended Owner	Rating	Timeframe
REC10	MMH to undertake further security reviews (penetration tests) and/or purple/red team activity on the MMH web and mobile applications. The results of this review should be shared with HNZ.	MMH	High	Within 3 months
REC11	MMH to undertake a full external assessment of HISF compliance by a provider who is conversant with the HISF framework. The output of this should be provided to HNZ as a contract holder and MoH as the health system monitor.	MMH	High	Within 3 months
REC03	HNZ to seek further clarification of any critical services provided to MMH by third-party suppliers, to ascertain the nature of the contract in place, and patient data accessible to third-party suppliers.	HNZ	High	Within 3 months
REC06	MoH, in their role as health system monitor, write to HNZ (and other contract holders) to confirm how they manage HISF compliance and what actions have been taken in cases of non-compliance.	HNZ	High	Within 6 months
REC07	HNZ to consider measures to strengthen HISF compliance among suppliers to the health sector, in particular suppliers that hold sensitive health information.	HNZ	High	Within 6 months
REC02	MoH and HNZ to better define process and procedures for patient notifications in the event of data breach involving data held by a third-party supplier, with defined roles and responsibilities set.	HNZ/MoH	High	Within 6 months

REC04	HNZ to comprehensively review and uplift its third-party risk management practices in-line with recommendations in the **[vendor name removed]** Cyber Maturity Assessment Report (Sep-25).	HNZ	High	6-12 months
REC09	MoH, as the health system monitor, defines thresholds and attributes for "high-risk" suppliers to the health sector; and regularly receives assurance from entities that hold contracts with "high-risk" third-party suppliers regarding their security status and HISF compliance.	MoH	Medium	Within 6 months
REC08	HNZ and other health sector entities to maintain registers of their suppliers that store or process sensitive health information, tiered by risk factors (including volume of records, sensitivity, criticality to care delivery).	HNZ	Medium	6-12 months
REC12	HNZ to seek assurances from MMH of the data management practices, aligned to HISF requirements and best practice, including details of user onboarding and offboarding processes, data retention periods, data access audit methodologies and whether patient data is accessible to any of MMH suppliers or related parties.	HNZ	Medium	6-12 months
REC01	HNZ to undertake regular tabletop incident response exercises with critical suppliers that hold sensitive health data, to practice and better define incident roles and responsibilities and ensure alignment across the sector.	HNZ	Medium	6-12 months
REC05	HNZ to develop a plan to engage with the sector to drive better third-party security assurance outcomes across the health sector, in line with HISO and HISF requirements.	HNZ	Low	12-24 months

1 Background of the Incident, Impact and Timeline

On 30 December 2025, the privately-owned patient portal operated by Manage My Health (MMH) - an entity owned by Cereus Health Group, and supplier to HNZ and the health sector more broadly, became aware of unauthorised access to its systems.

MMH operates a patient-facing health portal delivered via web, iOS, and Android applications. On the consumer side, patients can book appointments, request repeat prescriptions, message their practice, attend video consultations, and view records and lab results. On the health provider side, GP practices use it to manage those same interactions and push information out to patients. The company reports around 1.8 million registered users and more than 680 health centres using the platform, which makes it the largest patient portal in New Zealand by some margin.

MMH is not itself the source-of-truth clinical system. Practices do not upload records directly; data is synced from Practice Management Systems (PMSs) via an external interface, which sit upstream of the portal. In effect, the MMH portal is effectively a downstream aggregator of clinical data from PMS platforms.

The threat actor responsible for the incident claimed to have taken 108GB of data, made up of 428,337 files including names, medical records, test results and prescription details from the MMH portal platform. A small sample of data was published as proof.

At the time of the incident MMH had approximately 1.8 million registered users in New Zealand. Initial estimates of 126,000 impacted individuals were later downgraded to 99,416 impacted individuals during the incident response process, this figure was subsequently confirmed by MMH.

The threat actor responsible for the incident self-identified as "Kazu" — the same alias linked to an earlier 2025 exfiltration from Nepal's Ministry of Education. The threat actor posted a US$60,000 ransom demand initially setting a deadline of 15 January. However, this was later moved forward to 4 January, with a demand for payment within 48 hours accompanied by threats made via Telegram to release data within 48 hours.

The assessment team did not directly examine the affected data, but it has been reported the bulk of affected individuals (around 86,000) sat within Northland practices. Media reporting based on the published samples of data indicated the corpus included clinical notes for health providers, intimate imagery and documents such as scans of passports uploaded by users — high-sensitivity material that could drive further serious downstream harm scenarios (such as re-traumatisation, blackmail and identity fraud).

The MMH incident attracted intense media scrutiny due to the sensitive nature of the data exfiltrated and in the hands of the threat actor which were heightened by journalists claiming direct communication with the threat actor.

The incident triggered a response from MMH, HNZ and the broader health sector, supported by third parties and the wider government system.

The MMH incident represents one of the largest and most impactful cyber security incidents in New Zealand history, with the potential to cause significant downstream harm to individuals whose data was stolen

2 Quantifying the scope of the Incident and Breach

The MMH incident occurred due to a valid user's credentials (username and password) which had been compromised by an infostealer type malware (Lumma Stealer) as part of a separate sequence of events, being used by the threat actor to log in to the MMH portal. The threat actor then used flaws in an API (Application Programming Interface) component of the portal to obtain sensitive patient data.

This type of attack is neither technically sophisticated, nor particularly uncommon. Incidents that are similar in nature include the Snowflake customer breaches (2024), Peleton (2021), Optus (2022) and US Postal Service (2018).

Forensic analysis undertaken by **[vendor name removed]** on behalf of MMH identified that one module of the portal system — Health Documents — was compromised, rather than the core application database or other MMH systems. The assessment team concurs with this analysis and saw no evidence to confirm any wider compromise of MMH systems.

As is common during a cyber incident response, detail regarding the impact and scope of the incident were fluid and only partially available during the initial stages of the process. This is common, as substantial technical effort is required to verify and quantify an incident and data impacted. This verification and quantification process takes time to complete.

The assessment team sighted no evidence to suggest that MMH were intentionally withholding information from HNZ or the All of Government (AoG) Incident Management Team (IMT) during the initial stages of the incident or as the incident response process progressed.

Any details that were supplied to stakeholders that were misrepresented or incorrect are likely due both to capacity and capability constraints at MMH and decisions made to provide information regarding the scale and scope without providing caveats around these details.

However, the assessment team noted the HNZ timeline does indicate requests for technical reports from MMH were not delivered upon in a timely manner; and on 12 January 2026, HNZ emailed MMH with a statement of "reduced trust" and requested further evidence of forensic containment.

Regarding the files taken, there is some variance between threat actor claims of having taken 428,337 documents and the forensic reporting of 430,649 unique files being downloaded. This discrepancy is not fully explained in the forensic reporting, though could be due to the threat actor not being able stage and transfer all files (transfer failures) or duplication of files taken. There was no information sighted to infer that the forensic investigation methodology would have incorrectly determined the number of files affected.

In terms of quantifying impacted individuals, MMH statements did not uniformly quantify exact numbers of patients indicated. Rather, percentages of registered patients or estimates were used. On 1 and 2 January 2026, it was stated approximately 7% of the 1.8 million patients had been affected, which equates to an estimated 127,000 individuals. By 9 January MMH released a statement indicating that "*approximately 125,000*" patients were impacted. However, as of April 2026, the MMH's FAQs related to the cyber breach revised this figure, stating that "approximately 5-6% of users were affected by this incident," which suggests that the number of affected individuals ranges between 90,000-108,000.

This variance in reported figures is likely attributable to evolving technical findings throughout the course of the incident. The assessment team noted that during the interview with MMH they quantified the number of impacted individuals at "99,000", explaining the reasons behind the discrepancies due to "*the error was that there was a subfolder that we thought had been breached, but they didn't get into that subfolder. We thought that as they got into the parent folder that everything underneath that was affected, but in fact there was a subfolder that they didn't get to.*"

The figure of 99,000 impacted individuals is in line with MMH's FAQs related to the cyber breach and highlights the dynamic nature of the incident response, with further technical details becoming available over time. This was subsequently confirmed to be 99,416 impacted individuals.

Given no other data held by MMH has surfaced in other contexts or appeared for sale, at the time of writing (April 2026) and to the knowledge of the assessment team, it would appear that the scale and scope of the incident was correctly quantified by the closing stages of the incident response process.

3 Assessment of Incident Response Process

The response to the MMH incident was complex, multi-faceted and involved a wide range of stakeholders. The assessment team reviewed available forensic reports, internal and external communications; and interviewed key parties involved in the response including MMH, HNZ, NZ Police and NCSC.

3.1 Manage My Health response

MMH were notified of the incident by the NCSC and HNZ late on 30 December 2025, and were aware of the incident after receiving an email notification from the threat actor. MMH formally declared an incident in the early of hours of 31 December 2025. MMH subsequently engaged external legal counsel **[vendor name removed]** and **[vendor name removed]** to provide technical Digital Forensics and Incident Response (DFIR) support by 31 December 2025.

As stated by MMH in the interview with the assessment team, on or around 12 January 2026 MMH engaged **[vendor name removed]**, a legal and advisory firm to replace **[vendor name removed]** due to potential conflict of interest issues.

The assessment team noted that MMH had a basic cyber incident response plan in place prior to the incident, it was not tested in a tabletop exercise or similar crisis management response training process prior to the incident occurring.

The assessment team **recommends [REC01]** that HNZ undertake regular tabletop incident response exercises with critical suppliers that hold sensitive health data, to practice and better define incident roles and responsibilities and ensure alignment across the sector.

3.2 Legal and government response

MMH obtained a High Court injunction on 5 January 2026 restraining publication or use of the stolen data. Notifications were made under the Privacy Act 2020 (Privacy Act) to the Privacy Commissioner, and MMH engaged with HNZ, NZ Police, and the NCSC during the early stages of the incident. An AoG IMT was set up and operational on 1 January 2026, to assist and advise MMH, provide a conduit to the wider government system if required and to consider broader system risk. The IMT was led by HNZ. Separate working groups for AoG communications and technical advice were also stood up.

The assessment team notes that NZ Police continue to work on a criminal investigation in relation to the MMH incident at the time of writing (April 2026).

3.3 Communications and sector engagement

From the early stages of the incident there was intense media scrutiny of MMH, the affected platform and the incident response process. The first national media reporting appeared on 31 December 2025. The media reporting interest was likely compounded by both a claim the Threat Actor made on 30 December 2025 on a cybercrime forum claiming responsibility for the incident, and the fact the incident occurred during a period of public holidays.

Many health sector stakeholders and customers, such as Public Health Organisations (PHOs), clusters of General Practitioners (GPs) and individual medical practices initially learned of the breach from media reporting rather than direct notification from MMH. More positively the assessment team noted MMH subsequently provided regular meetings and written updates to PHOs and the general practice community through January and February 2026.

By 7 January 2026, MMH commissioned a free call '0800' number for affected individuals and launched a data breach page on their website with further information and a tool to provide incident status updates for potentially impacted individuals. However, it was reported that both the 0800 number and the MMH website were regularly overwhelmed and unable to service requests in the first two weeks of January, resulting in patient complaints.

Additionally, MMH implemented region locking on the affected portal on 1 January 2026. The impact of this was to essentially block users accessing the portal from outside of New Zealand. However, this control is a blunt instrument being technically simple to circumvent and affected legitimate users from accessing the portal. This action, while a reasonably standard measure, may have compounded both real and perceived access issues by affected individuals and other MMH portal users.

The assessment team noted that notifications for impacted individuals were often confused, overly optimistic and inaccurate. In their initial public statement on 1 January 2026, MMH confirmed that they would notify affected individuals directly via email, in line with the requirements of the Privacy Act. On 3 January 2026, MMH provided further clarification, specifying that notifications to impacted individuals would begin during the week of 6 January.

Notifications to affected individuals began on 9 January 2026 and were subsequently issued in stages on a cohort basis throughout January, February, and March 2026.

The initial timing for notification, as outlined by MMH, ultimately proved overly ambitious. Coordination challenges with HNZ and other stakeholders, coupled with the sheer scale of the notification effort, significantly delayed the process which extended over several weeks rather than being completed within the promised early January timeframe.

MMH also mistakenly notified some unaffected users after starting the notification process before completing the forensic investigation. While this decision can be considered defensible—made "*out of an abundance of caution and in the interest of transparency*"—it likely caused confusion and frustration among both affected and unaffected portal users.

According to MMH's update on 15 March 2026, all patient notifications have now been completed.

The assessment team **recommends [REC02]** that HNZ and MoH better define process and procedures for patient notifications in the event of data breach involving data held by a third-party supplier, with defined expectations and roles and responsibilities set.

More broadly, MMH's communications during the incident were largely CEO-led and ad hoc, particularly in the early stages of the response. A public holding statement was posted on the MMH website on 1 January 2026, with further updates provided as verified information became available. This was supplemented by media interviews with the CEO, including appearances on Radio New Zealand and Newstalk ZB. While MMH may have received communications advice from HNZ and NCSC, and a third-party (Alexander PR), it is unclear to what extent this advice was implemented during the initial phases of the response.

While a full review of MMH's crisis communication strategy is outside the scope of this assessment, the approach appeared transparent in principle but poorly structured in execution. While MMH's openness and willingness to acknowledge faults and engage with the media was unusual and commendable, the lack of a clear and organised communication plan meant this transparency contributed to reputational damage rather than restoring trust. Notably, the small size of the MMH team responding to the incident during the holiday period, coupled with visible fatigue across the team—including the CEO—raised questions about whether media interviews should have been conducted at all, given the heightened risk of miscommunication in such circumstances.

Based on a scan of media articles and commentary related to the incident, public sentiment regarding the incident reflected by media appeared to be overwhelmingly negative, a specific example of this was the CEO of a Primary Health Organisation publicly stating on 6 January that he had *"less than zero percent confidence*" in MMH's handling of the incident.

3.4 Technical response

On 31 December 2025, MMH engaged **[vendor name removed]**, a credentialled provider of Digital Forensics and Incident Response (DFIR) services, to undertake the technical response to the incident.

The assessment team reviewed available forensic reports and broadly assesses the DFIR component of the response was carried out to a professional standard. Regarding investigative steps, the incident was relatively straightforward in that indicators identified would be used for filter down searches for the next evidence source until they got to the final results. As such, the assessment team has no objections as to this overall approach.

At a more granular level, there are some concerns around the methodology used, particularly regarding possible gaps in the approach where they may not have been able to identify all potential threat actor activity or historical compromise. The following are specific gaps where evidence may have been missed or not documented within the final report. This information may exist in other artefacts that the assessment team did not have access to.

[Further details removed as these reports are legally privileged]

3.5 Resolution of the incident

As previously noted, the threat actor claimed to have exfiltrated 428,337 files totalling 108GB from MMH's health documents module and demanded a ransom of US$60,000 (approx. NZ$104,000) by an initial deadline of 15 January 2026.

The initial 15 January 2026 deadline was brought forward to early Tuesday 6 January 2026 and then subsequently extended to 0500 Friday 9 January, which also passed without further publication.

MMH declined to confirm whether it engaged with the attackers and as per the standard guidelines the government publicly recommended against payment.

The incident effectively wound down without the threatened bulk release and in operational terms the active extortion phase ended by mid-January 2026 with the data not publicly released, and

the initial samples taken down. Ultimately leaving the reputational, regulatory and policy fallout, rather than further leaks, as the lasting consequence of the incident.

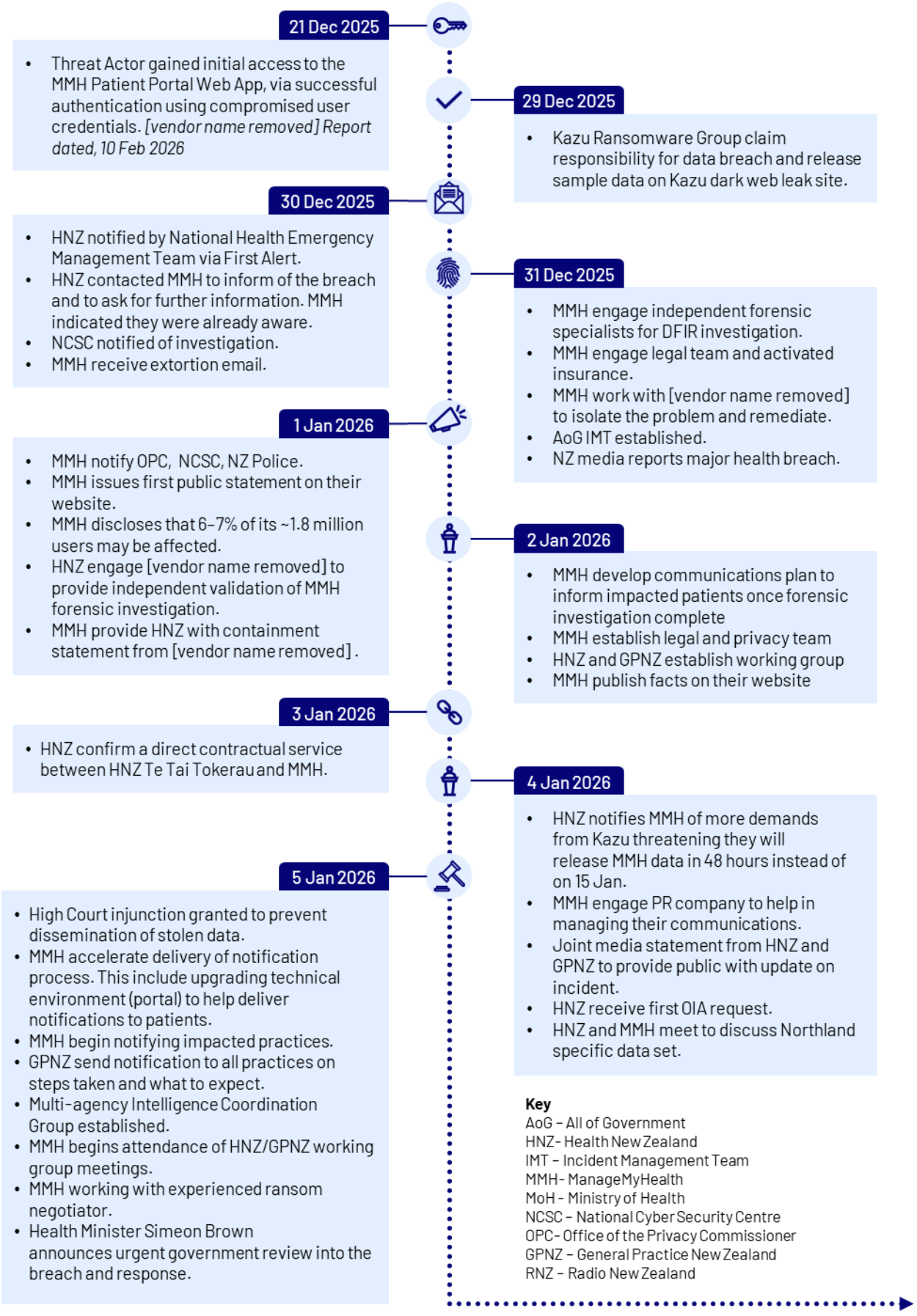
It was further noted in MMH's artefacts and interview that during January 2026:

"Forensic investigation completed and findings refined, confirming limited scope and no impact to GP PMS systems or core infrastructure."

As with any incident involving a data breach by a threat actor, a residual risk remains that threat actor has retained copies of the data exfiltrated and this data may reappear in the future. Though at the time of writing (April 2026) there is no evidence to suggest this is the case with the data involved in the MMH incident.

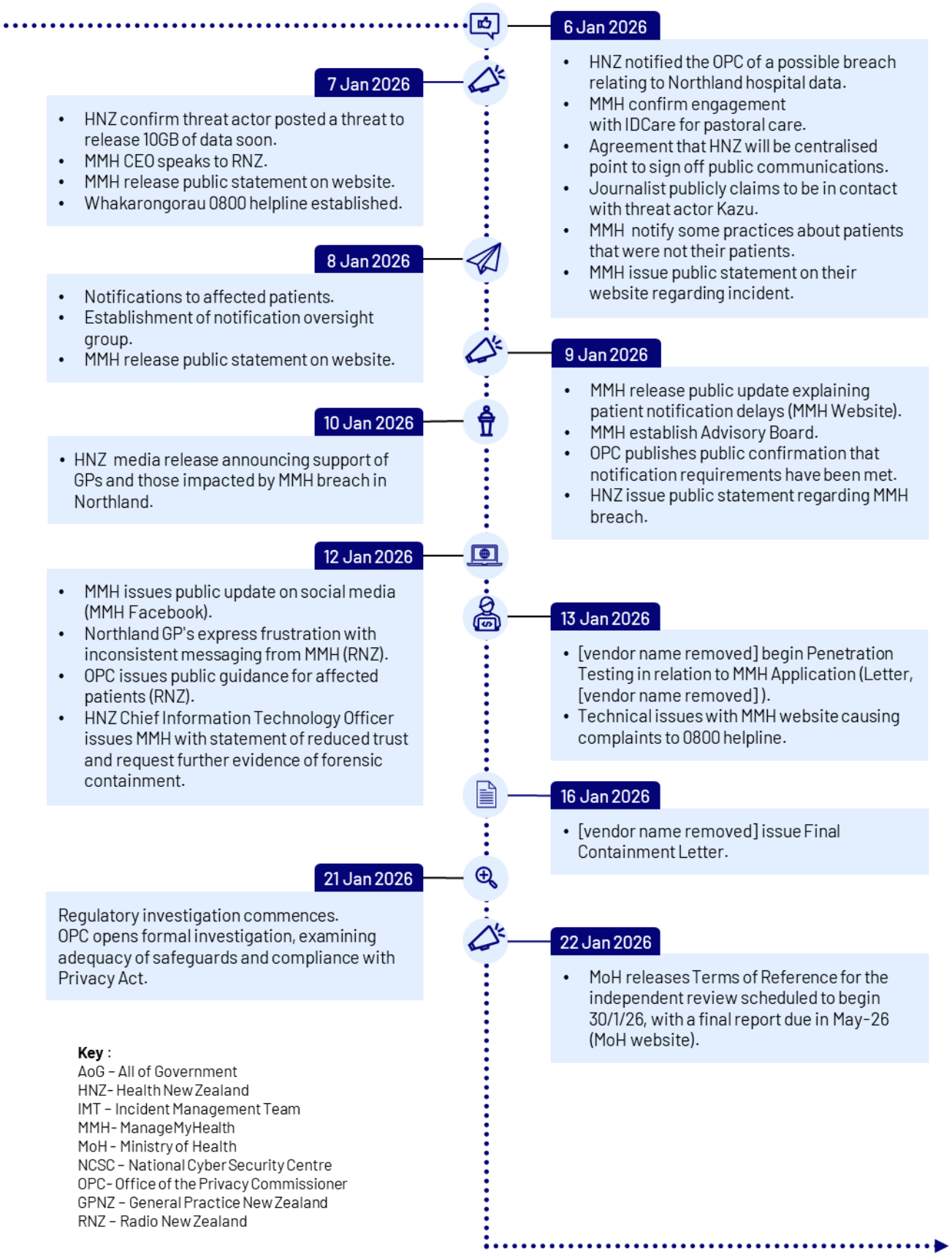
Incident Response Timeline

21 December 2025 – 22 January 2026



Incident Response Timeline

21 December 2025 – 22 January 2026



Key :
AoG – All of Government
HNZ- Health New Zealand
IMT – Incident Management Team
MMH- ManageMyHealth
MoH - Ministry of Health
NCSC – National Cyber Security Centre
OPC- Office of the Privacy Commissioner
GPNZ – General Practice New Zealand
RNZ – Radio New Zealand

4 Manage My Health Privacy & Security Posture Pre-Incident

4.1 Background and obligations

Manage My Health Limited (MMH) is a New Zealand-registered private limited company (NZBN 9429032552072, CIN 2174650), incorporated on 19 September 2008 and remains active at the time of this report (April 2026). It is headquartered, and has a registered office, at Level 1, 48 Market Place, Auckland.

As a New Zealand commercial entity and supplier to the New Zealand health sector, MMH is covered by a number of statutory regimes that apply directly, such as the Privacy Act 2020 (encompassing Health Information Privacy Code 2020) and other standard legal obligations applicable to a New Zealand company.

Health sector frameworks that should have applicable to MMH via contract rather than statute were:

- HISO 10029:2022 Health Information Security Framework (HISF)
- HISO 10029.4:2025 — supplier obligations

The commercial documentation between HNZ and MMH sighted by the assessment team did not contain explicit references to these frameworks or minimum security or privacy obligations agreed to between the contracting parties as could have been expected. The assessment team did not sight commercial documentation between MMH and PHOs, clusters of practices or individual practices.

In addition, MMH had been certified under ISO/IEC 27001:2022 an international standard for information security management systems, designed to support legal and regulatory compliance. For a health technology platform, it establishes standards to protect sensitive health records through controls such as access management, encryption, logging, risk assessments, incident response, and supplier security. In the context of MMH, certification demonstrates compliance with the Privacy Act and sector-specific security requirements such as Health Information Privacy Code 2020, ensuring risks are formally managed and monitored.

Achieving certification helps build trust with stakeholders—including GPs, hospitals, patients, and partners—by demonstrating a commitment to data protection. Certification also requires third-party validation, providing independent assurance beyond self-assessment.

According to the International Accreditation Forum, at the time of the MMH incident, MMH New Zealand's ISO 27001 accreditation had expired, meaning it was no longer certified. During the assessment team interview with MMH, they stated they believed they were ISO 27001 certified. It has subsequently been established that MMH Global Limited hold active certifications for ISO 9001 and ISO/IEC 27001:2022, MMH New Zealand appears to be included in MMH Global Limited's certifications, as a global certificate covers entities and sites specifically listed within its scope.

4.2 Manage My Health company background and related parties

Understanding key suppliers to third-party providers to the health sector is an important consideration when quantifying supply chain risk.

[Details withheld for privacy reasons]

MMH is a relatively small organisation, with approximately 20 employees, which is not uncommon for a Software-as-a-Service (SaaS) platform company.

A related entity, **[vendor name removed]** (**[vendor name removed]**) is an Indian company headquartered in Chennai. **[Details withheld for privacy reasons] [vendor name removed]** appears to function as MMH's 'build-and-run' engineering arm and appears to be the original developer of the widely used PMS platform **[vendor name removed]**, though the current status of the **[vendor name removed]** /**[vendor name removed]** relationship is unclear. At the time of writing a page on **[vendor name removed]** corporate website states: "**[vendor name removed]** *has been the technology partner behind ManageMyHealth (MMH) since its inception—driving development, localisation, and innovation across three distinct healthcare systems.*"

[Details withheld for privacy reasons]

In theory, the obligations contained in the HISO 10029:2022 Health Information Security Framework (HISF) should flow down to related parties such as **[vendor name removed]** through back-to-back contracting. As it was outside the scope of this assessment, the assessment team did not have access to any contracts that exist between MMH and **[vendor name removed]** to verify that that this was the case. The contractual applicability of HISF provisions between MMH and **[vendor name removed]** is potentially weakened by the drafting quality of said contract, the related-party contracting risk, and a lack of direct leverage or enforcement between HNZ (or other NZ contracting entity) and **[vendor name removed]**; with MMH having to seek remedy to any breach under their own contract with **[vendor name removed]**. This arrangement may indicate a related party, or fourth party supply chain risk.

The assessment team **recommends [REC03]** that HNZ, a contract holder with MMH, seek further clarification as to the services provided by **[vendor name removed]** to MMH, the nature of the contract in place, their alignment with HISF and patient data accessible to **[vendor name removed]**.

4.3 Pre-incident capability, technical controls, process

While it is difficult to fully and comprehensively assess the historic platform state of the MMH portal prior to the incident, several markers can serve as a guide to infer a pre-incident approximation of the state of the pre-incident capability, technical and process controls in place.

4.3.1 Historical security testing reports

A security review (penetration test) carried out by **[vendor name removed]** on behalf of MoH, on the mobile MMH application in April 2019 stated:

> *"The most critical issues relate to the API and the controls placed on the data stored in Manage My Health. Many of the vulnerabilities appear to stem from a lack of best practices around a secure software development lifecycle (s-sdlc)."*

While the issues identified in the 2019 security review are not exactly the same issue exploited by the threat actor during the 2025/2026 incident, they would be considered in the same class of attack (OWASP API Security Top 10 - API1:2023 Broken Object Level Authorization (BOLA) scenario and/or API5:2023 (Broken Function Level Authorization)).

MMH may have subsequently resolved the issues evident in the 2019 report; however, the same class of issue having been exploited in 2025 suggest a lack of best practice regarding secure development practices was still evident. No direct evidence was sighted that MMH had fully resolved the issues identified in 2019. It is noted that similar issues were not detected in security reviews (penetration tests) of the MMH web application and **[vendor name removed]** application and APIs also carried out in 2019.

Responsible vulnerability disclosure by independent security researcher

In December 2022 and again November 2025 an independent security researcher contacted MMH to report a number of issues present in the MMH portal. While the assessment team did not have access to the 2022 report, the 2025 report was supplied and stated:

> *"I reported some of these issues in December 2022, and while I can see that changes were made, they were drastically insufficient and many issues remain unfixed. Additionally, new features developed by Manage My Health have large oversights rendering them insecure."*

The 2025 report was sent to MoH and NCSC, as the independent researcher was unable to contact MMH directly using published support channels. MoH shared this report with MMH and HNZ on 17 November 25, the date of receipt.

The report and details provided to MMH via MoH/NCSC specifically called out issues with the MMH portal's API endpoint security.

Furthermore, the report includes reference to ***[endpoint URL removed]*** which appears to list health documents related to a user, and could be used to gather a list of health documents for any user due to API endpoint weaknesses.

Again, this has enough similarities to the attack method used by the threat actor to exfiltrate large amounts of data (using the ***[endpoint URL removed]*** API endpoint) to have raised serious concerns with MMH and should have prompted rapid remediation of these flaws. While MMH acknowledged the receipt of the notification via MoH/NCSC on 18 November 2025 and claimed to "*have begun our investigation into this matter*" there is no evidence to suggest that this was remediated prior to this incident occurring in December 2025.

It should not be inferred that the independent security researcher involved in the 2022 and 2025 notifications was in any way involved with the incident and they appear to have acted ethically and in good faith in relation to these notifications.

4.3.2 MMH supplied details

As part of the assessment process MMH provided their view of the status of key security and privacy controls in place prior to the incident, these were:

[Details removed]

These controls were highly unlikely to have prevented or detected to the type of attack as experienced in December 2025.

The fact that MMH were notified by third parties rather than through their own detection methods, demonstrates that there were wider significant detective control issues present in the MMH environment prior to the incident. These are summarised in the table below [4.3.3 MMH Control failures against current standards].

4.3.3 MMH control failures against existing standards

HISF (HISO 10029:2022) *	NZISM (v3.8 / v3.9)	NIST Cybersecurity Framework 2.0
Protect: An API authorisation flaw allowed authenticated users to access documents belonging to other patients (broken object-level access control).	**Application security controls were ineffective:** NZISM requires enforcement of authorisation at the application layer. The compromised API did not enforce user-to-data binding.	**Protect (PR.AA / PR.DS):** Identity-to-data binding failed; sensitive data was exposed via authorised sessions.
Detect: The incident was not detected internally; discovery occurred only after attacker disclosure.	**Monitoring and detection:** Required security logging did not surface cross-user access patterns before exfiltration occurred.	**Detect (DE.CM):** Lack of effective monitoring allowed prolonged unauthorised access.
Respond: Harm reduction relied on legal injunctions rather than technical containment alone.	**Incident discovery lag:** Detection via external disclosure indicates baseline monitoring controls were insufficient.	**Respond (RS.MI):** Response focused on post-incident containment rather than rapid internal mitigation.
		Govern (GV.RR): Governance mechanisms did not prevent or detect architectural risk prior to exploitation.

The assessment team concluded that MMH likely had systemic security control issues before the incident. Stronger access controls, monitoring, and secure software development practices could have prevented the incident or reduced its impact by enabling earlier detection.

4.4 The Multi-Factor Authentication Question

At the time of the incident MMH did not enforce any requirements for portal users to use a multi-factor authentication (MFA) method to access the portal.

While MFA controls are not infallible had they been in place it is likely these controls could have mitigated the initial access the threat actor had to the user's portal account and denied the opportunity for threat actor to ultimately enumerate and exfiltrate data in this incident.

When questioned why MFA usage was not enforced, MMH explained that it was optional for users due to concerns about equity for disadvantaged, elderly, and impaired users of the portal.

> MFA enhances security by combining two or more verification factors for accounts, making it harder for unauthorised users to gain access even if one factor is compromised (e.g., password).

While this position was defensible, the assessment team found no evidence that other user monitoring or access control measures - such as requiring users who hadn't logged in for a set period or those accessing the portal from unusual locations (e.g., overseas) to verify their log in via email - had been considered or implemented before the incident.

Furthermore, there did not appear to any unusual activity or location-based controls on the MMH portal prior to the incident, or that were triggered by the threat actor's malicious activity or authentication events during the incident.

4.5 Health sector system controls and risk management

The nature of the MMH incident highlights supply chain / vendor management issues. Supply chain risk management is a critical component of cyber risk management.

The interlocking HISO and HISF frameworks are and were the main vehicles to provide security and privacy guidance to third-party suppliers that hold personal health information such as MMH. Specifically, HISO 100.29.4:2025 provides HISF guidance and sets the expectation around cyber security for third-party suppliers.

4.6 HNZ cyber risk assurance

HNZ has a cyber risk assurance function for third parties. This is a vendor assessment process rather than a formal regulatory audit against HISF or other standards. HNZ may ask third parties to demonstrate HISF alignment as part of onboarding, contract renewal, or following a security incident.

By design, this is given effect only where contract requires HISF alignment and may not capture contracts where HNZ is not a contracting party.

During the assessment process, it was found that HNZ third-party / vendor assessment capability appears functional, taking a risk-based approach to assurance. This tends to be a 'paper based' process, with documentary evidence provided by the third-party being assured, rather than direct technical control validation.

Additionally, it was noted that the HNZ third-party / vendor assessment process is limited in capacity and may lack deep technical knowledge around software development processes.

An assessment undertaken by **[vendor name removed]** (*Te Whatu Ora, Health New Zealand Cyber Maturity Assessment)* in 2025 states:

> *"Third-Party Risk Management (TPRM) is specifically called out as the domain with the lowest maturity, highlighting the absence of a formalised, enterprise-wide approach to managing external cyber risk"*

Section 2.1 observation 01.15 of that report contains a number of thematic recommendations regarding third-party risk management, and the assessment team **recommends [REC04]** that HNZ should comprehensively review its third-party risk management practices in-line with the with recommendations in the **[vendor name removed]** Cyber Maturity Assessment Report (Sep-25).

As a supplier holding sensitive medical information, more stringent third-party risk management governance of MMH could have reasonably been expected by HNZ (and other contract holders with MMH) prior to the incident.

4.7 Other health sector cyber risk assurance

This assessment did not determine the capability of other health sector entities such as PHO's, individual practices (or clusters of practices), or other entities capability to assess supply chain risk when entering into commercial arrangements with third-parties. HNZ does provide both an "*Evaluating an IT Supplier*" template and an "*Information Security Clauses*" contract pack for smaller health sector entities and undertakes engagement with both smaller health sector entities and suppliers to the sector.

The assessment team **recommends [REC05]** that HNZ develop a plan to engage with the sector to drive better third-party security assurance outcomes across the health sector, in line with HISO and HISF requirements. This plan should consider a broader programme of activities to engage with smaller health sector entities, providing them with practical support for managing third-party cyber risk.

4.8 HISF compliance enforcement of suppliers

The enforcement of HISF requirements or compliance for suppliers is considerably more light touch than the weight of the framework documentation suggests. HISF has no direct legislative mandate and HNZ or any regulatory body cannot directly penalise suppliers for non-compliance.

The primary enforcement mechanism for contract holders is commercial. Non-compliance is considered a contract breach. While a market scan shows HISF compliance is increasingly being embedded into procurement and contracting processes e.g. the PHO Service Agreements, Data

Sharing Agreements, Remote Access Agreements etc. the scale of this coverage is outside the scope of this assessment.

Based on available sources it would appear that contractual penalties for HISF non-compliance are rarely invoked by HNZ or other contract holders in the health sector (though data sources for this assertion are commercial-in-confidence and not readily available). It is **recommended [REC06]** that MoH, in their role as health system monitor, write to HNZ (and other relevant contract holders) to confirm how they manage HISF compliance and what actions have been taken in cases of non-compliance.

The assessment team also **recommends [REC07]** that HNZ consider measures to strengthen HISF compliance among suppliers to the health sector, in particular suppliers that hold sensitive health information. This could be achieved through a number of mechanisms, outside of legislative change, such as:

- Maintaining a public (or available to primary care customers) listing of suppliers that have adequately demonstrated HISF compliance.
- Publish baseline technical controls that are binding for suppliers on top of HISF alignment.
- Ensure that all relevant contracts with relevant third-party suppliers include:
  - specified HISF maturity levels
  - independent third-party assessment (rather than self-assessment) against HISF at a regular cadence
  - right-to-audit clauses including the right to commission independent technical testing (pen tests, secure code review, API security testing) at the supplier's cost where risk warrants
  - mandatory breach notification timeframes tighter than the Privacy Act's "as soon as practicable" — 24 or 48 hours to HNZ specifically
  - sub-processor disclosure and flow-down obligations, so the supplier can't hand data to a fourth-party with weaker controls.

To support this uplift, the assessment team further **recommends [REC08]** that HNZ and other health sector entities maintain registers of their suppliers that store or process sensitive health information, tiered by risk factors (including volume of records, sensitivity, criticality to care delivery).

Additionally, it is **recommended [REC09]** that MoH as the health system monitor defines thresholds and attributes for "high-risk" suppliers to the health sector and regularly receives assurance from entities that hold contracts with those "high-risk" third-party suppliers regarding their security status and HISF compliance.

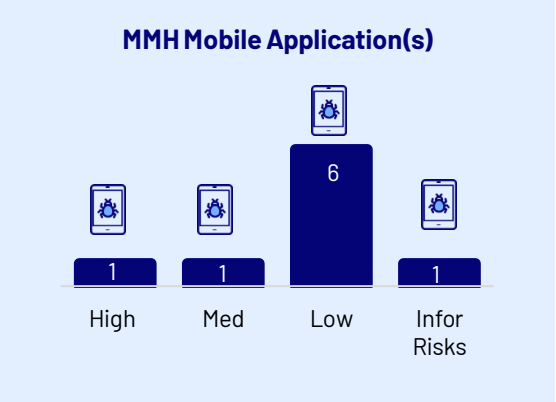
5 Manage My Health Privacy & Security Posture Post-Incident

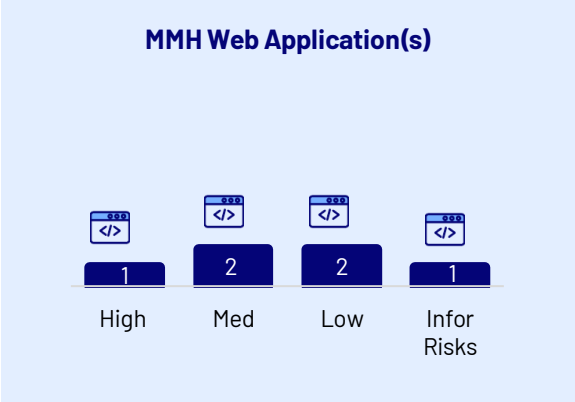
The assessment team found that MMH appears to have improved their security and privacy posture post-breach. However, it should be noted that the assessment team did not undertake technical testing of the efficacy of the enhanced controls, and this portion of the assessment was determined by documentation review and attestation received from MMH.

The suite of enhanced controls has been implemented by MMH, include:

[Details removed]

Additionally, MMH commissioned security reviews (penetration tests) from **[vendor name removed]** in January/February 2026 to confirm that security issues in both the MMH web and mobile applications had been resolved. These tests did not detect API endpoint issues similar to the issues that caused the incident. However, they detect other issues, a summary of which is provided below:





The assessment team sighted a security review (penetration test) re-test report for the MMH mobile application(s) that determined 7 risks had been addressed, with 2 risks outstanding (1 rated 'Medium' and one rated 'Low').

The assessment team did not sight a similar re-test report regarding the MMH web application.

MMH also commissioned other security reviews (penetration tests) from **[vendor name removed]** in February 2026 to test the newly commissioned MMH data breach check platform.

The report of Phase 1 of the review undertaken by **[vendor name removed]** states:

*"**[vendor name removed]** notes some omissions within **[vendor name removed]** reporting that give cause for concern regarding the quality of advice MMH is receiving. One notable example is **[vendor name removed]** not warning Cereus Health Group of the known weakness associated with using the Cipher Block Chain (CBC) encryption in association with use of Transport Layer Security protocols within this new platform."*

The assessment team concurs with this this observation. Furthermore, the assessment team **recommends [REC10]** that further security reviews (penetration tests) or purple/red team activity, independent of **[vendor name removed]**, be undertaken on the MMH web and mobile applications. Testing will provide assurance regarding the current state of the in-scope MMH applications and ensure appropriate alerts are triggered within MMH's security controls from simulated attack activity. This testing should be re-

A **Red Team** simulates real-world adversaries to test an organisation's defences by attempting to breach systems, while a **Purple Team** is a collaborative function where red and blue (defensive) teams work together in real time to share findings and improve detection and response capabilities.

run regularly (every 6-12 months) and after any major system changes.

The assessment team notes that forensic containment report dated 20 January states:

"Upon conclusion of the response MMH will also be conducting an external assessment against the NZ Health Information Security Framework (HISF) in order to assess for compliance".

The assessment team did not sight a copy of this compliance report and could not determine whether this assessment was undertaken. It was stated by MMH that a "*review of internal processes – post-incident assessment*" was marked as implemented in February 2026, though direct evidence of this was not sighted.

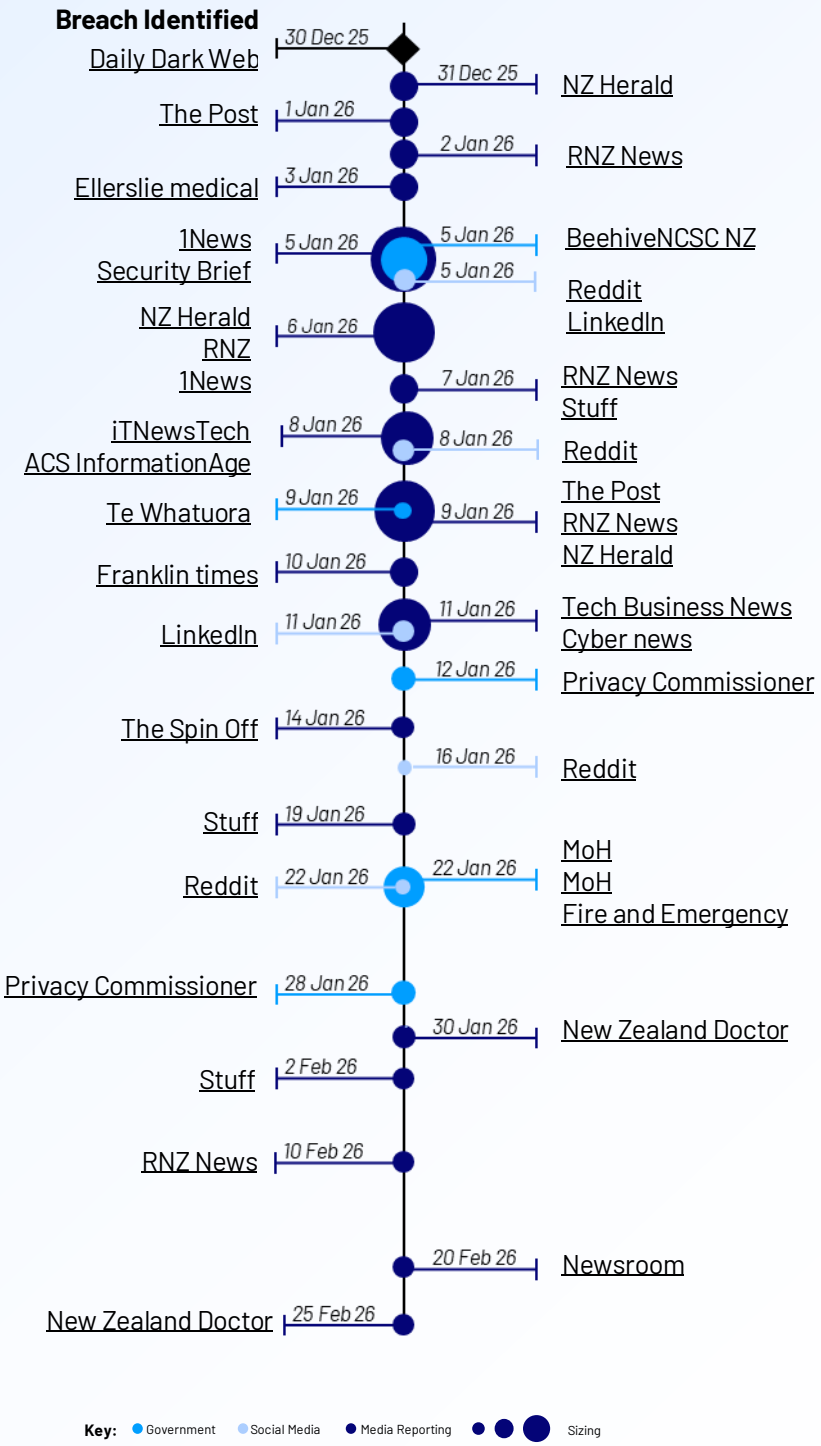
For the purpose of more complete assurance, it is **recommended [REC11]** that MMH undertake a full external assessment of HISF compliance by a provider who is conversant with the HISF framework. The results of this external assessment should be shared with HNZ and other relevant stakeholders, and any areas of non-compliance documented and tracked.

While outside the scope of this assessment, it is **recommended [REC12]** that HNZ seek assurances from MMH of the data management practices, aligned to HISF and best practice, including details of user onboarding and offboarding processes, data retention periods, data access audit methodologies and whether patient data is accessible to any of MMH suppliers or related parties.

6 Appendices

6.1 Appendix 2: High-Level Media Timeline

The following high-level timeline provides a snapshot of media activity relating to the incident. It is noted that MMH published regular updates on their website during this time. Daily updates were issued for the period 1/1/26 to 9/1/26, with subsequent updates published on 12/1/26, 13/1/26, 04/3/26, 15/3/26, and 24/3/26.



6.2 Appendix 3: References/Methodology

Ministerial Updates

Document Title	Date	Created By
03-01-2026 - MMH Minister Briefing - from HNZ	03/01/2026	HNZ
04-01-2026 - MMH Minister Update - from HNZ	04/01/2026	HNZ
05-01-2026 - MMH Minister Update - from HNZ	05/01/2026	HNZ
05-02-2026 - MMH Sitrep + Minister Briefing - from HNZ	05/01/2026	HNZ
06-01-2026 - MMH Sitrep + Minister Update - from HNZ	06/01/2026	HNZ
Minister's Update - 6th January 2026	06/01/2026	HNZ
07-01-2026 - MMH Sitrep + Minister Briefing - from HNZ	07/01/2026	HNZ
Minister's Report and SitRep - 7 January 2026	07/01/2026	HNZ
08-01-2026 - MMH Sitrep + Minister Briefing - from HNZ	08/01/2026	HNZ
Minister's Report and SitRep - 8th January 2026	08/01/2026	HNZ
09-01-2026 - MMH Sitrep + Minister Update - from HNZ	09/01/2026	HNZ
Minister's report - 9th January	09/01/2026	HNZ
10-01-2026 - (1 of 2 on 10 Jan) - MMH Sitrep + Minister Update - from HNZ	10/01/2026	HNZ
10-01-2026 - (2 of 2 on 10 Jan) MMH Sitrep + Minister Briefing - from HNZ	10/01/2026	HNZ
10-02-2026 - MMH Sitrep + Minister Briefing - from HNZ	10/01/2026	HNZ
Minister's report - 10th January	10/01/2026	HNZ
12-01-2026 - MMH Sitrep + Minister Update - from HNZ	12/01/2026	HNZ
12-02-2026 - MMH Sitrep + Minister Briefing - from HNZ	12/01/2026	HNZ
MMH Minister's update - 12 January	12/01/2026	HNZ
13-01-2026 - MMH Sitrep + Minister Update - from HNZ	13/01/2026	HNZ
MMH Minister's update - 13 January	13/01/2026	HNZ
14-01-2026 - MMH Sitrep + Minister Briefing - from HNZ	14/01/2026	HNZ
15-01-2026 - MMH Minister Update - from HNZ	15/01/2026	HNZ
16-01-2026 - MMH Sitrep + Minister Briefing - from HNZ	16/01/2026	HNZ
FW MMH Minister's update - 16 January	16/01/2026	HNZ
17-01-2026 - MMH Sitrep + Minister Briefing - from HNZ	17/01/2026	HNZ
17-02-2026 - MMH Sitrep + Minister Briefing - from HNZ	17/01/2026	HNZ
18-01-2026 - MMH Sitrep + Minister Briefing - from HNZ	18/01/2026	HNZ
19-01-2026 - MMH Sitrep + Minister Briefing - from HNZ	19/01/2026	HNZ
19-02-2026 - MMH Sitrep + Minister Briefing - from HNZ	19/01/2026	HNZ
20-01-2026 - MMH Sitrep + Minister Briefing - from HNZ	20/01/2026	HNZ
21-01-2026 - MMH Sitrep + Minister Briefing - from HNZ	21/01/2026	HNZ
FW MMH Minister's update - 21 January	21/01/2026	HNZ
23-01-2026 - MMH Sitrep + Minister Briefing - from HNZ	23/01/2026	HNZ
26-01-2026 - MMH Sitrep + Minister Briefing - from HNZ	26/01/2026	HNZ

28-01-2026 - MMH Sitrep - from HNZ	28/01/2026	HNZ
28-01-2026 - Updated MMH Minister Briefing - from HNZ	28/01/2026	HNZ
03-02-2026 - MMH Sitrep + Minister Briefing - from HNZ	03/02/2026	HNZ
20260225_Minister update Feb 25	25/02/2026	HNZ
FW_ MMH HNZ final data breach SitRep and Minister's update Mar 04	04/03/2026	HNZ
20260304_Minister update Mar 04	03/04/2026	HNZ

Situation Reports

Document Title	Date	Created By
Manage My Health Data Breach - Situation Report #1	01/01/2026	HNZ
Manage My Health Data Breach - Situation Report #2	02/01/2026	HNZ
Manage My Health Data Breach - Situation Report #3	03/01/2026	HNZ
Manage My Health Data Breach - Situation Report #4	04/01/2026	HNZ
Manage My Health Data Breach - Situation Report #5	05/01/2026	HNZ
Manage My Health Data Breach - Situation Report #6	06/01/2026	HNZ
Manage My Health Data Breach - Situation Report #7	07/01/2026	HNZ
Manage My Health Data Breach - Situation Report #8	08/01/2026	HNZ
Manage My Health Data Breach - Situation Report #9	09/01/2026	HNZ
Manage My Health Data Breach - Situation Report #10	10/01/2026	HNZ
Manage My Health Data Breach - Situation Report #11	11/01/2026	HNZ
Manage My Health Data Breach - Situation Report #12	12/01/2026	HNZ
Manage My Health Data Breach - Situation Report #13	13/01/2026	HNZ
Manage My Health Data Breach - Situation Report #14	14/01/2026	HNZ
Manage My Health Data Breach - Situation Report #15	15/01/2026	HNZ
Manage My Health Data Breach - Situation Report #16	16/01/2026	HNZ
Manage My Health Data Breach - Situation Report #17	17/01/2026	HNZ
Manage My Health Data Breach - Situation Report #18	18/01/2026	HNZ
Situation_Report #19 19 Jan 2026	19/01/2026	HNZ
Situation_Report #20 20 Jan 2026	20/01/2026	HNZ
Situation Report #21 21 Jan 2026	21/01/2026	HNZ
Manage My Health Data Breach - Recovery Situation Report #22	23/01/2026	HNZ
Manage My Health Data Breach - Recovery Situation Report #23	26/01/2026	HNZ
Manage My Health Data Breach - Recovery Situation Report #24	28/01/2026	HNZ
Manage My Health Data Breach - Recovery Situation Report #25	30/01/2026	HNZ
Manage My Health Data Breach - Recovery Situation Report #26	03/02/2026	HNZ
Manage My Health Data Breach - Recovery Situation Report #27	05/02/2026	HNZ
Manage My Health Data Breach - Recovery Situation Report #28	10/02/2026	HNZ
Manage My Health Data Breach - Recovery Situation Report #29	12/02/2026	HNZ
Manage My Health Data Breach - Recovery Situation Report #30	17/02/2026	HNZ
Manage My Health Data Breach - Recovery Situation Report #31	19/02/2026	HNZ
Manage My Health Data Breach - Recovery Situation Report 32	25/02/2026	HNZ

Manage My Health Data Breach - Recovery Situation Report 33	04/03/2026	HNZ

Commercials, Terms of Reference, Written Correspondence

Document Title	Date	Created By
RE UPDATED MMH Notification and self-review	03/02/2026	MMH/HNZ
22-01-2026 - Letter from Sir Brian Roche to Ms Audrey Sonerson - 22 January 2026	22/01/2026	MoH
02-03-2026 Letter from Audrey Sonerson - Phase 2 Review	02/03/2026	MoH
Vulnerability Reports Cover Statement 20260130	30/01/2026	HNZ
260106 ManageMyHealth Enterprise License and Service Agreement_ fully executed	08/12/2022	MMH/HNZ
260106 ManageMyHealth Enterprise License and Service Agreement_ fully executed	08/12/2022	MMH/HNZ
AA Manage My Health Enterprise Procurement Agreement (2)	08/12/2022	MMH/HNZ
AA Manage My Health Enterprise Procurement Agreement	08/12/2022	MMH/HNZ
HNZ SOW - Northland eReferral	Jul-25	MMH
HNZ SOW - Northland Lab Result Repository Integration	Nov-23	MMH
22-01-2026 Terms of Reference - Manage my Health Cybersecurity Incident	22/01/2026	MoH

Pre-Incident Technical and Security Assessments

Document Title	Date	Created By
20180401-10020_Manage_My_Health_Webapp_v1.0	1/04/2019	[vendor name removed]
20180409-10020_MoH_MMH_Critical_Issues_DRAFT_v1.0	9/04/2019	[vendor name removed]
20180415-10020_[vendor name removed] _Application_and_API_v1.0	15/04/2019	[vendor name removed]
20180418-10020_MoH_MMH_Mobile_SecRev_v1.0	18/04/2019	[vendor name removed]
-IN-CONFIDENCE [vendor name removed] Status Update on Primary Care Portals Discovery	29/01/2025	[vendor name removed]
[vendor name removed]Status Update on Primary Care Portals Discovery	29/01/2025	[vendor name removed]
HNZ CPA Maturity Assessment Report - v1.0	Sept-25	[vendor name removed]

Pre-Incident Vulnerability Notification

Document Title	Date	Created By
FW_ Vulnerability Disclosure for Manage My Health	17/11/2025	Consultant
FW_ Vulnerability Disclosure for Manage My Health Nov25	17/11/2025	MoH

Digital Forensics Reports & Threat Intelligence

Document Title	Date	Created By
[vendor name removed]- MMH - Incident Response Statement - 2026-01-02	2/01/2026	[vendor name removed]
2026-01-16 - ManageMyHealth - Containment Statement - Final	16/01/2026	[vendor name removed]
2026-01-16 - ManageMyHealth - Containment Report - Final	20/01/2026	[vendor name removed]
21 January 2026 - Threat Intelligence Report - Kazu	23/01/2026	[vendor name removed]
2026-02-10 - Manage My Health - Digital Forensics and Incident Response - Ransomware - FINAL	10/02/2026	[vendor name removed]

Post-Incident Technical and Security Assessments

Document Title	Date	Created By
MMH_Web_VAPT_Retest_Report_31_Dec_25	31/12/2025	[vendor name removed]
MMH_Web_Production_Security_Assurance_Report_02_Jan_26	2/01/2026	[vendor name removed]
[vendor name removed]- MMH - Penetration Testing (Phase 2) - Redacted	04/01/2026	[vendor name removed]
[vendor name removed]- MMH - Penetration Testing (Phase 1) - Redacted	09/01/2026	[vendor name removed]
[vendor name removed]- MMH - Testing of Vulnerability - 2026-01-13	13/01/2026	[vendor name removed]
30012026 Manage My Health Web Application Penetration Test Report v1.0	30/01/2026	[vendor name removed]
MMH_Document_Display_portal_Web_VAPT_Initial_Report_07_Feb_2026	07/02/2026	[vendor name removed]
MMH DBS Pen test -Retest reportFinal	08/02/2026	[vendor name removed]
11022026 Manage My Health Mobile Application Penetration Test Report v1.0	11/02/2026	[vendor name removed]
RE URGENT Important Vulnerability Assessment and Pen Testing report	13/02/2026	[vendor name removed]
16022026 Manage My Health Mobile Application Penetration Retest Report v1.0	16/02/2026	[vendor name removed]

MMH Cyber Security Review Phase 1

Document Title	Date	Created By
Manage My Health Cyber Security Review - [vendor name removed]- March 2026	06/03/2026	[vendor name removed]

CyberCX Independent Assurance Review Interviews

Organisation	Attendees	Date / Time
HNZ	[name removed], Group Manager Security Incident Management National Security Incident Response, Data & Digital *[Online]* [name removed], Group Manager Security Assurance & Security AI, Cyber Security | Digital Services *[Online]* [name removed], National CISO *[Online]*	25/03/2026 1300 – 1430
NCSC	[name removed], Manager, Incident Management *In person* [name removed], Manager Engagement, Communications and Partnerships *In person* [name removed], Director, Cyber Defence Operations *In person*	26/03/2026 1400 – 1530
MMH	[name removed], CEO *[In person]* [name removed], General Manager, Product & Innovation *[In person]* [name removed], Advisor *[Online]* [name removed], Chief Technology Officer *[Online]* [name removed], Technical and Enterprise Architect *[Online]*	31/03/2026 1300 – 1430
NZ Police	[name removed], Cybercrime Investigator High Tech Crime Group *[Online]* [name removed], Cybercrime Unit, High Tech Crime Group *[Online]*	14/04/2026 1100 - 1130

CyberCX Independent Assurance Review Follow Up Calls and Email Correspondence

Title	Date	Created By
Follow up requests to MMH for missing documentation. Refer '6.3.11 MMH Documentation' for artefacts received.	10/4/2026 17/4/2026	CyberCX/MMH
Follow up with NCSC on potential additional interview attendees	1/4/2026	CyberCX/NCSC
Follow up clarification questions and request for copy of Timeline	10/4/2026	HNZ
HNZ SIMT MMH Timeline 24032026 (to 16-Jan)	10/4/2026	HNZ
Clarification call with MOH on 2019 Security Reports	17/4/2026	CyberCX/MoH
Email CCX/MMH - Clarification questions to MMH	24/4/2026	CyberCX/MMH

MMH Documentation

Document Title	Date	Created By
MMH Privacy Policy	18/09/2023	MMH
MMH Business Terms and Conditions	19/06/2024	MMH
Business Continuity Plan (BCP) Procedure	04/07/2025	MMH
Disaster Recovery Procedure	04/07/2025	MMH
Information Security Incident Management Policy	10/08/2025	MMH
Crisis Management Action Register	Jan-26	MMH
MMH_Staging and Production Environments_12_Jan_26	12/01/2026	MMH
Customer Care Department Procedure	31/03/2026	MMH
MMH_CyberCx_Security_Briefing_Final	31/03/2026	MMH

6.3 Appendix 4: Report Terms of Reference

1. Purpose
This report aims to provide a focused analysis of the December 2025 Manage My Health Cyber Security Incident, and deliver actionable insights based on the agreed scope of work.

2. Scope of the Report
The report will address:

- Incident response and reporting appropriateness
- Adequacy of system controls and risk management at the time of the incident.
- Execution of remediation actions.

The assessment will be conducted via:

- Direct engagement with MMH, HNZ, and relevant stakeholders
- Review/assessment of technical audits, change management activities, and system updates, pre and post the incident
- Review/ assessment of remediation actions and supporting documentation
- Comparison of MMH Review phase 1 outputs with current system controls.
- As is practically possible, provide a view of the pre-incident MMH platform state.

3. Out of Scope
The following items are excluded:

- Broader Regulatory Environment: No assessment of the broader legislative environment within which Manage My Health operate.
- Review or assessment of other providers: The report will not review or benchmark the practices or performance of other healthtech providers.
- Adequacy of Healthcare Information Security Framework (HISF): No assessment of the general sufficiency or applicability of the HISF beyond its direct relevance to the defined scope.
- Other General Topics: Broader industry trends or areas unrelated to the defined scope are excluded.

5. Timeline

- 02 March 2026 - 30 April 2026

New Zealand head office:

CyberCX Pty Ltd
L10, 10 Brandon Street
Wellington
ABN: 94 290 421 64678

Tel: 0800 031 274
Email:info@cybercx.co.nz
Web: cybercx.co.nz

LEGAL NOTICE

This incident report has been prepared based exclusively on documentary information, records, and statements provided by Ministry of Health, ManageMyHealth, Health New Zealand or made available to CyberCX. CyberCX has not independently verified the accuracy, completeness, or reliability of the supplied materials. Accordingly, no representation or warranty is given regarding the correctness of the information contained herein. While reasonable care has been taken to present the details clearly and coherently, CyberCX accepts no liability for any errors, omissions, or discrepancies arising from information supplied by a third-party. This report is provided solely for informational purposes and does not constitute professional advice, a formal finding, or a binding determination of liability. The document may be updated or amended should further verified information become available.

In preparing this report, CyberCX used a proprietary and internal AI tool to assist with a preliminary review of the applicable standards. At all times there was a human reviewing the outputs and the AI did not influence or contribute to any decisions or recommendations contained in the report.