Deloitte.

Together makes progress

Health NZ Manage My Health Cyber Breach Review

Confidential and Legally Privileged

Version 4, May 2026

Contents

Statement of Responsibility

This engagement ("**the review**") was performed in accordance with the terms contained in our Consultancy Services Order with Health New Zealand ("**our client**") signed and dated 3 February 2026. Where Deloitte has provided advice or recommendations to our client, we are not responsible for whether, or the manner in which, suggested improvements, recommendations, or opportunities are implemented. The management of our client, or their nominees, will need to consider carefully the full implications of each of these suggested improvements, recommendations, or opportunities, including any adverse effects and any financing requirements, and make such decisions, as they consider appropriate.

The review was advisory in nature and does not constitute an assurance engagement in accordance with Statement of Review Engagement Standards ("RS1") or International Standard on Assurance (New Zealand) 3000 ("ISAE (NZ) 3000") or any form of audit under the International Standards on Auditing (New Zealand) ("ISA(NZ)s") and consequently no opinions or conclusions intended to convey assurance under these standards are expressed.

The matters detailed in our report are only those which came to our attention during the course of performing our review and did not necessarily constitute a comprehensive statement of all the weaknesses or issues that exist or actions that might be taken. Accordingly, management should not rely on our report to identify all weaknesses and issues that may exist in the systems and procedures discussed. The report should be read in the context of the scope of our work.

This report should not be relied upon as a substitute for actions that our client should take to assure itself that the relevant controls are operating efficiently.

This report is provided solely for our client's exclusive use and solely for the purpose of the review. Our report is not to be used for any other purpose, recited or referred to in any document, copied or made available (in whole or in part) to any other person without our prior written express consent. We accept or assume no duty, responsibility or liability to any other party in connection with the report or this engagement, including without limitation, liability for negligence in relation to the factual findings expressed or implied in this report.

Version Control and Contact

Version	Date	Comment
1	2 April 2026	Draft for first complete internal review
2	10 April 2026	Draft for client review
3	15 May 2026	Final draft report
4	18 May 2025	Final report

Contact for more information

For more information in relation to this report, please contact David Lovatt, Partner, Deloitte by email dlovatt@deloitte.co.nz or telephone +64 21 490 016.

Executive Summary

Introduction

A cyber breach is a distressing and high-pressure event for the people who are responding and the individuals whose information or access to services is impacted by the breach. These events are often characterised by limited or conflicting information, short timeframes to identify attack pathways, secure systems and restore services while also identifying potential impacts, assessing harms, and managing communications with customers and stakeholders. The response becomes even more challenging when multiple parties and systems are involved, and the root cause of the breach may have taken place months or years before the event is recognised.

In a healthcare setting the pressures and consequences are even higher, with sensitive patient health and identity information often involved – a reason why bad actors increasingly target the rich seam of data in the increasing number of digital systems and services that underpin the smooth operation of our health system. Releases of personal data, or denial of access to critical systems and information, can create harm, paralyse services and weaken trust in public institutions and services. Learnings from cyber incidents and responses can make the systems and organisations involved better, stronger and more resilient in the face of this ever-increasing threat.

It is in this context that Deloitte was engaged by Health New Zealand (HNZ) to undertake an independent review following the December 2025 Manage My Health (MMH) cyber incident. The focus of the review is to investigate how HNZ's responsibility to protect patient information has been met in relation to the information transferred to MMH, how this cyber incident and its impact on HNZ was responded to, to identify any shortcomings that should be addressed and any lessons learned that apply more broadly to HNZ.

The full scope of the review is described in Appendix C, including detail of the specific scope areas and review questions.

Purpose (from the Terms of Reference)

The purpose of the review is to enable HNZ's legal team to respond to regulatory investigations and enforcement, and any claims arising out of the MMH cyber incident.

Background (from the Terms of Reference)

Manage My Health Limited, a privately held New Zealand company, offers the digital product ManageMyHealth™ Patient Portal. This portal enables patients to access their personal health information digitally, as shared by their healthcare providers or General Practitioners (GPs). Patients can also email and communicate with their doctors through the ManageMyHealth™ Patient Portal by agreement with both parties.

In 2021, Northland District Health Board (NDHB) and MMH undertook a pilot programme of the ManageMyHealth™ Patient Portal, including inpatient discharge summaries and clinical letters. Since November 2023, this solution has facilitated the distribution of patient documents, helping to streamline discharge processes, patient referrals and laboratory results for consumers in Te Tai Tokerau.

In December 2025 MMH experienced a cyber-attack that led to the extraction of over 400,000 patient documents by the threat actor "Kazu" on or around 23 December 2025. HNZ became aware of the attack and activated a response on 30 December 2025.

Approach to the review

We completed the following key tasks over the eight-week period of our review:

- Conducted interviews with key stakeholders to understand their involvement and gather insights on actions performed leading up to and during the incident response and recovery.
- Sourced relevant documentation to validate facts, findings and dates, including those relating to the establishment of MMH services to HNZ, advice provided and decisions made over the period under review.
- Produced an interim output with a timeline of events and supporting facts in relation to the six scope areas (a-f) in the terms of reference.
- Generated a set of key findings and reviewed those with Deloitte subject-matter experts to identify important learnings and improvement opportunities, that provide the foundation for our recommendations.
- Provided a draft report to HNZ and received additional documents that helped to build a more complete understanding of the timeline, actions, decisions and events that relate to the review scope.

Structure of this report

This report consists of this executive summary followed by three key sections and supporting appendices:

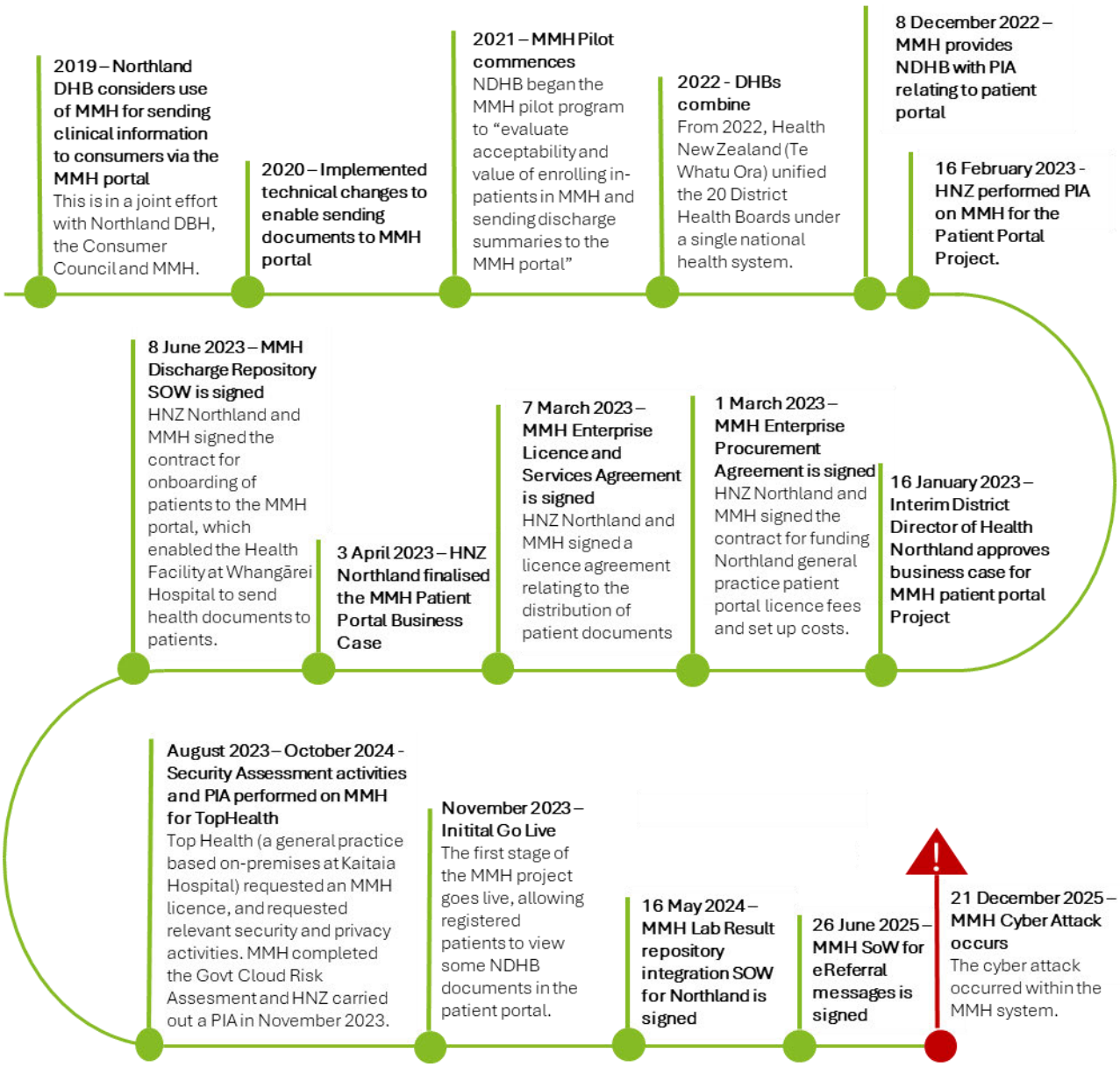
- Background and context for the events that took place from 2019 to 2026 relating to the establishment of NDHB's MMH pilot and HNZ Northland's further use of MMH, through to the cyber breach and incident response and recovery.
- Key insights and findings established from the analysis of interviews, documents, and relevant leading practices and Deloitte subject-matter expertise. Improvement opportunities are noted in this section under each scope area.
- Recommendations for action in response to the insights and findings.

Our review focused on the period to March 2026. Many actions are now underway to address matters mentioned in our review, and we've noted those where we are aware of them.

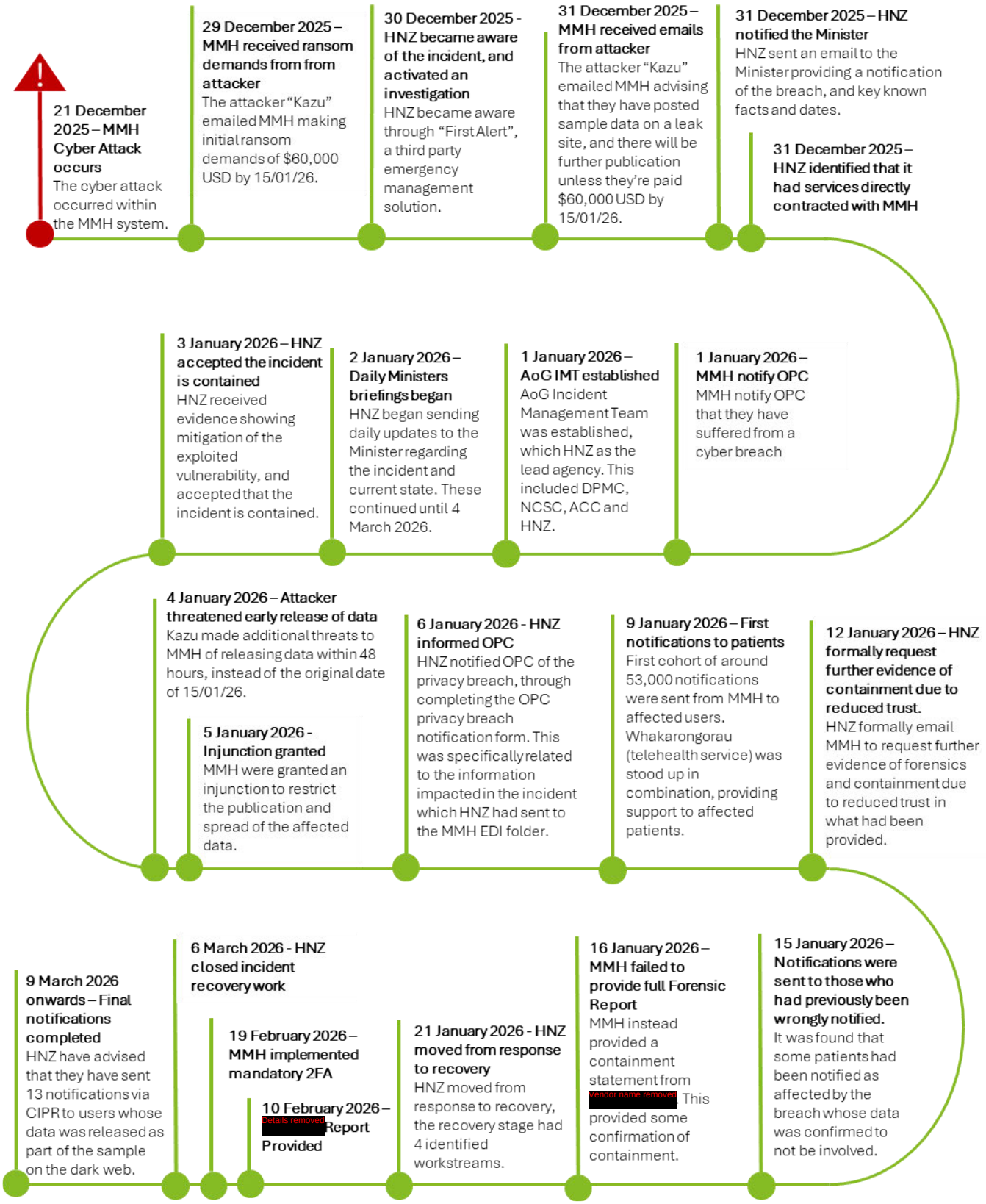
Acknowledgements

We would like to thank all the contributors and interviewees that supported this review, and acknowledge their willingness to share information, context and perspectives that will help protect our health data and systems, and strengthen responses to future cyber breaches. We also acknowledge the considerable effort expended over long days by many people in HNZ, MMH, their advisors and service providers in the response and recovery period, at the cost to many of their usual summer break.

Timeline – Pre-Incident (2019 – 2025)



Timeline – Post-Incident (December 2025 – March 2026)



Key findings from the review

Background and context

HNZ's direct relationship with MMH and use of its services began in 2019 with a pilot programme in Northland DHB to share discharge summaries with patients via the ManageMyHealth™ Patient Portal, and continues now. The services provided by MMH have expanded over this time to also include e-referrals and laboratory test results, enabling HNZ to share health information digitally with patients in Northland, saving time and cost while improving the patient experience. A contract termination for some MMH services was considered in late 2024 (effective December 2025) but was not actioned.

The incident

The incident occurred through the breached credentials of a standard user account being used to gain access into MMH, and then configuration issues of a core application programming interface (API) being identified and utilised to iterate through and extract patient documentation. We understand the documents impacted by the breach included discharge summaries, clinic letters and operation reports stored by MMH in the Patient Portal. This incident impacted 99,416 individuals, with 90,850 of those specifically including data from HNZ. No HNZ systems or other processes are known to be impacted by the breach.

Health New Zealand's role

HNZ was heavily involved in the response from the outset, even including proactively contacting MMH about it having occurred and providing support before realising HNZ had data included within the impacted system. HNZ also led the All of Government (AoG) Incident Management team. HNZ have received advice on the containment and root cause mitigations through various security assessments and containment reports provided to MMH by its vendors. Additionally, further changes and testing were performed by MMH to address retention of a greater range and volume of HNZ data than was understood by HNZ to be held by MMH.

Resourcing the response

Both HNZ and MMH invested considerable resources into the incident response and recovery. Considering the time of year and the challenges involved in coordinating a response in a high-profile incident with elevated media interest and imperfect information, all parties involved mobilised significant resources that responded commendably and with commitment. However, the intensity, time commitment and duration, along with other incident responses occurring before and after the MMH breach, had wellbeing impacts on those involved in the response and recovery.

Restoring confidence

HNZ and MMH have plans to perform a Health Information Security Framework (HISF) assessment on MMH's systems. An assessment has been agreed and we understand this is now underway. It would also be appropriate at the same time to ensure that HNZ data held within MMH's systems is only what is necessary to be retained for the agreed purpose.

Securing the data

Cyber security and privacy requirements were not defined in detail within MMH-HNZ contracts and were not clearly defined by the initial project. Assessments of security and data privacy protection were performed by HNZ and MMH, but this was not reflected in new contractual provisions or retrospective testing of what had been put in place for the Patient Portal project.

A much bigger issue that demands a system response

Security across the digital health landscape is inconsistent and insufficient. HNZ has a large number of service providers and data sharing arrangements utilising a range of technology solutions provided by third parties, each of which is expected to meet the requirements of the Privacy Act, the Health Information Privacy Code, and specific provisions written into individual agreements at each layer of the health and software supply chain, Information security can be compromised at any point in this complicated web of relationships, and with the waning public trust of health technology following three significant breaches in 2026 so far, this demands a sector-wide response if we want to confidently keep New Zealanders' health data safe.

Primary recommendation

It is this last finding that we want to address first in our recommendations. MMH is just one of over 5,000 applications in use by HNZ and its providers, many of which are delivered under contract from digital health businesses across New Zealand and overseas. The combination of a highly fragmented provider and technology landscape, rapidly increasing cyber threats targeting valuable identity and health information, inconsistent security practices including a lack of routine testing and verification, and very limited resources spread thinly across the public sector and digital health businesses, leads to a high likelihood of continued cyber incidents and privacy breaches that ultimately compromise some of the most vulnerable individuals in our society.

If in New Zealand we believe that health information is as important to secure as (for example) financial information or digital identity information, then it seems appropriate to be taking similar steps towards ensuring consistent application of cyber security and privacy practices across the sector. And just like in those sectors, it is not enough to expect individual organisations to contract for standards and then self-assure compliance – this is inefficient and prone to gaps that leave information exposed. The expectations of the Privacy Act and Health Information Privacy Code are clear; it is the implementation of these that is inconsistent and lacking transparency, independent verification, and public confidence. This is the basis for our primary recommendation:

1. **HNZ to work with the Ministry of Health to put in place independent assurance that the mandated standards for New Zealanders' health information security and privacy are being routinely met, through consistent sector-wide attestation, verification and review arrangements, with enforceable actions to remediate risks and issues.**

Actions are already underway in relation to government services and critical infrastructure (including hospitals) through the NCSC Minimum Cyber Security Standards and Government's Cyber Security Action Plan. This recommendation focuses on a systemic response in health to assure compliance with existing expectations and deal with the legacy problem of thousands of systems in daily use. Regular testing, attestation and independent assurance should be modelled on similar arrangements for financial services and digital identity services in New Zealand, and arrangements for health information used in other jurisdictions. Operationalise this with resourcing and mandate to be discussed with the Ministry, and verification to be provided by qualified third parties funded by digital solution providers.

Supporting recommendations

The supporting recommendations 2 - 8 are targeted at actions HNZ can take or initiate, with support from other agencies, to better enable a robust and proactive approach to health information management and responses to incidents when they inevitably occur:

2. **HNZ to ensure it consistently applies cyber security and privacy, procurement, contracting, and third-party risk management policies and standards in all situations, and takes a proactive approach to assuring and documenting compliance with these requirements.**

Consistently implement HNZ policies and GCDO standards (of August 2025) around cyber security and privacy risk assessments when contracting for new (or renewed or extended) services. Ensure third-party contractual obligations are put in place prior to services being provided. Regularly review that these expectations are being consistently applied, and that suppliers' compliance with expectations is being evidenced and assured. For custom developments, verify that as-built is consistent with pre-approvals based on design artefacts.

3. **HNZ to keep a detailed register of health information held or accessed by third parties, and the associated contracts and data retention for those services.**

Continue the implementation of the Digital Services Hub as a preferred model for secured access to health information (rather than copying information to other systems) as this is fundamentally a sound approach. Maintain contact information for all providers along with this register to facilitate rapid and coordinated responses where breaches occur. Migrate the existing data sharing register to a robust system and expand it to track all access to health information by third parties.

4. **HNZ to address remaining outstanding security and privacy items internally, and with MMH related to this incident.**

Building on the assurance work already completed, plan and set dates for corrective actions around removal of non-compliant data once MMH has satisfied obligations to provide the data as part of patient notifications and responding to the OPC inquiries. Perform HISF assessment on MMH, uplift MMH contract to address known gaps, and perform further validation that data deletion and matching processes are effectively implemented.

5. **HNZ to perform risk assessment across its digital portfolio as part of a systemic approach to focus remediation efforts on higher-risk data, digital systems and services, and where these are identified seek to uplift capability, close gaps, address risks and verify compliance.**

This should particularly look to uplift historic contract and documentation gaps, require vendors to provide evidence they do not have security issues, and to confirm that data provided by HNZ is only being used as intended and retained for the appropriate amount of time.

6. **HNZ to work with the Ministry and sector partners to enable policies such as patient or whānau notifications and consent related to storage, accessing and processing of health information to be standardised across the sector.**

This will allow providers of health information systems (including portals) to have a single approach that works consistently whether the information has been provided by or is being used by public health (HNZ or ACC) or private health (PHOs, GPs, laboratories, radiology providers, etc) organisations.

7. **HNZ to continue investment in growing its cyber incident response capabilities based on improvements identified throughout this review and the broader incident response.**

Mandate that harms analysis are formally documented as part of all HNZ incident response activities once there is potential for privacy to be impacted. Require documentation of critical decisions related to incident scoping and potential harm, and – if this cannot occur – documenting the relevant rationale.

8. **HNZ to continue working with other agencies to strengthen guidance, capabilities and capacity to manage, resource and sustain All of Government level responses.**

This will help ensure the lead agency and its staff have access to broader sector capabilities and are not unduly impacted by long-running response timelines which can directly affect responder wellbeing.

Further details on the recommendations and supporting actions are covered in the main body of our report.

Report

Background and Context

The following timeline outlines the progression of the relationship between HNZ and MMH. It examines how MMH's role evolved as a software vendor delivering a patient-facing online portal that provides access to digital health information originating from HNZ. It also describes the nature of HNZ's engagement with MMH, along with the major phases of activity leading up to, during, and after the cyber security incident and privacy breach.

HNZ Relationship with MMH (Pre-2022)

MMH is a privately owned company that was originally operated alongside Medtech. Before **2020**, Medtech provided the core general practice (GP) clinical systems while MMH functioned as its tightly integrated patient portal, together forming a single end-to-end platform spanning clinical records and patient access. Both digital solutions were embedded partners to primary care organisations, shaping how practices interacted with patients and shared information, while remaining commercially separate from the DHBs and the Ministry of Health **[Medtech Global media release, 3 June 2020]**.

With an objective of improving patient engagement and experience, in **2019** NDHB collaborated with MMH and Vendor name removed to explore a feasible way of sharing patients' health information via a consumer portal, specifically clinical documents such as discharge summary notes from the hospitals to patients directly. The concept of utilising an existing patient portal product with a Patient Management Solution (PMS) was initiated by the NDHB IT team in conjunction with the Northland Health Consumer Council and selected the ManageMyHealth™ Patient Portal due to it being the most widely used patient portal in Northland. NDHB's Health Pathways initiative, MMH and Vendor name removed initially started investigating the possibility of sending NDHB clinical documents to the consumers using the ManageMyHealth™ Patient Portal in absence of a formal contractual agreement **[ISGG Decision Paper, July 2021]**.

Through **2020** the necessary technological changes were implemented to enable the transfer of clinical documents to the ManageMyHealth™ Patient Portal **[ISGG Decision Paper, July 2021]**.

In **June 2020**, Medtech Global was sold to private equity while MMH was retained under ownership of the original NZ founder, resulting in the separation of the

PMS from the ManageMyHealth™ Patient Portal **[Medtech Global media release, 3 June 2020]**.

A formal pilot project commenced in **2021** to evaluate the acceptability and value of enrolling in-patients with MMH and sending their discharge summaries to the ManageMyHealth™ Patient Portal. Data was collected over a four-month period from patients in various medical wards, with a focus on utilisation and engagements via metrics such as ethnicity, gender and age group. The results of the pilot as of **September 2021** indicated positive adoption rates of the new solution **[MMH pilot review.docx, 2021]**.

In **November 2021**, the NDHB presented to the Health System Design Council (HSDC) on providing consumer access to clinical information through the ManageMyHealth™ Patient Portal. The HSDC endorsed the ongoing direction of the project **[Minutes HSDC Manage My Health, November 2021]**.

HNZ Relationship with MMH (2022-2025)

Following the amalgamation of 20 District Health Boards into Te Whatu Ora – Health New Zealand (HNZ) in **June 2022**, HNZ Northland continued driving the ManageMyHealth™ Patient Portal project in collaboration with MMH.

In **December 2022**, HNZ received draft contracts from MMH, along with a Privacy Impact Assessment report (PIA). The PIA was an internal review to meet the requirements of the Privacy Act 2020 and Health Information Privacy Code 2020 **[PIA Report (MMH) – Consumer Portal (221205), December 2022]**.

Following the receipt of the PIA from MMH, HNZ completed a Business Case for the MMH patient portal in **December 2022 [Business Case (Patient Portal) v1.0 Issued.docx, 03 April 2023]**. This was then delivered for endorsement through a decision paper to the Interim District Director (IDD), gaining sign-off from the IDD of HNZ Northland on **16 January 2023 [Decision paper to Interim District Director re patient portal.pdf, 15 December 2022]**.

HNZ Northland then completed an internal PIA for the ManageMyHealth™ Patient Portal on **1 February 2023** that indicated MMH complied with all the Information Privacy Principles (IPPs) **[Privacy Impact Assessment (Te Tai Tokerau Consumer Health Portal) v1.0 Issue (Signed).docx, February 2023]**.

The first two contracts were subsequently signed between HNZ Northland and MMH in **March 2023**. These contracts incorporate MMH's Privacy Policy, Business T&Cs, Terms of Use, Code of Conduct and Security Policies.

1. Manage My Health Enterprise Procurement Agreement **[AA Manage My Health Enterprise Procrurement Agreement.pdf, March 2023]**, signed **1 March 2023**, between HNZ Northland and MMH that funds general practice patient portal license fees and set up costs (new practices). Covers general contracting areas like background, obligations, and termination.

2. MMH Enterprise Licence and Services Agreement **[260106 ManageMyHealth Enterprise Licence and Service Agreement_ fully executed.pdf, March 2023],** Signed **7 March 2023,** services include Discharge Summary & Repository for:
    a. 190,000 patients (Northland HNZ for specific Health Facility/hospital in Whangarei)
    b. 300,000 emails

c. 5TB data.

The Te Tai Tokerau Consumer Health Portal Steering Group is also formed at this time, with their first meeting taking place on **6 March 2023 [Te Tai Tokerau Consumer Health Portal Steering Group Meeting Minutes, 6 March 2023]**.

ManageMyHealth Discharge Portal and Repository Onboarding SOW was also executed on **8 June 2023**. This is between HNZ Northland and MMH to assist with onboarding patients on to ManageMyHealth™ Patient Portal through email communications **[HNZ SOW - Northland Discharge Portal Repository Onboarding.pdf, June 2023]**.

To support the implementation of the ManageMyHealth™ Patient Portal at Top Health, a general practice located within Kaitaia Hospital and operating on HNZ's network, several security assessments specific to the Patient Portal were undertaken between **December 2023** and **24 January 2024** by healthAlliance Northern Region for HNZ: **[RE: MMH – Top Health, 24 January 2024]**

- Vulnerability Assessment and Penetration Test **[MMH_VAPT_Retest_Report_09Feb2022 - Non-prod.pdf, 9 February 2022]**
    - This is a Vulnerability Assessment and Penetration Test (VAPT), retest report performed by Vendor name removed on MMH's non-production environment.
    - Details removed
- Initial Solution Request Information **[ISRS Information - Top Health to use Manage My Health.pdf, 31 August 2023]**
    - This Initial Solution Request Information (ISRS) was requested as HNZ needed the ISRS and related assessment to enable a configuration change for Top Health to access the ManageMyHealth™ Patient Portal.
- Technical Risk Assessment - **[TRA Manage My Health.xlsx, 16 September 2024]**
    - The Technical Risk Assessment (TRA) outlines key security controls and risks related to the ManageMyHealth™ platform.
    Details removed
- Privacy Impact Assessment - **[Privacy Impact Assessment Top Health, November 2023]**
    - This was a Privacy Impact Assessment (PIA) performed by HNZ on the planned Top Health implementation of the MMH Patient Portal.

- System Risk Summary - **[SRS Report_ Top Health to use Manage My Health (ISRS 678) v1.0.pdf, 23 October 2024]**
    - Details removed
- Cloud Risk Assessment Tool - **[Copy of Northern Region full CRAT v1.1.1 - ManageMy Health.xlsx, 1 November 2023]**
    - The Cloud Risk Assessment Tool (CRAT) was provided to MMH to answer various questions for HNZ Northern Region. This includes high-level questions about the data storage location, privacy information, incident response, data retention and backups and more.
    - This CRAT was referenced in the above Privacy Impact Assessment for Top Health.

Two more contracts were executed in **2024** and **2025** that extended functionality for the patient portal:

1. MMH Lab Result repository integration SOW, and MMH Reporting Dashboard and Search SOW, with email confirmation provided as sign off in May 2024. These contracts between HNZ Northland and MMH extended functionality of ManageMyHealth™ Patient Portal to include lab results for patients **[HNZ SOW - Northland Lab Result Repository Integration.pdf, May 2024].**

2. MMH Northland eReferral - Development SOW – executed 26 June 2025 is between HNZ Northland and MMH for the development work of the eReferral functionality **[HNZ SOW - Northland eReferral.pdf, 1 July 2025]**.

In **December 2024**, HNZ considered terminating the Patient Portal agreement with MMH effective December 2025, on the basis of cost and regional consistency. In all other districts, patient portals are paid for by general practice rather than directly by HNZ. Funding for the Enterprise License and Service (Discharge Summary and Repository) Agreement was to transfer to another budget in HNZ and that agreement would continue. This termination did not proceed. **[Termination of Manage My Health Patient Practice Portal Agreement, 11 December 2024]**

Incident (December 2025)

In December 2025, Manage My Health experienced a cyber security breach involving unauthorised access to, and copying of, patient information held on its systems. The breach involved extraction of data from the ManageMyHealth™ Patient Portal, and posed a risk of further access or disclosure of that information beyond authorised users.

On **21 December 2025 [HNZ Transition to Recovery Plan_ MMH incident_Jan26.pdf, 21 January 2026]**, a threat actor compromised a legitimate ManageMyHealth™ Patient Portal account. This threat actor identified and exploited a vulnerability within an application programming interface (API) to obtain clinical documentation **[2026-01-16 - ManageMyHealth- Containment Statement – Final.pdf, 16 January 2026]**. The breach was confined to user-

uploaded files and HNZ Northland hospital clinical letters that were sent to MMH **[DM7_1_Numbers of people and data impacted.pdf, 2026]**.

On **29 December 2025**, Kazu Ransomware Group claimed responsibility for a data breach within the ManageMyHealth™ Patient Portal and released sample data on a dark web leak site. They made ransom demands to MMH **[SIMT MMH Timeline 29 Dec to 13 Jan – 24032026.pdf, 24 March 2026].**

On **31 December 2025** MMH received emails to its general inbox, claiming to be from the attackers. This advised the sample data had been published on a data leak website, and there would be further publication to "various hacker forums" unless a confidentiality fee of $60,000 USD ([Details removed]) was paid. **[2026-NZHC-2Injunction.pdf, 5 January 2026]**

On **1 January 2026**, MMH identified the data leak website, and identified the ransom demand was set to expire on **15 January 2026 [2026-NZHC-2Injunction.pdf, 5 January 2026]**. On the same date, it notified the OPC of the data breach.

The number of individuals whose HNZ information was impacted by the MMH cyber security breach was a total of 90,850, with 16,351 of those under 16 years of age, and 2,686 of those between 16 and 18 years of age **[FW_ Information for Response to Privacy Commissioner - Information Urgently Required Today.msg, 13 March 2026]**. There were a further 8,566 individuals whose patient-uploaded information was also impacted in the breach. This meant that a total of **99,416** individuals were impacted in the breach **[DM7_1_Numbers of people and data impacted.pdf, 2026]**.

Incident Response (December 2025-January 2026)

On **30 December 2025**, HNZ identified the presence of a potential cyber security breach at MMH. This was identified by the National Health Emergency Management Team (NHEMT) through the alerting platform First Alert and was escalated to the HNZ Incident Controller. The HNZ Incident Controller then raised the potential breach to the Cyber Security Incident Response Team (CSIRT) and activated an investigation **[SIMT MMH Timeline 29 Dec to 13 Jan – 24032026.pdf, 24 March 2026]**.

An initial email was also sent by HNZ to an MMH representative enquiring about the breach, and any potential risk or exposure that could impact HNZ **[FW ManageMyHealth Breach.msg, 30 December 2025]**.

As HNZ maintained full coverage over the New Year's break, CSIRT and National Security Operations Centre (NSOC) teams were able to act rapidly, identifying that there no impacts on HNZ systems or clinical care delivery, which was delivered in an email to key stakeholders at 6:30 pm **[SIMT MMH Timeline 29 Dec to 13 Jan – 24032026.pdf, 24 March 2026]**.

On the morning of **31 December** Cyber IMT met with the MMH CEO, they provided suggestions for actions that MMH should action and identified next steps for engagement between the HNZ and MMH **[No Surprises Heads Up Manage My Health Cyber Incident.msg, 31 December 2025] [SIMT MMH Timeline 29 Dec to 13 Jan – 24032026.pdf, 24 March 2026]**.

At 6:00 pm **31 December 2025**, HNZ legal team provided the 'no surprises' briefing in full to DPMC, to be distributed to Minister's Office, Prime Minister's

Office, Minister for GCSB and Minister for ACC **[20251231 FW_ No Surprises_ Manage My Health Breach.msg, 31 December 2025].**

On **1 January 2026,** an All of Government Stakeholder Incident Management Team (AoG IMT) was then engaged, with HNZ as the lead agency. This team was designated to coordinate intel, communications and breach response activities, with a daily cadence of meetings established **[RE ManageMyHealth Cyber Breach - Urgent Briefing.msg, 1 January 2026]**

On **1 January 2026**, HNZ connected with various key stakeholder groups, with engagements including but not limited to: **[20251231 FW_ No Surprises_ Manage My Health Breach.msg, 31 December 2025] [SIMT MMH Timeline 29 Dec to 13 Jan – 24032026.pdf, 24 March 2026]**.

- Initial AoG IMT meeting held
- Assurance discussion with MMH
- Initial engagement with GPNZ
- Briefed Northland GDO
- Second AoG meeting with greater representation from Government agencies
- Initial meeting with Health Minister
- Technical briefing with MMH and [redacted]
- Initial briefing meeting to PHOs
- Briefed the National GDO group

On **2 January 2026**, MMH formally progressed breach confirmation and disclosure activities following the cyber incident. Internal and external communications were approved and issued, historical vulnerability information was provided to HNZ and privacy teams, and forensic investigations continued **[SIMT MMH Timeline 29 Dec to 13 Jan – 24032026.pdf, 24 March 2026]**.

MMH also provided HNZ with interim containment information from [redacted], confirming the initial attack vector, advising that the vulnerability had been contained and further mitigative controls had been deployed **[[redacted] - MMH - Incident Response Statement - 2026-01-02.pdf, 2 January 2026].**

HNZ stated on **2 January** that there was no evidence that My Health Account had been compromised, which had been an initial concern **[20260102 RE Minister's update.msg, 2 January 2026]**

On **3 January 2026**, the HNZ Acting Controller accepted that the incident is contained, and HNZ engaged [redacted] to provide independent validation of the MMH forensic investigation **[SIMT MMH Timeline 29 Dec to 13 Jan – 24032026.pdf, 24 March 2026]**. A subsequent note in the same document records the GM Assurance states further information would be required to confirm containment.

On **3 January** HNZ IMT discovered one direct contractual relationship between HNZ Northland and MMH. Before this date the IMT was unaware of the specific direct contract between them **[20260103 Minister's update MMH - 3 January 2026.msg, 3 January 2026]**.

4 January 2026, HNZ notifies MMH that Kazu Ransomware Group has publicly reduced the timeframe allowed before the data is released to approximately **5:30am, Tuesday 6 January 2026 [Intel Report - Kazu Release Deadline 04012026.pdf, 4 January 2026].**

On **5 January 2026**, MMH are granted an injunction regarding the possession and publication of the data stolen from the ManageMyHealth™ Patient Portal **[2026-NZHC-2Injunction.pdf, 5 January 2026]**.

On **6 January 2026**, HNZ and MMH advanced notification planning for affected individuals and organisations, including cohort definitions and contact-centre support arrangements. Public communications were coordinated, including media statements and guidance to the primary health network **[MMH Breach – Support pathways 08012026.pdf, 6 January 2026].**

As part of this notification planning HNZ developed a risk matrix considering the risks related to the notification process for the MMH incident. This included a consideration of the risks related to the proposed early notification process and had some analysis of social risk. **[MMH Scenario Risk Matrix.pdf, January 2026]**

7 January 2026, HNZ requested additional engagement from MMH regarding clarifications to the communications plan they had provided, which was not as comprehensive as was required **[SIMT MMH Timeline 29 Dec to 13 Jan – 24032026.pdf, 24 March 2026]**.

After an initial test batch of notifications on **8 January 2026**, the first cohort of 53,000 notifications is sent by MMH on **9 January 2026** with the Whakarongorau helpline stood up to support in conjunction **[20260109 Minister's report - 9th January.msg, 9 January 2026]**.

11 January 2026, [redacted] deliver their initial feedback, noting that the security assurance is insufficient with actions to gain the required information being initiated **[SIMT MMH Timeline 29 Dec to 13 Jan – 24032026.pdf, 24 March 2026]**.

MMH delay sending further notifications due to a technical issue reducing confidence in the accuracy of delivered notifications **[20260111 Re_ Minister's report - 11th January.msg, 11 January 2026]**.

12 January 2026, HNZ receive update from MMH that some individuals were notified incorrectly. HNZ provide support to review the data and potential implications **[20260112 MMH Minister's update - 12 January.msg, 12 January 2026]**.

HNZ's Acting Chief Information Technology Officer (CITO) formally emailed MMH, requesting further evidence of forensics and containment [redacted]. A deadline of 13 January 2026, "12 noon" was also applied due to ongoing delays in assurance activities **[FW Request for immediate delivery of security evidence and assurance Manage My Health.msg, 12 January 2026]**.

14 January 2026, Whakarongorau received reports of technical difficulties from patients, specifically around the MMH website and notification letters. HNZ prompted MMH for a response regarding the technical difficulties but there is no evidence to suggest they received one. **[20260114 MMH Minister's update - 14 January.msg, 14 January 2026]**.

14 January 2026 HNZ provided MMH with an introduction to [redacted], a specialist legal and advisory firm to assist with their approach to remaining notifications

[FW MMH Notification Support - Introduction with [redacted].msg, 14 January 2026].

On **15 January 2026** notifications were completed for the 13,900 individuals wrongly notified, advising them they were not impacted **[20260121 FW_ MMH Minister's update - 21 January.msg, 21 January 2026].**

15 January 2026 HNZ requested clarification about account registration questions from MMH. **Answers were provided back on 16 January 2026.** These confirm that there were six patient record and account types linked to the patient entity in Manage My Health, which showed: **[SG NDHB_Queries_15Jan2026.docx, 16 January 2026] [DM6_1_MMH User Record Account Types.pdf, 22 March 2026]**

- Five types of patient records were classified as registered but not activated (SEHR Registered, Easy Booking Registered, GP Registered, Hospital Registered, Self Registered), but these do not have an activated MMH portal account and therefore the individuals relevant to them do not have visibility of documents that may be attached to them.
- Subsequent clarification issued by MMH further detailed that "portal accounts" referred to clinic-registered (by a GP or hospital) or self-registered but non-activated accounts; and to activated accounts.
- The HNZ data held by MMH was being matched against records which patients cannot access, which were Easy Bookings and the Shared Electronic Health Record (SEHR), but these did not initiate a portal account.

16 January 2026, HNZ received a containment statement from [redacted] which indicated the Threat Actor had successfully authenticated to the MMH Patient Portal on 21 December 2025 and interacted with an API to access information stored within the Patient Portal. **[MMH Containment Report – Final, 16 January 2026].** MMH state they expected to provide the [redacted] report by the 16th, however this was not provided [**MMH Data Breach – SitRep #14, 14 January 2026].**

18 January 2026, HNZ re-engaged [redacted] to provide assurance on MMH's systems, including providing confidence that their environment is secure **[20260118 MMH Minister's update - 18 January.msg, 18 January 2026]**.

20 January 2026, [redacted] shared a containment report with HNZ, describing the containment of the incident with more detail regarding improvements made since the incident **[2026-01-20 - ManageMyHealth - Containment Report – Final.pdf, 20 January 2026]**.

On **20 January 2026** MMH finalised the Functional Design Specifications (FDS) HNZ Northland Documents – Receipt, Processing and Visibility document. This outlined use cases that HNZ has approved, which differ from the previously implemented MMH solution by specifying that documents should only be stored in MMH against an activated account that is not in "suspended" state, and that non-complying documents previously ingested should be deleted. **[FDS- HNZ Northland Documents - Receipt, Processing & Visibilityv1.0 16-Jan-26.docx, 20 January 2026]**

Incident Recovery (January 2026-March 2026)

From **21 January 2026**, the focus shifted from incident response to recovery, with HNZ prioritising the stabilisation of critical functions while reducing residual risk arising from the incident. The initial target timeline for the recovery period was eight weeks, from 21 January to 17 March **[HNZ Transition to Recovery Plan, 21 January 2026]**. The incident recovery had four workstreams **[ELT Briefing_MMH incident and primary care information sharing.docx, 12 February 2026]**:

- Notifications: "Supporting MMH to complete the notifications process"
- Northland Solution: "design and implementation of a sustainable solution for information sharing in Health NZ Northland"
- Privacy Issues arising in Primary Care: "working with primary care to understand wider privacy issues arising from the initial breach"
- Review Support Workstream: "Facilitating information requests for the various reviews, working with MOH, OPC and Health NZ"

On **26 January 2026**, HNZ were completing the planning of remaining notifications in collaboration with MMH. There was also work underway for a long-term technical solution for the data flow between HNZ Northland and the ManageMyHealth™ Patient Portal. Penetration testing of the APIs and app was also completed by Vendor name removed **[20260126_Minister update Jan 26.pdf, 26 January 2026]**.

On **5 February 2026**, the HNZ Recovery function entered Sprint 2, shifting from maintenance of the IMT functions to long-term planning of identified workstreams via BAU processes **[20260205_Minister update Feb 05.pdf, 5 Feb 2026]**.

On **10 February 2026** the Details removed report was released by Vendor name remo to HNZ **[MMH Data Breach – Recovery SitRep #28, 10 February 2026]**

On **19 February 2026**, HNZ received all outstanding documentation from MMH in relation to forensic reporting and penetration testing. HNZ then shared the documents with Vendor nam to complete their assurance reporting **[20260219_Minister update Feb 19.pdf, 19 February 2026]**.

On **6 March 2026**, HNZ formally closed the IMT recovery structure, with the final Ministers Update being distributed on **4 March 2026 [20260304_Minister update Mar 04.pdf, 4 March 2026].**

Final mention of planned notification was for **9 March 2026**, which were for Details individuals who had their data exposed on the dark web. MMH did not have reliable contact details for these, and therefore HNZ planned to perform notification to these individuals via its CPIR system **[MMH Recovery Timeline.docx, March 2026].** We have been advised that these notifications proceeded as planned.

Key Findings

Within the Terms of Reference for this review there are six scope areas (a-f) to be addressed through this report. The findings, supporting commentary and recommended actions (scope area g) for each of these areas are outlined below.

A. Background

What is the nature / history of Health NZ's relationship with MMH? What service does MMH provide to HNZ that is relevant to this cyber breach? What security and privacy obligations and supporting processes are in place for that service in Health NZ and MMH? Any other context that is relevant to the Investigation Report?

HNZ's direct relationship with MMH and use of its services began in 2019 with a pilot programme in Northland DHB to share discharge summaries with patients via the ManageMyHealth™ Patient Portal, and continues now.

The history of the working relationship between HNZ and MMH started with NDHB's Health Pathways initiative in 2018. With an objective of improving patients' engagement and experience, the initiative initiated a formal pilot programme of ManageMyHealth™ Patient Portal with Discharge Summary Notes between 2019 to 2021 with MMH, in collaboration with [redacted].

The MMH product relevant to this incident is the MMH Discharge Summary and Repository software module which enables patients with registered MMH accounts to use their MMH patient portal to view discharge summaries and other clinical information. As such, it involves the handling of patient data and is within scope for privacy, cyber security, and third-party risk considerations.

HNZ began a direct commercial supply relationship with MMH from 1 January 2023, whereby MMH provides Software as a Service (SaaS) solutions to HNZ. Prior to this time, MMH directly provided software services to primary health organisations (PHOs and GP practices) who chose to operate their patient portal, one of a number of companies operating in this space.

An Enterprise Licence and Services Agreement was executed between Te Whatu Ora Te Tai Tokerau (HNZ Northland) and MMH on7 March 2023, with a retrospective commencement date of 1 January 2023. **[260106 ManageMyHealth Enterprise Licence and Service Agreement_ fully executed.pdf, March 2023]** This agreement is supported by three associated Statements of Work: Northland Discharge Portal Repository Onboarding, Northland eReferral, and Northland Lab Result Repository Integration. These solutions include ManageMyHealth™ Patient Portal, Discharge Summary, eReferral, and Lab Test Results, enabling HNZ to share health information digitally with its consumers, with a particular focus on those residing in Northland.

The software supply contract between HNZ and MMH was based on the standard MMH service agreement template, with MMH's online Privacy Policy, Business Terms and Conditions, Terms of Use and Code of Conduct specifically incorporated by reference. **[260106 ManageMyHealth Enterprise Licence and Service Agreement_ fully executed.pdf, March 2023]** The online terms and conditions referenced were not retained as offline copies at the time the contract was executed, and these terms can be modified by MMH without contractual obligations to notify HNZ.

When MMH's services were engaged, the security and privacy obligations were not defined in detail. However, MMH confirmed, amongst other things, that both the organisation and its secure technology services would fully comply with the Privacy Act 2020, as well as the requirements set out in the Health Information Privacy Code 2020, as outlined in its Privacy Policy. **[12-02-2026 Privacy Policy _ Manage My Health.pdf, 18 September 2023, clause 1.2, last updated on 18 September 2023]**

Findings

FA1. Initial engagement with third-party vendor(s) could have more directly addressed requirements, design and risks.

The consumer portal requirement was a part of NDHB's Digital Programme since late 2019. The Health Pathways initiative at NDHB and MMH co-designed the portal project from 2018 to 2020. They worked together in good faith without formal agreements such as a Memorandum of Understanding or Mutual Confidentiality Agreement to outline the basic objectives, obligations and confidentiality safeguarding measures. **[Decision paper to Interim District Director re patient portal.pdf, 15 December 2022]**

Security, privacy and procurement policies and guidelines established by healthAlliance and regional IT functions were in place to govern engagement with 3rd party vendors. However, there is no evidence to support that the initial baseline due diligence by NDHB, such as a Privacy Impact Assessment, was undertaken during the initial exploration of the pre-pilot concept and subsequent solution discussions. The first Privacy Impact Assessment for the Patient Portal project was completed by MMH in December 2022. **[Procurement Policy.pdf, May 2022] [Northland - Privacy Confidentiality Statutes and Regulations.pdf, August 2022] [PIA Report (MMH) – Consumer Portal (221205), December 2022]**

FA2. ManageMyHealth™ Patient Portal did not meet the procurement and contract review thresholds at the time due to low contractual value, despite the high risk data involved.

The procurement of digital solutions and services was guided by the procurement and security policies and procedures of each DHB. When engaging with MMH for the pilot programme, NDHB was expected to follow the Northern Region procurement framework overseen by healthAlliance during that period. However, as the contractual value was below the review threshold of $100,000, it was not formally reviewed. **[Interviews, Feb – Mar 2026] [Procurement Policy.pdf, May 2022]**

The Northern Region Procurement Policy specified that procurement processes should be proportionate to the size/value, complexity and associated risks of each initiative. All risks are expected to be identified and managed consistently to the risk appetite with the Northern Region DHB. While policy compliance is the responsibility of the user, the Policy did not provide a detailed definition of risks

or reference a relevant risk framework to support users in making informed procurement decisions. **[Procurement Policy.pdf, May 2022]**

The Enterprise Licence and Services Agreement was established using MMH's standard licence agreement template, without introducing any notable changes that reflect the nature of the engagement, risk profile associated with the data and standard operational and procedural considerations. It is typical for software vendors, especially those offering Software as a Service, to favour their own licence agreements in order to maintain consistency in their core terms across all customers. In this case we note that: **[260106 ManageMyHealth Enterprise Licence and Service Agreement_ fully executed.pdf, March 2023] [Interviews, Feb – Mar 2026]**

- The security clauses are generic and do not cover third-party subcontractor information or their security requirements. It is unclear if MMH told the former DHB or HNZ about outsourcing technical work. Risks linked to using subcontractors were not addressed in the original agreement or during renewal.
- MMH's Privacy Terms are published online and incorporated by reference in the agreement. This limits HNZ's ability to effectively monitor and address context-specific risk assessments and any material impacts that may arise from unannounced changes to the online terms.
- Contractual term is evergreen and includes an auto-renewal clause after the initial 2-year term. This arrangement limits HNZ's ability to address gaps, review and update provisions such as service scope and performance, security and privacy and operational service delivery management.
- The Service Schedules in the original licence agreement gave only a basic outline of the services. They lacked details on technical and business roles from pilot to operational phase, making it hard to quickly identify stakeholders, clarify obligations, and assess business impact during the Incident Response Phase.
- In relation to agreement execution and commencement dates, typically a subscription starts after a successful pilot. This engagement did not do so, reducing HNZ's commercial leverage, and creating legal risks if the pilot was not fit for purpose.

There is no indication that any additional provisions or amendments have been incorporated into the sequential contract renewal in 2025, which marked the renewal anniversary following the completion of the initial two-year term of the original evergreen contract executed on 9 February 2023.

FA3. The business case for the ManageMyHealth™ Patient Portal and supporting documents should have provided more technical details, and the approval of outstanding conditions were not followed up thoroughly.
The initial solution design concepts and data flows outlined in the original business case and approval documents deviated from those implemented in the final delivered solution. The ambiguity was regarding the process by which HNZ information held by MMH in the Patient Portal Repository, is reconciled with the consumer's portal account.

There is no evidence that HNZ's relevant experts reviewed and approved the revised technical solution design. Differences were found between documented service design, processes, scope, and stakeholders' understanding, as well as in incident response records. This led to confusion about the services and affected

the initial response to the incident. **[Patient Portal Requirements, 19 November 2021] [Interviews, Feb – Mar 2026]**

The two PIAs completed, one by MMH in December 2022 and the other by HNZ in February 2023, had different and inconsistent understandings of the Patient Portal design for data storage. For example, MMH stated that portal information was retained indefinitely unless deletion was requested by the patient, while HNZ stated information would be regularly reviewed and disposed of. In addition, the MMH PIA showed MMH patient records interacting with SEHR patient records and noted that patients who were not MMH-activated would have information stored about them that they would not be aware of or be able to access, but the HNZ PIA stated that prior consent to storage would be obtained and data would be visible to patients. **[PIA Report (MMH) – Consumer Portal (221205), December 2022] [Privacy Impact Assessment (Te Tai Tokerau Consumer Health Portal) v1.0 Issue (Signed).docx, February 2023]**

The business case was developed by the project team to support the funding request. It was clearly stated that the follow-up activities such as data governance and security due diligence needed to be completed prior to the conclusion of the pilot phase. **[Business Case (Patient Portal) v1.0 Issued.docx, page 16-17, 03 April 2023]** We were not able to establish whether the identified assessments have been followed through during and post the pilot phase. There is some evidence from the subsequent Top Health security reviews that actions had been taken to address Patient Portal vulnerabilities.

FA4. Transition from the pilot to production could have been managed more effectively.
The ManageMyHealth™ Patient Portal with Discharge Summary had its initial go-live in November 2023 yet the service relationship remains managed by the project team at the time of the incident and at the time of writing. Clear operational/business and technical service ownership have not yet been formally established. This has weakened accountability for appropriate risk and security controls, and ongoing third-party risk management. **[Interviews, Feb – Mar 2026]**

Recommended actions

A-1. Ensure commercial and procurement processes use risk-based measures for activities like vendor oversight, contractual reviews and compliance checks. This is reflected in current HNZ policies and should be enforced in practice, for example using risk decision templates to guide operational activities. Assessments should factor in data type, quantity, breach impact, and service criticality.

A-2. A centralised register, such as a contract management solution or technology asset management solution, should be used to provide a single, authoritative source of information on software/services, vendors, and contracts. This approach can improve the effectiveness of incident prevention, response, recovery, and third-party and supply chain risk management. It also supports compliance and clarifies HNZ's internal ownerships and accountabilities.

A-3. A unified service gateway should be provided to channel all HNZ digital investments and planned procurements. This will establish a single point of entry for users which provides a streamlined path to all the required services including procurement, legal, digital services, data, privacy, and risk management. Service

requests should be captured and triaged early, enabling thorough vendor assessment before commitments are made. This also ensures clear ownership and accountability which supports ongoing risk management, and enables recommended action A-1, through providing a front door which assesses the risk of a proposed digital service or system.

A-4. Remediate MMH contract. *(HNZ has indicated planning for this recommended action is underway.)* HNZ should work with MMH to address the gaps in the existing Enterprise License and Services Agreement. Indicatively these could include matters such as:

- Security and privacy protection requirements
- Reporting, including incident reporting
- Information handling (retention, processing purposes etc).
- Rights for HNZ under specific scenarios
- Audit and assurance rights of HNZ
- Service management and ongoing requirements
- Subcontracting.

B. MMH Cyber Breach

What was the timeline and the specifics of the breach and the response by Health NZ? What is Health NZ's understanding of how the cyber breach occurred, including how the root cause was determined, the adequacy of security and privacy protections that were in place (to the extent that Health NZ patient information was compromised or at risk), and the impact of the breach on Health NZ services, patients and the wider sector?

A timeline of the breach and response is shown in the Background and Context section. This is broken down into five key timeframes:

- HNZ Relationship with MMH (Pre-2022)
- HNZ Relationship with MMH (2022-2025)
- Incident (December 2025)
- Incident Response (December 2025-January 2026)
- Incident Recovery (January 2026-March 2026)

HNZ's initial understanding of how the cyber breach occurred was based on conversations with MMH, and Vendor name removed. **[Interviews, Feb – Mar 2026]** On 3 January 2026, HNZ initially accepted that the incident was contained after receiving evidence regarding mitigation of the exploited vulnerability. **[Situation Report #21, 21 January 2026]**

However, after realising that some of the information was not relevant to the situation, HNZ moved to gain additional confidence and understanding which was informed by Vendor name removed. **[20260112 MMH Minister's update - 12 January.msg, 12 January 2026]** Vendor name removed were initially engaged on 31 December 2025 to conduct the digital forensics and incident response investigation of the MMH environment following the identification of the cyber incident. Specifically, Vendor name removed provided an initial incident response statement that confirmed the cyber breach access vector was a legitimate patient credential. This access vector was then used to identify a vulnerability within the portal, which when exploited allowed the threat actor to obtain documents stored in the Health Documents module of the portal. The Vendor name rem [redacted] incident response statement also outlined initial containment actions MMH

took to restrict access and further control the incident. **[Vendor name removed - MMH - Incident Response Statement - 2026-01-02.pdf, 2 January 2026]**

Further understanding of the root cause was provided in a containment statement from Vendor name removed on 16 January 2026 which indicated the Threat Actor had successfully authenticated to the ManageMyHealth™ Patient Portal on 21 December 2025 and interacted with an Application Programming Interface (API) to access information stored within the Patient Portal. From this containment statement, HNZ also understood that there was no evidence to support that the threat actor had interacted with any other MMH infrastructure or systems outside of the activities observed within the portal. **[2026-01-16 - ManageMyHealth- Containment Statement – Final.pdf, 16 January 2026]**

Details removed

As part of the response, Vendor name removed requested MMH to provide information regarding the pre-existing controls that were deployed within the MMH environment. These pre-existing controls – in addition to the specific incident containment actions taken by MMH as part of the response – enabled HNZ to have confidence that MMH had adequate security and privacy protections in place to contain the cyber breach. All MMH pre-existing and incident containment controls are listed in the Vendor name removed containment report from the 20 January 2026. Details removed

[2026-01-20 - ManageMyHealth - Containment Report – Final.pdf, 20 January 2026]

HNZ considered the likelihood of serious harm for the purposes of notifications under the Privacy Act and notified the Privacy Commissioner. HNZ also identified some harm scenarios within its MMH Scenario Planning - Individual Notifications Process **[MMH Scenario Risk Matrix.pdf, 2026]**. Both assessments were focussed on notification processes. Neither MMH or HNZ conducted a more detailed harms analysis to determine the impact of this data breach, and the impact that a leak of the data included could have on different types of patients and the wider sector. HNZ was unable to directly determine the extent that HNZ patient information was compromised or at risk due to not being provided direct access or copies of the data MMH held within the impacted systems. **[Interviews, Feb – Mar 2026].** Without access to the required information from MMH and a more detailed harm analysis being performed on the impacts of the data breach, HNZ cannot determine what response actions are appropriate for different types of patients or data breach categories – such as what communications that will be sent out, or what additional controls need to be implemented such as monitoring.

HNZ actively enabled support pathways to be available as needed to impacted patients. This included funding for free GP consultations where impacted patients needed support from their GP. Support was also made available through ID Care for extra pastoral and social care. **[MMH Breach – Support pathways 08012026.pdf, 6 January 2026] [20260110 Minister's report - 10th January, 10 January 2026]**

As part of the response HNZ discussed the risk of the MMH breach impacting further HNZ systems and services, and determined this incident was limited to just the MMH platform and did not have broader impacts to HNZ systems **[20260104 Minister's update - 4 January.msg, 4 January 2026]**. However, there was no formal documentation of the analysis performed to come to this conclusion. **[Interviews, Feb – Mar 2026]**

Findings

FB1. Existing security and privacy controls were not appropriate or validated as being effective.

Details removed [redacted]

The pre-existing controls deployed within the MMH environment were understood through the Vendor name removed background information requests as part of the response. While this enabled HNZ to determine that security and privacy controls were in place and further strengthened by incident containment controls, this information relies on statements from MMH and has not otherwise been independently validated.

FB2. Best practice guidance is for more complete documentation around critical incident response escalation and decision-making.
Initial identification and confirmation of a cyber incident at MMH required HNZ to reach out through the parent vendor to identify that there was an incident, in the absence of documented contact details for MMH. **[FW Removed for pri contact deets.msg, 31 December 2025]**

HNZ did not document the risk assessments for impacts to broader HNZ systems and services. While this is a credible assumption given the MMH system involved in the breach, we believe the inconsistencies in the Patient Portal design documentation and PIAs, and a lack of clarity on exactly what data was flowing to MMH and being retained in the Patient Portal, would warrant further investigation to fully understand and document the impacts. **[Interviews, Feb – Mar 2026]**

Recommended actions

B-1. Ensure that harms analysis performed as part of all HNZ incident response activities where there is potential for personal information to be impacted is used to determine appropriate activity by HNZ – such as notifications needed, additional controls required, monitoring required and support mechanisms that must be put in place – which may differ for different types of patients of data breach categories. HNZ's ability to do harms analysis for the MMH breach was impacted by access to information, and so where third-party vendors are involved in the breach, this may require HNZ to have contractual provisions to enable access to data to facilitate the analysis and response.

B-2. Define the expectations of what is sufficient evidence for security assurance of third-party solutions. These should include:

- Expectations for which environments penetration tests can be performed on, such as if testing is performed on a development

environment that penetration test must provide evidence that this is the same as production.
- Scoping requirements for penetration tests emulating attack types – specifically making sure these are not complete black box testing but also include abuse cases where legitimate credentials and accounts can access data/files they should not be able to.

B-3. Take additional steps to ensure all critical decisions and related rationale during incidents are documented with supporting evidence, such as HNZ system and impact assessments which has a critical bearing on the determination of incident scope and potential harm. Where this detail is not able to be documented, the reasoning for this must be captured to provide transparency of decision making and a defensible decision for HNZ.

B-4. Record the key contact details for third-party suppliers that support HNZ in the event of an emergency. These should be available alongside a catalogue of HNZ-provided data they have access to, and the digital services and systems they provide.

C. Other HNZ impacts

Were any other non-MMH systems or processes compromised in the cyber breach? What is the adequacy of the security and data protections related to those systems?

From the current incident investigation and forensic analysis conducted independently by Vendor name removed and Vendor name removed, commissioned by MMH, HNZ acknowledges that the incident is contained and no other non-MMH systems or processes were compromised in this cyber breach. [**Interviews, Feb – Mar 2026], [2026-01-16 - ManageMyHealth- Containment Statement – Final.pdf, 16 January 2026]**

(For noting) As there is no evidence to indicate that any non-MMH systems and processes were compromised during this cyber breach, therefore, the adequacy of the security and data protections related the non-MMH systems cannot be assessed at this stage.

HNZ has implemented dark web monitoring to detect activity related to MMH, and no anomalous activity has been detected currently. **[Re MMH Internal Review Questions (CSIRT).msg, 24 March 2026]** Details removed .

Findings

FC1. Evidence indicates no compromise of non-MMH systems or processes, and understanding of the breach's broader implications across HNZ's wider portfolio remains limited.

HNZ and MMH have stated with evidence from forensic analysis that no directly connected systems have been compromised. There is currently no evidence of comprehensive technical analysis or diagnostics to confirm that risks in the end-to-end solution are sufficiently well understood and controlled. **[Vendor nam MMH - Independent review of MMH data breach reports 110526.pdf, 11 May 2026] [Minister's Update, 4 January 2026]**

FC2. Considerable effort would be required to investigate the wider HNZ digital portfolio, and a prioritised approach would likely be required to do so.

Given that HNZ has identified over 5,000 digital products and platforms within its

ecosystem, a considerable level of effort and both business and technical expertise is required to ensure that no other systems have inadequate security and data protections. **[Interviews, Feb – Mar 2026]**. In their report on patient portals, [redacted] examined the varying approaches to patient portals across New Zealand's health ecosystem, including the differences in contract management arrangements, due diligence or security assurance. The extent of this risk cannot be understood without further analysis, and there remains a knowledge gap when considering the security and data protections for these systems in the wider portfolio. **[Signed_04 Mar_RCSD_Health NZ - Primary Care Sector - Patient Portal Discovery Report.pdf, 4 March 2026]**

FC3. The Digital Services Hub is an effective tool for securing and standardising access to health information. HNZ's Digital Services have also established the Digital Services Hub, a developer platform, to streamline and secure access to New Zealand Heath Information Data under the custodianship of HNZ. The platform is intended to offer a unified, secure, and standards-driven environment to integrate with HNZ's hosted data and digital services. **[Health New Zealand Digital Services Hub, 2026]**

Recommended actions

C-1. Perform risk assessment across HNZ's portfolio to focus efforts on higher-risk data, digital systems and services, and where these are identified these must undergo targeted cyber security and privacy assessments.

C-2. Continue the deployment of the Digital Services Hub as a preferred model for secured access to health information to limit the unnecessary copying of data.

D. Incident Response

What was Health NZ's role in supporting the incident response? How effective was the support from Health NZ to that response? How has Health NZ obtained confidence that the incident has been contained, and that the root cause and contributing factors have been identified and been mitigated? If not yet contained or mitigation actions yet to be completed, how is Health NZ supporting the response and maintaining oversight?

As part of the response HNZ took on the lead agency role as part of an All of Government Incident Management Team (AoG IMT) with responsibility for aligning supporting government agencies and MMH as well as providing one source of truth for this incident. **[RE ManageMyHealth Cyber Breach - Urgent Briefing.msg, 1 January 2026]**

As the lead agency HNZ expended a large amount of time and resources to lead the All of Government (AoG) response and support the MMH breach. MMH also committed significant resources to the response and remedial actions. Interviews noted the long days, missed weekends and holidays, and personal investment made by many individuals who were part of the wider response team. **[Interviews]** This level of effort was appropriate due to the inherent nature of the data contained within the MMH breach, specifically the identity and health data. Early indications showed that a lack of proper care could result in negative public perception and media commentary focused on HNZ despite it being MMH's problem to resolve. **[20260105 FW_ Minister's update - 5 January.msg, 5 January 2026]**

The effectiveness of HNZ role in the AoG response was made more challenging by the following issues:

- HNZ identified on 31 December 2025 that it provides a channel for the public to create an MMH account through the HNZ My Health Account service. Email briefings indicated that no evidence was found to suggest that the My Health Accounts were compromised and there were no technical impacts for HNZ but this took time to establish as MMH was initially unable to share how the attack occurred. **[RE ManageMyHealth Cyber Breach - Urgent Briefing.msg, 1 January 2026]**
- Due to the nature of HNZ's relationship with MMH as outlined in the Background and Context section, HNZ had not established a contractual option to enable it to play an active role in MMH's response. The only avenue that enabled HNZ to take supportive actions in relation to the MMH breach was that the breach involved HNZ-provided data. Initially HNZ looked to work with MMH to get access to the compromised data to be able to undertake parallel analysis **[20260103 Minister's update MMH - 3 January 2026.msg, 3 January 2026].** No evidence was provided to indicate that the compromised data set was received by HNZ. On 12 January HNZ's acting CITO emailed a directive to MMH's Chief Executive Officer stating that the information provided by MMH to date was insufficient to enable confidence in the security of the MMH platform and that the email was a formal request for MMH to provide evidence that the incident had been contained and the broader platform secured by the following day 13 January at midday. **[FW Request for immediate delivery of security evidence and assurance Manage My Health.msg, 12 January 2026]**. The first confirmation by HNZ that this assurance information had been received in totality was on 21 January, confirming that the incident had been contained, the vulnerability remediated and there is no evidence of attacker presence. **[20260123_Minister update Jan 23 2026.pdf, 23 January 2026]**

HNZ's response IMT formally transitioned to a recovery IMT on 21 January 2026 following conversations and agreement between the DPMC, AoG IMT and HNZ as the lead agency. **[20260123_Minister update Jan 23 2026.pdf, 23 January 2026]** The transition from response to recovery was supported with a transition to recovery plan dated 21 January 2026 which outlined the rationale for transitioning the response into recovery, specifically stating:

- HNZ systems remain secure and are not impacted by the breach, with no impacts to clinical care.
- An interim solution for the privacy issue identified in Northland has been agreed and is in development.
- Wrap around support is in place for notified individuals.
- There are two remaining cohorts for notification, which can be addressed as recovery actions.

Underpinning these points, the transition to recovery enabled the IMT team members to stand down and rest as a key risk mitigation for HNZ's ability to respond to its own cyber-attacks **[HNZ Transition to Recovery Plan_ MMH incident_Jan26.pdf, 21 January 2026].** We noted in our interviews while response team members take their jobs very seriously as professional individuals, being active for up to 22 days without reprieve can lead to fatigue and take a toll on individual wellbeing. **[Interviews, Feb – Mar 2026].**

As outlined in section Incident Response (December 2025-January 2026), HNZ obtained confidence that the incident had been contained through the initial incident response statement provided by Vendor name removed. This confirmed the cyber breach access vector as a legitimate patient credential. These credentials were then used to identify a vulnerability within the ManageMyHealth™ Patient Portal, which when exploited allowed the threat actor to obtain documents stored in the Health Documents module of the portal. The Vendor name removed incident response statement also outlined initial containment actions MMH took to restrict access and further control the incident. [Vendor name removed **- MMH - Incident Response Statement - 2026-01-02.pdf, 2 January 2026]**

HNZ gained confidence that the incident was contained through a range of technical tests on the ManageMyHealth™ Patient Portal to identify any potential security issues. This testing was carried out by Vendor name removed and Vendor name removed; who delivered the following:

- Details removed

Further understanding of the root cause was provided in a containment statement from Vendor name removed on 16 January 2026 which indicated the Threat Actor had successfully authenticated to the ManageMyHealth™ Patient Portal on 21 December 2025 and interacted with an Application Programming Interface (API) to access information stored within the Patient Portal. From this containment statement, HNZ was also provided with confidence that there was no evidence to support the threat actor had interacted with any other MMH infrastructure or systems outside of the activities observed within the portal. **[2026-01-16 - ManageMyHealth- Containment Statement – Final.pdf, 16 January 2026]**

Incident response containment and mitigation actions in relation to the data that has already been taken by the threat actor has been identified within the MMH systems, with impacted individuals notified. HNZ will continue to monitor internet forums for potential future leaks of the data that was taken by the threat actor through dark web monitoring **[Re MMH Internal Review Questions (CSIRT).msg, 24 March 2026].** Beyond ongoing oversight and monitoring actions related to the data breach, traceability of the threat actor actions has not been documented, and no evidence has been gathered to indicate that the Threat actor has disposed of the stolen data. This means individuals' health data exists on the internet and could lead to further impact in the future.

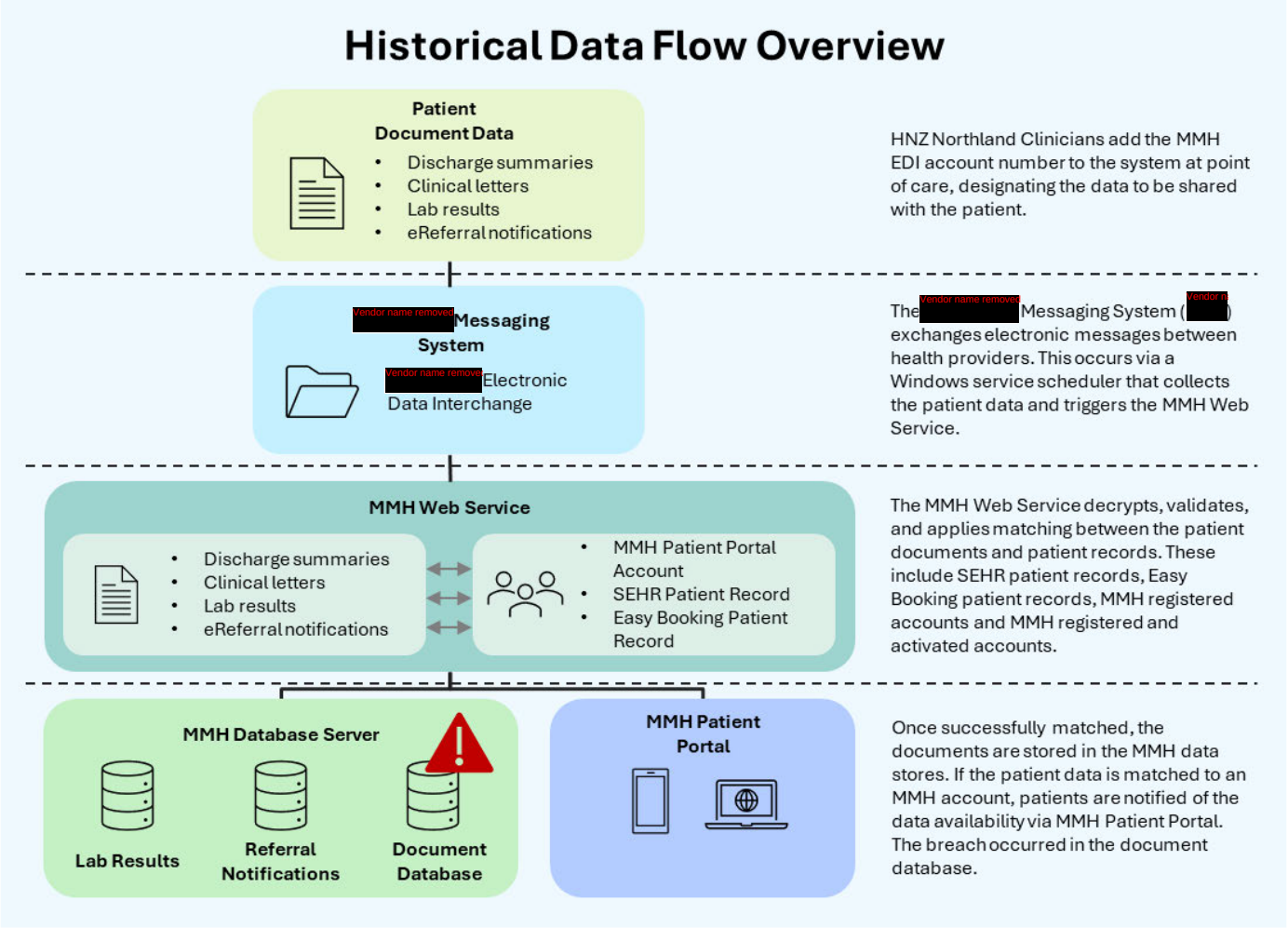
With HNZ supporting the MMH response to the data breach that occurred, HNZ sought an independent review of the digital forensics, privacy and security testing conducted in connection with the MMH Breach by [redacted]. The report provided an outline of actions taken to contain the unauthorised access, trace what data had been exfiltrated, and identify the root cause for the breach. The report observed that some granular detail was present for the work completed but was not present across all areas [redacted] expected to be included and [redacted]

[redacted]

The MMH Patient Portal was retaining data from HNZ for patients who had non-activated and suspended accounts. **[ELT Paper - Manage My Health - Health NZ Actions_4.15pm (002).docx, 16 January 2026].** These were stored in the MMH environment and no evidence of the specific timeframe this was retained for has been identified, although MMH's PIA indicated retention of this data was "indefinite". Some of this information would not have been visible to the patient given the different types of patient record in the system, for example if matched against SEHR for non-activated accounts. **[PIA Report (MMH) – Consumer Portal (221205), December 2022]** HNZ advised two immediate actions for MMH to complete, the first being to stop uploading documents issued by HNZ to non-activated and suspended accounts, and the second action was to delete material that is not matched to a currently activated account. **[ELT Paper - Manage My Health - Health NZ Actions_4.15pm (002).docx, 16 January 2026]**

To address the first issue, the patient matching criteria within the ManageMyHealth™ Patient Portal was changed to only match with MMH activated accounts that were not in a suspended state, effective from January 2026 with document delivery blocked and files discarded if the patient matching criteria was not met. **[DM2_1_MMH-HNZ-Information-Architecture_v2.0.pdf, 19 March 2026]**

To address the second issue relating to existing HNZ Northland documents being attached to non-activated users, HNZ instructed MMH to execute a one-time historic data removal for non-compliant documents. However, due to a need to continue notifying impacted individuals HNZ looked to explore creating a secure store of the removed documents to allow impacted users to view the documents in conjunction with a breach notification. **[FDS- HNZ Northland Documents - Receipt, Processing & Visibilityv1.0 16-Jan-26.docx, 20 January 2026]**



HNZ later clarified to MMH on 11 March 2026 that a copy of all personal information that was stored for "non-registered" patients which was impacted in the cyber-breach should be kept securely and be used only for the purposes of fulfilling MMH's obligation to notify impacted patients and responding to any Office of the Privacy Commissioner (OPC) inquiry. HNZ's Legal Counsel suggested that the information be retained by MMH for the next two months, which would then be reviewed if an ongoing need to hold the data arose. **[FW_ Information for Response to Privacy Commissioner - Information Urgently Required Today.msg, 13 March 2026]**

Further complicating the response, 16,461 under-16-year-olds were identified as impacted by the breach. **[DM7_1_Numbers of people and data impacted.pdf, 2026]** This caused challenges and additional risks within the notification process as there was concern parents may be notified and not have the appropriate consent to access this information. HNZ provided MMH with requested support for planning the appropriate notification to these individuals, as their parents/guardians may not have visibility of the health information and related treatment. **[Aide Memoire - Update on notification process - HNZ00200643 - Sent to MO 13.2.26.pdf, 12 February 2026]**

Findings

FD1. Guidance for All of Government (AoG) Responses could provide more advice for resourcing long-running responses to avoid a disproportionate load on the lead agency. Acting as the lead agency for the AoG response placed

sustained pressure on HNZ's response capability. The 22-day response period required the handover of in-progress actions to recovery workstreams, enabling response personnel to reprioritise wellbeing and core responsibilities. Although the effort was appropriate and necessary, it highlighted potential risks should multiple incidents arise concurrently. HNZ has commenced work to build sector capability along with other agencies, which is a good initiative and could be further supported by formal guidance. **[national-resilience-system-handbook-may2025.pdf, May 2025]**

FD2. There could have been more directional questions/objectives to focus specific actions on high priority elements that needed to be determined and definitively answered. These questions would have focused actions to most effectively and urgently address the required outcomes contextual to the breach. especially in relation to how the incident impacted HNZ and its data. The objectives we have seen are related to managing the AoG response **[Situation Report #21 21 Jan 2026.pdf, 21 January 2026]**, and internal structure/mechanism for response – notably named "response objectives" **[20260102 initial Action plan MMH .pdf, 01 February 2026]** Best practice would suggest there is a benefit to having guiding questions/objectives which HNZ needed to address in relation to it experiencing an incident (indirectly through its third party and HNZ data being impacted).

FD3. HNZ were too quick to accept assertions that the vulnerabilities were remediated through third-party security assurances. HNZ initially derived confidence from MMH's selected penetration testing vendor [redacted] but this was later reversed when HNZ found the scope of testing to be limited to the demo environment and did not directly apply to the ManageMyHealth™ Patient Portal in production. This led to HNZ sending a formal request to MMH for additional information to gain confidence that the issue was fully remediated within the ManageMyHealth™ Patient Portal **[FW Request for immediate delivery of security evidence and assurance Manage My Health.msg, 12 January 2026]**.

FD4. Findings and recommendations from independent reviews of digital forensics, incident response and testing work are in progress or to be completed. [redacted]. HNZ and MMH have agreed to complete a HISF assessment for MMH, and we are advised this is underway. **[MMH - HNZ Assurance Update 10 Feb Jan.pptx, 10 February 2026]**.

FD5. Data retention and removal timelines have not yet been clarified. There were different understandings between MMH and HNZ on the duration MMH was expected to retain health information after the user account and consent validation processes are completed. The interviewees provided varied understanding about the data retention processes **[Additional data flow questions from HNZ - 2 Feb 2026.docx, 2 February 2026]**. HNZ has outlined that all historic non-compliant information within MMH must be deleted, however there is also a need for this data to be available for MMH to fulfil its obligations to provide the data as part of patient notifications and responding to the OPC inquiries. While the plan is to review the situation in two months, there is currently no indication of the actual timeframe for when this clean-up will occur.

FD6. New processes to enable immediate deletion, and only saving data against the patient portal, are insufficiently evidenced. On 20 January 2026 HNZ and MMH established agreed use cases that outline MMH will only store documents against activated registered accounts, and if no match is identified, the data is deleted. **[FDS- HNZ Northland Documents - Receipt, Processing & Visibilityv1.0 16-Jan-26.docx, 20 January 2026].** MMH provided attestation and screenshots that these were implemented **[FW Recommendation to Proceed with Active Accounts change in Manage My Health.msg, 19 March 2026], [Not Match recovered Deleted.png, 22 January 2026], [Match patient Record.msg, 22 January 2026].** Without further information and context, this evidence is insufficient to validate that these processes are working appropriately.

Recommended actions

D-1. Address outstanding findings and recommendations from independent reviews of digital forensics and incident response and testing work so that HNZ can close any issues related to MMH. Determine and agree timings, and perform the planned HISF assessment on MMH. Where MMH is found to not align to the HISF assessment these outstanding items must be identified, tracked and monitored to ensure progress of these remediation items. (*HNZ has indicated the HISF assessment of MMH is underway.)*

D-2. Provide additional guidance on how lead and support agencies in a long-running All of Government level response are managed so that the lead agency is not disproportionately resource constrained by long-running response timelines, which can impact responder wellbeing.

D-3. Strengthen contractual governance through a risk-based tiering approach to contract clauses across HNZ's portfolio of digital services and systems. Indicatively these should consider additional requirements related to security, privacy, information-handling, subcontracting, service management, incident reporting, rights when incidents occur, and audit and assurance rights. These should be applied based on the risk profile and proportional controls required for the contracts going forwards, as well as to support contract negotiation processes. In addition, these requirements should be incorporated into existing contracts as they are renewed or extended.

D-4. Establish key questions for each incident to guide the response, including for an AoG level response. Questions should be established for any incident/breach that impacts HNZ directly or indirectly (e.g. through a third party). This provides clear overall direction for the response, the communication provided to internal and external stakeholders (e.g. the Board and Ministers), and improves ease of centralised tracking of relevant outcomes and progress on activities. It should be noted that these are different from HNZ's response objectives as they are not about the mechanisms and process steps of the response, but instead the thinking that would be applied to enable core concerns to be considered and addressed with focus and urgency. This can be integrated alongside the CIMS process, and does not intend to replace it. For example in an incident like this, the questions could be:

- How did the threat actor obtain entry – do we know the specific vulnerabilities and causal factors? Have these been addressed?
- Do we need to consider, and if so what are the implications of suspension of the affected service?
- What are our rights by contract and how do we effectively direct / influence the response?

- Have we understood and stopped the bleeding?
- Have we resolved the full extent of what the problem is?
- What was the extent of impact in terms of privacy and information disclosure? What is the harm posed and what are our obligations?
- What steps do we need to take to have confidence in continuing with all customer functionality?
- What can we learn here and need to implement immediately, and as a more planned and measured improvement?

D-5. Require evidence be provided for any assertion of security controls effectiveness and incident mitigation, to provide confidence that controls that have been bypassed or broken during an incident can be relied upon on an ongoing basis and have not introduced additional vulnerabilities, and that root cause exposures have been remediated.

D-6. Capture findings and recommendations from independent reviews of digital forensics and incident response and testing work so that HNZ can refine security practices and apply any lessons learned from this incident to future incident responses.

D-7. Plan and set dates for corrective actions around removal of non-compliant data once MMH has satisfied obligations to provide the data as part of patient notifications and responding to the OPC inquiries. (*HNZ has indicated they are working through the logistics and consequences of requesting this.)*

D-8. Establish HNZ internal information retention standards and guidance. This should specifically include expectations on retention of health information stored or processed by third parties providing health digital services on HNZ's behalf.

D-9. Set clear expectations for patient and whānau consent collection across the health sector, specifically in relation to front line health organisations (hospitals, GPs, ACC etc) collecting data, and putting this into vendor systems. This should enable effective collection and alignment to the Privacy Act 2020. Where there is direct collection of patient data into vendor systems (such as individual uploads of additional data into the MMH Patient Portal), this must be considered within the expectations.

D-10. Perform validation of newly implemented data deletion and matching processes implemented at MMH to provide full confidence that the implementation has been successful. This should include obtaining context on the implementation of matching and deletion processes related to the screenshots provided.

E. Cyber Security and Privacy

What relevant security and privacy requirements were in place by MMH in relation to HNZ information and how much involvement did Health NZ have in setting these requirements? How has Health NZ assured itself that these requirements were being appropriately met by MMH both when Health NZ established the relationship with MMH and ongoing? Has Health NZ been notified by MMH of any cyber incidents or material vulnerabilities or privacy concerns prior to this incident occurring?

When initially established, HNZ did not establish specific detailed security and privacy requirements to be fulfilled or maintained by MMH when provisioning the services. The Enterprise Licence and Services Agreement between HNZ Northland and MMH provides the key overview of services to be delivered by MMH and is intended to cover the general security and privacy clauses.

The contract template was based on MMH's standard Licence and Services Agreement. Through the use of this template, the MMH Privacy Policy, Security Policy, Business Terms and Conditions, Terms of Use, and Code of Conduct have been incorporated and made available online, with the understanding that these terms may change without advance notice. Consequently, without proactive monitoring and contractually required notification, HNZ may not be aware of the privacy and security implications arising from any changes to these terms; and whether such changes materially differ from HNZ's security and privacy requirements. **[Manage My Health Systems & Security, April 2026], [Manage My Health Terms of Use, April 2026] [260106 ManageMyHealth Enterprise Licence and Service Agreement_ fully executed.pdf, March 2023]**

These security and privacy requirements were not specifically negotiated or tailored to address the particular privacy data involved. In contrast, an alternative approach was used in the Details removed contract executed on 25 November 2025, with the commencement date of 1 July 2025. In that case the HNZ standard contract template is used as the head agreement for engagement with MMH. This includes the provision of HNZ's standard privacy, confidentiality, third party subcontracting, audit, indemnity, warranties, dispute and remediation clauses. Specific annexes outlining explicit service description and performance expectations, special terms and provisions set out by HNZ for MMH to deliver. [Details removed **Contract.pdf, page 2-24, 25 November 2025]**

No evidence was found that HNZ performed any security assurance activities relevant to the services provided by MMH in the initial pilot phase before November 2022. A PIA was performed by MMH and another was completed by HNZ in advance of the Business Case being approved, and no other relevant cyber security assessments by HNZ were identified until the subsequent Top Health request to access the MMH Patient Portal. **[Privacy Impact Assessment (Te Tai Tokerau Consumer Health Portal) v1.0 Issue (Signed).docx, February 2023]**

The security and data privacy assurance activities that were performed on MMH are as follows:

- The PIAs performed before the Business Case were inconsistent with each other and not consistent with the solution design or maintained to reflect the as-built solution or the later extensions to capability that were added (Lab Results, e-referrals). **[PIA Report (MMH) – Consumer**

Portal (221205), December 2022] [Privacy Impact Assessment (Te Tai Tokerau Consumer Health Portal) v1.0 Issue (Signed).docx, February 2023].

- A set of security and privacy assessments were performed on Top Health (a general practice based on premises at Kaitaia Hospital), which provided some relevant information about the MMH Patient Portal. It is not clear if this information resulted in actions to strengthen the wider patient portal project's cyber security and privacy stance, and therefore they only provided partially relevant assurance for these services. **[TRA Manage My Health.xlsx, 16 September 2024], [SRS Report_ Top Health to use Manage My Health (ISRS 678) v1.0.pdf, 23 October 2024], [Privacy Impact Assessment Top Health, November 2023].**
- HNZ maintained the Te Tai Tokerau Consumer Health Portal Steering Group which included MMH staff as a standing attendee. Key activities of the project included "Technical aspects to send appropriate documents to the portal", with no specific mention of security or privacy expectations. **[Te Tai Tokerau Consumer Health Portal Steering Group Meeting Minutes, 6 March 2023]**

The application of current security and data protection processes can vary within and across HNZ. Engaging with the relevant HNZ security and privacy process is typically managed through a self-service model **[Engagement Process as per National Cyber Security Home Site.pptx, 2026]**. While the functional areas, including privacy, security, and procurement, have developed comprehensive frameworks, guidance, and resources, getting the appropriate support continues to depend significantly on the requestor's knowledge of the digital solutions or services they intend to procure, and their understanding of the associated risk implications.

As such, security's involvement is only required for assurance activities where a system fits the scope of a "high workflow", otherwise the security activities can be performed without security's involvement. While the MMH solution would fit the scope of a high workflow if it was to be assessed today, completing this process would require the project team to be aware that security processes must be applied, identify the service/project as high risk, and to engage security in line with this high rating **[Engagement Process as per National Cyber Security Home Site.pptx, 2026]**.

MMH has not gone through the current security process due to this being a historic service that existed in advance of the newer security assurance process, which was implemented in 2025. **[Interviews, Feb – Mar 2026]**.

The process for privacy's involvement relies on the projects, teams and the wider HNZ organisation to reach out to the privacy team to determine the need for assessments. **[Interviews, Feb – Mar 2026]**

During the engagement with MMH, one privacy incident and one vulnerability was raised to HNZ about MMH. The vulnerability was not provided by MMH directly but by Ministry of Health, who had been informed by an independent security researcher, who then informed HNZ **[RE Vulnerability Disclosure for Manage My Health.msg, November 2025]**. This vulnerability was determined to not be relevant to the incident by HNZ **[20260103 Minister's update MMH - 3 January 2026.msg, 3 January 2026].**

Findings

FE1. At the time, HNZ did not establish clear, specific, or enforceable security and privacy requirements for MMH services that process or store HNZ patient information. The security and privacy obligations that did exist relied on MMH's standard contractual terms, which were not tailored to reflect the sensitivity or scale of health information involved, and afforded limited opportunity for HNZ to require ongoing alignment with its expectations.

FE2. HNZ did not undertake adequate security or privacy assurance activities at the commencement of its relationship with MMH, when contracts were entered into or extended, or when new MMH services were introduced. The PIAs completed in December 2022 and February 2023 were inconsistent, did not reflect the design, and was not maintained to reflect the as-built solution or subsequent expansions in functionality, including lab results and e-referrals. Security and privacy assessments undertaken in other contexts (such as Top Health) were performed later and did not provide complete assurance over MMH services relevant to the incident.

FE3. Processes for triggering security and privacy assurance activities rely on self-identification by delivery teams, resulting in gaps for historic services such as MMH. MMH not undergoing initial assurance activities can also mean that it not be picked up later as contract renewals/extensions can assume prior security reviews have been completed. Although HNZ was notified of a prior privacy incident and a separate vulnerability related to MMH, notification was informal and/or indirect, escalation was inconsistent, and neither event resulted in a broader reassessment of MMH security and privacy assurance.

Recommended actions

E-1. Define, document and follow thresholds for privacy and security reassessment activities. This should be applied where there are significant changes to existing services, when onboarding new digital services or systems (through the unified service gateway), or on renewal/extension if privacy and security assessments have not previously been completed.

F. Looking beyond MMH

What regulation, standards and policy/processes apply to cybersecurity and data privacy generally in NZ? To what extent are these formally prescribed versus industry good practice? What is the role of the HISO function in Health NZ defining these and how should HNZ assure itself that these requirements are appropriately met by third party suppliers?

New Zealand's cyber security and privacy ecosystem is disjointed and inconsistent, applying unevenly across different sectors. The cost of implementing strong security practices is often far higher than any penalties incurred under any regulation for a privacy breach.

The Privacy Act 2020 is the only legislation to provide a universal, legally binding baseline across the country. All other security and data privacy standards, policies and processes are either:

- Mandated only for certain government agencies (PSR, NZISM, NCSC Minimum Standards),
- Voluntary / sector-led guidance (HISO standards, HISF), or
- Industry recognised good practice (ISO 27001, ISO 27799)

Third-party suppliers operate under variable expectations, and the protections afforded to individuals' data depend heavily on the sector controlling it.

Across all frameworks, the implications of non-compliance vary from formal legal risk (in the case of the Privacy Act) to governance, operational, reputational, and contractual consequences (for optional or government-only frameworks).

Standard	Regulatory Status	Authority	Implications of Non-Compliance
Privacy Act 2020	Mandated for all agencies that collect or hold personal information in NZ.	Office of the Privacy Commissioner (OPC).	Maximum penalty of $10,000 for failure to notify the OPC of a breach. Non-compliance of an information privacy principle risks maximum compensation of $350,000.
Protective Security Requirements (PSR)	Mandated for all New Zealand public service departments and certain Government agencies (not HNZ) that collect or hold personal information in NZ.	No external authority. Agencies are held accountable by their Chief Executives, with stewardship provided by the Government Chief Information Security Officer (GCISO).	No formal implications.
The New Zealand Information Security Manual (NZISM)	Mandated for all New Zealand public service departments and certain Government agencies (not HNZ) that collect or hold personal information in NZ, recommended for other agencies.	No external authority. Compliance is assessed through Certification and Accreditation (C&A) process, where the accreditation authority is the agency Chief Executive or the GCISO for certain high-assurance system.	No formal implications.
National Cyber Security Centre (NCSC) Minimum Security Standards	Mandated for all New Zealand public service departments and certain Government agencies (not HNZ) that collect or hold personal information in NZ.	Compliance is assessed through the Protective Security Requirements (PSR) assurance reporting process, with the NCSC providing assessment and oversight.	No formal implications.
Health Information Standards Organisation (HISO)	Not mandated.	No certification or enforcement authority.	No formal implications.
The Health Information Security Framework (HISF)	Not mandated.	No certification or enforcement authority.	No formal implications.

International Standards Organisation (ISO)	Not mandated.	No direct certification authority; individual standards may support third-party certification (e.g., ISO/IEC 27001).	No formal implications.
ISO 27001, 27002 & 27799:	Not mandated.	ISO standards are voluntary; ISO/IEC 27001 may be certified by accredited bodies, while ISO/IEC 27002 and ISO 27799 provide supporting guidance and are not certifiable.	No formal implications.

In the sections below we explore each standard in more detail.

Privacy Act 2020:

Regulatory Status: Mandated for all agencies that collect or hold personal information in NZ

Authority: Office of the Privacy Commissioner (OPC)

Implications of Non-Compliance: Maximum penalty of $10,000 for failure to notify the OPC of a breach. **[Privacy Act 2020, Section 118]** Non-compliance of an information privacy principle could be taken to the Human Rights Review Tribunal, who hear claims of breaches of the Privacy Act and have the authority to award damages, by an individual affected by a breach for a maximum compensation of $350,000. [**Human Rights Review Tribunal, 2026]**

Overview: The Privacy Act 2020 is New Zealand's primary data privacy law that applies for all agencies that collect or hold personal information. It establishes 13 Information Privacy Principles governing how personal information is collected, used, disclosed, retained, accessed, and protected, including a mandatory notifiable privacy breach regime. Compliance is overseen by the Office of the Privacy Commissioner, which has investigation and enforcement powers. Where personal information is shared with third parties, the originating agency remains responsible for ensuring compliant handling through appropriate contractual and governance controls.

The Privacy Act 2020 is supplemented by legally binding Codes of Practice, which modify or replace the Information Privacy Principles for specific industries, organisations, or types of information. These Codes apply across multiple domains, including health information, credit reporting, telecommunications, biometrics, and CCTV, and are used where information types or sector contexts warrant more prescriptive rules. Where a Code applies, compliance is assessed against the Code rather than the general IPPs, while oversight and enforcement remain with the Office of the Privacy Commissioner.

The Health Information Privacy Code 2020 (HIPC) is one such Code and illustrates how this model operates in practice, replacing the IPPs with sector-specific rules for handling particularly sensitive information; similar approaches are taken in other regulated sectors, such as credit reporting and telecommunications. Obligations under a Code cannot be avoided through

outsourcing, and agencies remain accountable for ensuring third parties who are operating as an agent handle information in accordance with the applicable Code.

Protective Security Requirements (PSR):

Regulatory Status: Mandated for all New Zealand public service departments and certain Government agencies (not HNZ) that collect or hold personal information in New Zealand.

Authority: No external authority. Agencies are held accountable by their Chief Executives, with stewardship provided by the Government Chief Information Security Officer (GCISO)

Overview: The Protective Security Requirements are the New Zealand Government's overarching protective security policy framework, covering personnel, physical, and information security. PSR sets mandatory security expectations for government agencies and establishes accountability at chief executive level for managing security risks. The Director-General of the NZSIS holds the role of Government Protective Security Lead (GPSL). The GPSL provides protective security leadership, guidance, and support for chief executives, organisations, and systems across New Zealand. The NZSIS develops, maintains, and supports government agencies to implement the Protective Security Requirements (PSR). [**Protective Security Requirements – Roles and Responsibilities, 2026]** When agencies engage third parties, PSR requires security risks to be managed across the supply chain, with accountability retained by the agency.

The New Zealand Information Security Manual (NZISM):

Regulatory Status: Mandated for all New Zealand public service departments and certain Government agencies (not HNZ) that collect or hold personal information in NZ, recommended for other agencies.

Authority: No external authority. Compliance is assessed through Certification and Accreditation (C&A) process, where the accreditation authority is the agency Chief Executive or the GCISO for certain high-assurance systems.

Overview: The New Zealand Information Security Manual (NZISM) is the Government's primary manual for information assurance and system security and sits within the PSR framework. It defines baseline and additional security controls across areas such as access management, logging, incident response, cloud security, and supply chain risk. NZISM is mandatory for prescribed government agencies and encouraged for Crown entities, local government, and private sector organisations. Supplier security requirements are enforced through contracts and service agreements, while overall responsibility for security outcomes remains with the agency.

National Cyber Security Centre (NCSC) Minimum Security Standards:

Regulatory Status: Mandated for all New Zealand public service departments and certain Government agencies (not HNZ) that collect or hold personal information in NZ.

Authority: Self-assessment is included within the PSR self-assessment tool which provides NCSC with the assurance method for implementing the

standards. [**National Cyber Security Centre – Minimum Cyber Security Standards, 2026]**

Overview: The NCSC Minimum Cyber Security Standards define a focused set of foundational cyber security controls aligned to PSR and NZISM. They clarify minimum expectations for cyber hygiene and maturity across government agencies. The standards are mandatory for GCISO-mandated agencies and assessed through assurance and reporting mechanisms. Where services are outsourced, agencies must ensure suppliers meet equivalent minimum controls through contractual arrangements.

Health Information Standards Organisation (HISO):

Regulatory Status: Not mandated.

Authority: No certification or enforcement authority.

Overview: The HISO maintains open, non-proprietary standards for health providers and their industry partners and includes members from various health sector organisations. Their standards set requirements for the safe, secure and equity-led use of health information in New Zealand. They oversee the selection, development and adoption of data and digital standards through the health sector. HISO standards are not legally mandated by default but are widely adopted across the sector. Compliance is typically driven through policy alignment, procurement expectations, and sector stewardship rather than formal certification.

The Health Information Security Framework (HISF):

Regulatory Status: Not mandated.

Authority: No certification or enforcement authority.

Overview: The Health Information Security Framework is a sector-specific cyber security framework developed to address risks associated with health information. It defines security obligations, functional processes, segmentation, and maturity expectations, and is published in multiple parts to reflect different organisation types, including suppliers. While not legally mandated, the framework is treated as authoritative sector guidance and is aligned with NZISM and the NIST Cybersecurity Framework as well as health specific ISO frameworks. Supplier requirements are explicitly addressed and commonly enforced through contractual mechanisms.

International Standards Organisation (ISO):

Regulatory Status: Not mandated.

Authority: No direct certification authority; individual standards may support third-party certification (e.g., ISO/IEC 27001).

Overview: The ISO/IEC information-security standards provide globally recognised frameworks and guidance for establishing, implementing, and improving organisational security practices. They cover governance, risk management, technical and operational controls, and sector-specific requirements. While not legally mandated, ISO standards are widely treated as authoritative best-practice references and are frequently adopted to demonstrate due diligence, meet contractual expectations, and align with international security norms. Many jurisdictions and industries use ISO

standards to underpin policy, certification schemes, and procurement requirements.

ISO 27001, 27002 & 27799:

Regulatory Status: Not mandated.

Authority: ISO standards are voluntary; ISO/IEC 27001 may be certified by accredited bodies, while ISO/IEC 27002 and ISO 27799 provide supporting guidance and are not certifiable.

Overview:
ISO/IEC 27001, 27002, and 27799 form a cohesive suite of international standards that define best-practice information-security governance and controls. ISO/IEC 27001 establishes the requirements for implementing and operating an Information Security Management System (ISMS), including risk management, governance responsibilities, and continuous-improvement processes. ISO/IEC 27002 provides detailed guidance on the selection and implementation of security controls across organisational, people, physical, and technical domains. ISO 27799 extends these principles to the health sector, offering specialised guidance for protecting personal health information and managing security across clinical workflows, medical devices, and health-data environments.

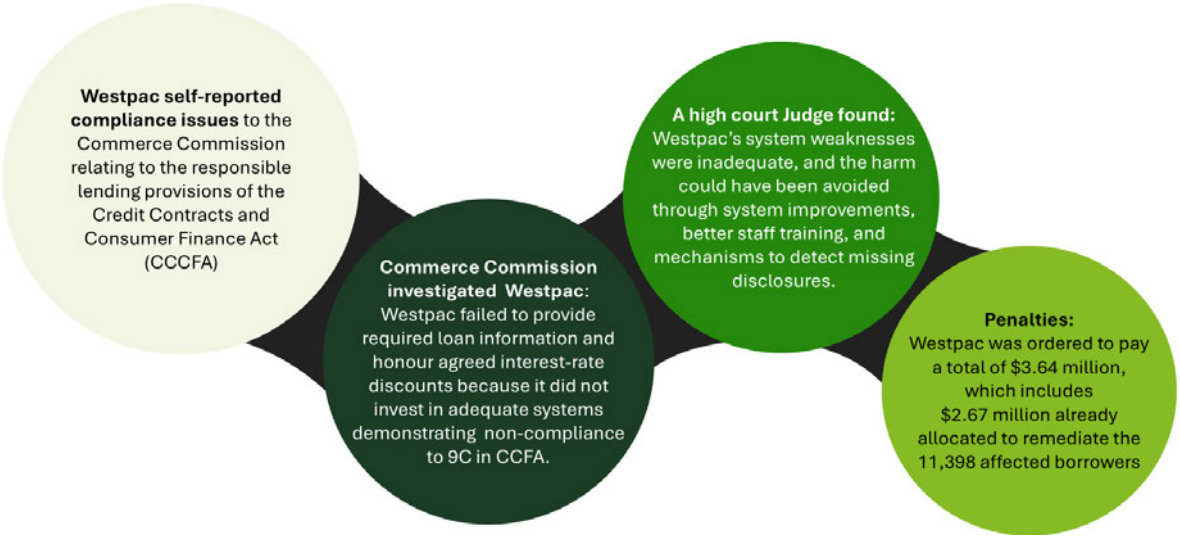
Outside of the Privacy Act 2020 there is no cybersecurity regulation, standards or policy/processes that are formally prescribed across the whole of New Zealand.

A number of the frameworks for cybersecurity and data privacy described above apply only to government, or on a sector-by-sector basis. This unevenly applied regulation leads to a fractured security landscape within the country as different sectors and agencies have varying levels of maturity.

Variation between sectors
Well-resourced, heavily regulated sectors, such as financial services, telecommunications, and critical infrastructure, typically adopt advanced security frameworks aligned with global standards. These organisations often exceed New Zealand-specific requirements because of international regulatory exposure, threat environments, and commercial risk.

By contrast, health, social services, and many parts of the public sector outside the central government mandate operate under non-mandatory frameworks (e.g., HISO standards, HISF), unclear and unenforced security expectations, legacy systems, resource constraints, and competing operational priorities.

Financial services, a case study:



What are other countries doing?
The European GDPR which is generally considered the world's leading data privacy regulation enforces maximum fines of €20 million or 4% of annual turnover with lower tier fines still reaching €10 million or 2% of annual turnover. **[EU General Data Protection Regulation, Article 83]** The Australian Privacy Act enforces 'civil penalty provisions' which apply to serious or repeated interference with privacy up to a maximum of the greater of: **[Office of the Australian Information Commissioner, Chapter 7: Civil penalties]**

- $50,000,000; or
- three times the value of the benefit obtained directly or indirectly by the body corporate and any related bodies corporate, that is reasonably attributable to the conduct constituting the contravention; or
- if the court cannot determine the value of the benefit, 30% of the body corporate's adjusted turnover during the breach turnover period for the contravention.

In October 2025 we saw a first enforcement of this following a privacy breach of Australian Clinical Labs (ACL) which resulted in the unauthorised access and exfiltration of personal health information of 223,000 individuals. The Federal Court ordered ACL to pay $5.8 million in civil penalties for various failings under the Privacy Act including failure to take reasonable steps to protect personal information. **[OAIC - Australian Clinical Labs ordered to pay penalties in relation to Medlab Pathology data breach in first for Privacy Act, 9 October 2025]**

How does HISF compare to Health Insurance Portability and Accountability Act (HIPAA)?
A key limitation of HISF is that it is not mandated and therefore not legally enforceable. HIPAA is federal law in the United States which contains security and privacy rules which mandate the minimum safeguards to protect electronic protected health information. HIPAA is legally enforceable, can result in imprisonment for wilful misuse of protected health information, and is backed by civil penalties of up to millions of USD.

While not directly comparable, as HIPAA is federal law and HISF is a best-practice framework, a comparison of these two systems highlights the possibility for legal enforcement for securing health information, and how New Zealand has not chosen to do so.

HIPAA does not offer a framework for testing or certifying compliance. HITRUST is an independent assurance framework that operationalises HIPAA and other international standards into auditable, certifiable controls, allowing organisations to certify that they are meeting legal requirements and best practices.

The HISO maintains open standards and includes members from various health sector organisations. The HISO committee is chaired by the Group Manager Data and Digital Standards at HNZ and works alongside the HNZ standards team to define the national standards for health information management. Their standards set requirements for the safe, secure and equity-led use of health information in New Zealand. They oversee the selection, development and adoption of data and digital standards through the health sector **[HISO Terms of Reference November 2025, November 2025]**.

In practice, HISO works with HNZ to define what acceptable looks like for security within the health sector of New Zealand. This includes maintaining the HISF and ensuring that this is comprehensive and fit for purpose while following international standards for health information management. **[Health Information Standards Organisation]**

HNZ's further role is to ensure they comply with HISO standards as an organisation, as HISO itself does not have any enforcement authority. This can look like aligning procurement practices and security assessments to HISF and requiring all vendors to complete a HISF self-maturity assessment. As the primary body managing health information within New Zealand, HNZ holds a key responsibility to ensure that it is advocating for fully mature privacy and cybersecurity obligations and has the opportunity to be the key driver for change in this area.

Findings

FF1. Generally, in New Zealand, cyber security and data privacy regulations and laws fall behind those of other countries. New Zealand legislation and regulation on these matters appear to reflect a less serious view of the safety of health data and the resilience of health systems as being critical to the provision of care. There is a lack of standardised and legally mandated regulations in many sectors, but specifically within health. The standards that do exist often cannot easily be assessed or formally certified against. This results in vast differences between the cyber maturity of different agencies and exposes New Zealanders' data to a high level of risk. Additionally, the privacy penalties that are currently applied through the Privacy Act are not high enough to deter insufficient protections, or encourage appropriate controls to be implemented.

Recommended actions:

F-1. HNZ to work with the Ministry of Health to define industry practice security standards that are required of organisations storing, or processing health data, or providing key digital services to health organisations. This can either be the existing HISF standards if HNZ is satisfied these provide sufficient security expectations, or another appropriate custom built or pre-existing industry standard.

F-2. Explore mechanisms to introduce mandated alignment to defined standards, and associated penalties on organisations that process or store health data (as identified above). HNZ to operationalise this with resourcing and mandate to be discussed with the Ministry.

F-3. Seek to implement a framework to assess the compliance of health organisations and vendors through regular attestation, testing and verification. Independent assurance could be provided by qualified third parties funded by digital solution providers. This will inform decision making on the vendors being used, and the level of alignment these have with the requirements.

Recommendations

In response to the review findings, eight recommendations have been identified to address the systematic industry issues, mitigate existing limitations HNZ has relevant to the MMH relationship, and reduce the likelihood of similar issues reoccurring.

The recommendations below respond to the Key Findings arising from our review, as shown below:

Recommendation	**Scope area recommended actions**					
	A	B	C	D	E	F
1. HNZ to work with the Ministry of Health to put in place independent assurance that the mandated standards for New Zealanders' health information security and privacy are being routinely met, through consistent sector-wide attestation, verification and review arrangements, with enforceable actions to remediate risks and issues.						F-1, F-2, F-3
2. HNZ to ensure it consistently applies cyber security and privacy, procurement, contracting, and third-party risk management policies and standards in all situations, and takes a proactive approach to assuring and documenting compliance with these requirements.	A-1, A-3			D-3, D-5	E-1	
3. HNZ to keep a detailed register of health information held or accessed by third parties, and the associated contracts and data retention for those services.	A-2	B-4	C-2			
4. HNZ to address remaining outstanding security and privacy items internally, and with MMH related to this incident.	A-4			D-1, D-7, D-10		
5. HNZ to perform risk assessment across its digital portfolio as part of a systemic approach to focus remediation efforts on higher-risk data, digital systems and services, and where these are identified seek to uplift capability, close gaps, address risks and verify compliance.		B-2	C-1			
6. HNZ to work with the Ministry and sector partners to enable policies such as patient or whānau notifications and consent related to storage, accessing and processing of health information to be standardised across the sector.				D-8, D-9		
7. HNZ to continue investment in growing its cyber incident response capabilities based on improvements identified throughout this review and the broader incident response.		B-1, B-3		D-4, D-6		
8. HNZ to continue working with other agencies to strengthen guidance, capabilities and capacity to manage, resource and sustain All of Government level responses.				D-2		

1. HNZ to work with the Ministry of Health to put in place independent assurance that the mandated standards for New Zealanders' health information security and privacy are being routinely met, through consistent sector-wide attestation, verification and review arrangements, with enforceable actions to remediate risks and issues

Since this report was commissioned (3 February 2026) there have been two further public examples of New Zealand digital health systems that have experienced cyber breaches. **[RNZ - Private healthcare provider IntraCare hit by cyber breach, 27 March 2026] [RNZ - MediMap hack: Pharmacists implement manual system to maintain safe care levels, 25 February 2026]**. This indicates a need for sector wide uplift in security, and signals that if things continue the belief in technology across the health sector will continue to dwindle.

It is essential for the wider health sector to establish clearly defined security and privacy requirements for digital solutions and services. This will provide a solid foundation for setting standards and ensuring the New Zealand public can have confidence in a technology-enabled health sector. At a high level, we believe this requires the establishment of mandatory standards, and a process for verification of compliance.

To achieve this, HNZ should prioritise the following recommended actions:

- **F-1. HNZ to work with the Ministry of Health to define industry practice security standards** that are required of organisations storing, or processing health data, or providing key digital services to health organisations.
- **F-2. Explore mechanisms to introduce mandated alignment to defined standards, and associated penalties on organisations that process or store health data (as identified above).** HNZ to operationalise this with resourcing and mandate to be discussed with the Ministry.
- **F-3. Seek to implement a framework to assess the compliance of health organisations and vendors** through regular attestation, testing and verification.

While we recommend that alignment to these standards is mandatory with enforceable penalties, there are many complexities to achieve this outcome. Because of this, we recommend HNZ should work with the Ministry of Health to determine the appropriate process and mechanisms for this to happen. We believe the HNZ has a key role to play as the primary body managing health information, along with independent qualified assessors who can provide confidence that standards are being met across the sector.

The adoption of a model such as the approach used by the Digital Identity Services Trust Framework should be considered, as it will support the establishment of a legal framework for delivering secure and trusted digital health services to individuals, as well as public and private organisations. **[Digital Identity Services Trust Framework, 2026]**

Implementing a framework of this type is intended to address systemic challenges within the sector, while remaining mindful of the resources and time required from individual organisations. This approach will assist digital health vendors in strengthening their security, privacy, and compliance, supporting HNZ and the broader health sector to build greater confidence in digital products and services. Ultimately, this will enhance the sector's ability to deliver a higher standard of care to New Zealanders.

2. HNZ to ensure it consistently applies cyber security and privacy, procurement, contracting, and third-party risk management policies and standards in all situations, and takes a proactive approach to assuring and documenting compliance with these requirements.

Effective third-party risk management is essential to obtaining visibility of an organisations overarching risk profile and ensuring risks are managed to an acceptable level.

To achieve this, HNZ should prioritise the following recommended actions:

- **A-1. Ensure commercial and procurement processes use risk-based measures** for activities like vendor oversight, contractual reviews and compliance checks. This is reflected in current HNZ policies and should be enforced in practice.
- **A-3. A unified service gateway** should be provided to channel all HNZ digital investments and planned procurements. This will establish a single point of entry for users which provides a streamlined path to all the required services including procurement, legal, digital services, data, privacy, and risk management.
- **D-3. Strengthen contractual governance through a risk-based tiering approach to contract clauses across HNZ's portfolio of digital services and systems.** Indicatively these should consider additional requirements related to security, privacy, information-handling, subcontracting, service management, incident reporting, rights when incidents occur, and audit and assurance rights.
- **D-5. Require evidence be provided for any assertion of security controls effectiveness and incident mitigation,** to provide confidence that controls that have been bypassed or broken during an incident can be relied upon on an ongoing basis and have not introduced additional vulnerabilities, and that root cause exposures have been remediated.
- **E-1. Define, document and follow thresholds for privacy and security reassessment activities.** This should be applied where there are significant changes to existing services, when onboarding new digital services or systems (through the unified service gateway), or on renewal/extension if privacy and security assessments have not previously been completed.

3. HNZ to keep a detailed register of health information held or accessed by third parties, and the associated contracts and data retention for those services.

Maintaining visibility of systems and services provided to HNZ is crucial in ensuring that where issues arise, HNZ can quickly triage and understand the potential impact this may have on the organisation and potential patients, along with understanding how to engage the relevant third party where needed.

To achieve this, HNZ should prioritise the following recommended actions:

- **A.2. A centralised register**, such as a contract management solution or technology asset management solution, should be used to provide a single, authoritative source of information on software/services, vendors, and contracts.
- **B.4. Record the key contact details for third-party suppliers** that support HNZ in the event of an emergency. These should be available alongside a catalogue of HNZ-provided data they have access to, and the digital services and systems they provide.
- **C-2. Continue the deployment of the Digital Services Hub** as a preferred model for secured access to health information to limit the unnecessary copying of data.

The application of these recommendations will support overarching data minimisation across HNZ and its provider landscape, and where needed will provide HNZ with the ability rapidly identify the extent of impact to HNZ where third parties experience breaches.

4. HNZ to address remaining outstanding security and privacy items internally, and with MMH related to this incident.

Through the security and privacy support activities undertaken by HNZ internally, with MMH or by third parties for HNZ, various items were identified that must be formally closed out to remove future reoccurrence of issues to HNZ and MMH. These items include:

To achieve this, HNZ should prioritise the following recommended actions:

- **A-4. Remediate MMH contract.** *(HNZ has indicated planning for this recommended action is underway.)* HNZ should work with MMH to address the gaps in the existing Enterprise License and Services Agreement. Indicatively these could include matters such as:
    - Security and privacy protection requirements
    - Reporting, including incident reporting
    - Information handling (retention, processing purposes etc).
    - Rights for HNZ under specific scenarios
    - Audit and assurance rights of HNZ
    - Service management and ongoing requirements
    - Subcontracting
- **D-1. Address outstanding findings and recommendations** from independent reviews of digital forensics and incident response and testing work so that HNZ can close any issues related to MMH. Determine and agree timings, and perform the planned HISF assessment on MMH. Where MMH is found to not align to the HISF assessment these outstanding items must be identified, tracked and monitored to ensure progress of these remediation items. *(HNZ has indicated the HISF assessment of MMH is underway.)*
- **D-7. Plan and set dates for corrective actions around removal of non-compliant data** once MMH has satisfied obligations to provide the data as part of patient notifications and responding to the OPC inquiries. *(HNZ has indicated they are working through the logistics and consequences of requesting this.)*
- **D-10. Perform validation of newly implemented data deletion and matching processes** implemented at MMH to provide full confidence that the implementation has been successful. This should include

obtaining context on the implementation of matching and deletion processes related to the screenshots provided.

These measures would provide HNZ with the ability to enforce strengthened security and privacy expectations, and to maintain visibility of risks within MMH.

5. HNZ to perform risk assessment across its digital portfolio as part of a systemic approach to focus remediation efforts on higher-risk data, digital systems and services, and where these are identified seek to uplift capability, close gaps, address risks and verify compliance.

It is essential that HNZ makes sure that there are no other high-risk systems that hold significant amounts of health information and have not undergone appropriate security or privacy assessments ever or since significant change.

To achieve this, HNZ should prioritise the following recommended actions:

- **B-2. Define the expectations of what is sufficient evidence** for security assurance of third-party solutions.
- **C-1. Perform risk assessment across HNZ's portfolio to focus efforts on higher-risk digital systems and services,** and where these are identified these must undergo targeted cyber security and privacy assessments.

HNZ should consider the need to increase internal resourcing for privacy and security to enable this activity to be performed.

6. HNZ to work with the Ministry and sector partners to enable policies such as patient or whānau notifications and consent related to storage, accessing and processing of health information to be standardised across the sector.

There were challenges in identifying those affected by this incident and in determining the most appropriate way to notify and address the underlying causes. This included difficulties with notifying individuals under 16 years of age due to uncertainties around parental consent, as well as the retention of information from the breach that had been matched to patients without registered and activated MMH accounts. There is a need to improve consistency around data retention standards and the application of consent processes across the sector.

To achieve this, HNZ should prioritise the following recommended actions:

- **D-8. Establish HNZ internal information retention standards and guidance.** This should specifically include expectations on retention of health information stored or processed by third parties providing health digital services on HNZ's behalf.
- **D-9. Set clear expectations for patient and whānau consent collection across the health sector,** specifically in relation to front line health organisations (hospitals, GPs, ACC etc) collecting data, and putting this into vendor systems. This should enable effective collection and alignment to the Privacy Act 2020. Where there is direct collection of patient data into vendor systems (such as individual uploads of additional data into the MMH Patient Portal), this must be considered within the expectations.

7. HNZ to continue investment in growing its cyber incident response capabilities based on improvements identified throughout this review and the broader incident response.

During the incident there were a range of items not performed or documented which has led to insufficient evidence of critical response actions closed. To improve the effectiveness of these activities and maintain appropriate traceability of these relevant actions continue uplift is required in HNZ's cyber and crisis response capability.

To achieve this, HNZ should prioritise the following recommended actions:

- **B-1. Ensure that harms analysis performed** as part of all HNZ incident response activities where there is potential for personal information to be impacted is used to determine appropriate activity by HNZ – such as notifications needed, additional controls required, monitoring required and support mechanisms that must be put in place – which may differ for different types of patients of data breach categories.
- **B-3. Take additional steps to ensure all critical decisions and related rationale during incidents are documented with supporting evidence,** such as HNZ system and impact assessments which has a critical bearing on the determination of incident scope and potential harm.
- **D-4. Establish key questions for each incident to guide the response, including for an AoG level response.** Questions should be established for any incident/breach that impacts HNZ directly or indirectly (e.g. through a third party).
- **D-6. Capture findings and recommendations from independent reviews of digital forensics and incident response and testing work** so that HNZ can refine security practices and apply any lessons learned from this incident to future incident responses.

8. HNZ to continue working with other agencies to strengthen guidance, capabilities and capacity to manage, resource and sustain All of Government level responses.

Due to the response being drawn out over an extended period, there was large pressure on involved HNZ (as well as MMH) response team members. This combined with the need for HNZ to lead two further AoG responses to cyber incidents following the MMH incident put further strain on individuals who were heavily relied on for the incident.

To achieve this, HNZ should prioritise the following recommended action:

- **D-2. Provide additional guidance on how lead and support agencies in a long-running All of Government level response** are managed so that the lead agency is not disproportionately resource constrained by long-running response timelines, which can impact responder wellbeing.

HNZ should consider its role within these AoG incidents and with the relevant increasing frequency of such issues increase its internal resourcing to be able to manage this workload, while also continuing to work with other health sector agencies to build capability and capacity for future responses.

Appendices

Appendix A: Acknowledgement of Interviews

Name	Role	Organisation
Details removed for privacy reasons	BAU: Group Manager Security Incident Response Response: National Controller Cyber Incident Management Team	Health New Zealand
Details removed for privacy reasons	Acting CITO	Health New Zealand
Details removed for privacy reasons	Director of Digital Applications and Products	Health New Zealand
Details removed for privacy reasons	Group Manager for Security Assurance	Health New Zealand
Details removed for privacy re	National Chief Information Security Officer (Acting)	Health New Zealand
Details removed for privacy	Group Director of Operations (GDO) Northland	Health New Zealand
Details removed for privacy reason	BAU: Programme Director MMH Recovery: National Controller Recovery	Health New Zealand
Details removed for privacy reasons	Director Living Well, (Planning, Funding, Outcomes) Primary Care	Health New Zealand
Details removed for	Privacy Officer	Health New Zealand
Details removed for privacy reasons	Chief Communications & Government Services Officer	Health New Zealand
Details removed for privacy reason	Consumer Health Portal Product Owner	Health New Zealand
Details removed for privacy r	Technology Commercial Manager	Health New Zealand
Details removed for privacy reasons	Chief Technology Officer	Manage My Health
Details removed for privacy reasons	Chief Executive Officer	Manage My Health
Details removed for privacy reasons	General Manager Strategy and Innovation	Manage My Health
Details removed for privacy reason	Executive Director	Manage My Health
Details removed for privacy reasons	Solution Architect	Manage My Health

Appendix B: List of Information Sources

Number	Document Title
1	Medtech Global media release, 3 June 2020. Retrieved 9 April 2026 from https://www.nzdoctor.co.nz/article/undoctored/medtech-global-pms-business-sold-and-manage-my-health-split-out.
2	ISGG Decision Paper, July 2021
3	MMH pilot review.docx, 2021
4	Minutes HSDC Manage My Health, November 2021
5	PIA Report (MMH) – Consumer Portal (221205), December 2022
6	Business Case (Patient Portal) v1.0 Issued.docx, 03 April 2023
7	Decision paper to Interim District Director re patient portal.pdf, 15 December 2022
8	Privacy Impact Assessment (Te Tai Tokerau Consumer Health Portal) v1.0 Issue (Signed).docx, February 2023
9	AA Manage My Health Enterprise Procrurement Agreement.pdf, March 2023
10	260106 ManageMyHealth Enterprise Licence and Service Agreement_ fully executed.pdf, March 2023
11	Te Tai Tokerau Consumer Health Portal Steering Group Meeting Minutes, 6 March 2023
12	HNZ SOW - Northland Discharge Portal Repository Onboarding.pdf, June 2023
13	RE: MMH – Top Health, 24 January 2024
14	MMH_VAPT_Retest_Report_09Feb2022 - Non-prod.pdf, 9 February 2022
15	ISRS Information - Top Health to use Manage My Health.pdf, 31 August 2023
16	TRA Manage My Health.xlsx, 16 September 2024
17	Privacy Impact Assessment Top Health, November 2023
18	SRS Report_ Top Health to use Manage My Health (ISRS 678) v1.0.pdf, 23 October 2024
19	Copy of Northern Region full CRAT v1.1.1 - ManageMy Health.xlsx, 1 November 2023
20	HNZ SOW - Northland Lab Result Repository Integration.pdf, May 2024
21	HNZ SOW - Northland eReferral.pdf, 1 July 2025
22	HNZ Transition to Recovery Plan_ MMH incident_Jan26.pdf, 21 January 2026
23	2026-01-16 - ManageMyHealth- Containment Statement – Final.pdf, 16 January 2026
24	DM7_1_Numbers of people and data impacted.pdf, 2026
25	SIMT MMH Timeline 29 Dec to 13 Jan – 24032026.pdf, 24 March 2026
26	2026-NZHC-2Injunction.pdf, 5 January 2026
27	FW_ Information for Response to Privacy Commissioner - Information Urgently Required Today.msg, 13 March 2026

28	FW ManageMyHealth Breach.msg, 30 December 2025
29	No Surprises Heads Up Manage My Health Cyber Incident.msg, 31 December 2025
30	20251231 FW_ No Surprises_ Manage My Health Breach.msg, 31 December 2025
31	RE ManageMyHealth Cyber Breach - Urgent Briefing.msg, 1 January 2026
32	Vendor name removed - MMH - Incident Response Statement - 2026-01-02.pdf, 2 January 2026
33	20260102 RE Minister's update.msg, 2 January 2026
34	Intel Report - Kazu Release Deadline 04012026.pdf, 4 January 2026
35	MMH Breach – Support pathways 08012026.pdf, 6 January 2026
36	20260109 Minister's report - 9th January.msg, 9 January 2026
37	20260111 Re_ Minister's report - 11th January.msg, 11 January 2026
38	20260112 MMH Minister's update - 12 January.msg, 12 January 2026
39	FW Request for immediate delivery of security evidence and assurance Manage My Health.msg, 12 January 2026
40	20260114 MMH Minister's update - 14 January.msg, 14 January 2026
41	FW MMH Notification Support - Introduction with Vendor name re.msg, 14 January 2026
42	20260121 FW_ MMH Minister's update - 21 January.msg, 21 January 2026
43	SG NDHB_Queries_15Jan2026.docx, 16 January 2026
44	20260118 MMH Minister's update - 18 January.msg, 18 January 2026
45	2026-01-20 - ManageMyHealth - Containment Report – Final.pdf, 20 January 2026
46	FDS- HNZ Northland Documents - Receipt, Processing & Visibilityv1.0 16-Jan-26.docx, 20 January 2026
47	ELT Briefing_MMH incident and primary care information sharing.docx, 12 February 2026
48	20260126_Minister update Jan 26.pdf, 26 January 2026
49	20260205_Minister update Feb 05.pdf, 5 Feb 2026
50	Manage My Health Data Breach - Recovery Situation Report #28.pdf, 10 February 2026
51	20260219_Minister update Feb 19.pdf, 19 February 2026
52	20260304_Minister update Mar 04.pdf, 4 March 2026
53	MMH Recovery Timeline.docx, March 2026
54	Details removed Contract.pdf, 25 November 2025
55	Procurement Policy.pdf, May 2022
56	Northland - Privacy Confidentiality Statutes and Regulations.pdf, August 2022
57	12-02-2026 Privacy Policy _ Manage My Health.pdf, 18 September 2023
58	Patient Portal Requirements, 19 November 2021
59	20260104 Minister's update - 4 January.msg, 4 January 2026
60	FW Details removed contact deets.msg, 31 December 2025
61	Re MMH Internal Review Questions (CSIRT).msg, 24 March 2026
62	Vendor nam MMH - Independent review of MMH data breach reports 110526.pdf, 11 May 2026

63	Signed_04 Mar_[redacted]_Health NZ - Primary Care Sector -Patient Portal Discovery Report.pdf, 4 March 2026
64	Health New Zealand Digital Services Hub. Retrieved 9 April 2026 from https://www.tewhatuora.govt.nz/health-services-and-programmes/digital-health/digital-services-hub.
65	Engagement Process as per National Cyber Security Home Site.pptx, 2026
66	IT Information Security Policy.pdf, 30 April 2018
67	Northern Region Cloud Cyber Security Policy.pdf, 26 April 2023
68	20260105 FW_ Minister's update - 5 January.msg, 5 January 2026
69	20260103 Minister's update MMH - 3 January 2026.msg, 3 January 2026
70	20260123_Minister update Jan 23 2026.pdf, 23 January 2026
71	MMH_Web_VAPT_Retest_Report_31_Dec_25.pdf, 31 December 2025
72	MMH_Web_Production_Security_Assurance_Report_02_Jan_26.pdf, 2 January 2026
73	[redacted] - MMH - Testing of Vulnerability - 2026-01-13.pdf, 13 January 2026
74	30012026 Manage My Health Web Application Penetration Test Report v1.0.pdf, 30 January 2026
75	MMH_Document_Display_portal_Web_VAPT_Initial_Report_07_Feb_2026.pdf, 7 February 2026
76	2026-02-10 - Manage My Health - [redacted] – FINAL.pdf, 10 February 2026
77	16022026 Manage My Health Mobile Application Penetration Retest Report v1.0.pdf, 16 February 2026
78	ELT Paper - Manage My Health - Health NZ Actions_4.15pm (002).docx, 16 January 2026
79	DM2_1_MMH-HNZ-Information-Architecture_v2.0.pdf, 19 March 2026
80	Additional data flow questions from HNZ - 2 Feb 2026.docx, 2 February 2026
81	Aide Memoire - Update on notification process - HNZ00200643 - Sent to MO 13.2.26.pdf, 12 February 2026
82	MMH - HNZ Assurance Update 10 Feb Jan.pptx, 10 February 2026
83	Manage My Health Systems & Security. Retrieved 9 April 2026 from https://managemyhealth.co.nz/security/.
84	Manage My Health Terms of Use. Retrieved 9 April 2026 from https://managemyhealth.co.nz/terms-of-use/.
85	Te Tai Tokerau Consumer Health Portal Steering Group Meeting Minutes, 5 May 2025
86	Health Information Security Framework. Retrieved 31 March 2026 from https://www.tewhatuora.govt.nz/health-services-and-programmes/cyber-hub/cyber-standards.
87	RE Vulnerability Disclosure for Manage My Health.msg, November 2025
88	Privacy Act 2020, Section 118. Retrieved 31 March 2026 from https://www.legislation.govt.nz/act/public/2020/31/en/latest/#LMS23508.
89	Human Rights Review Tribunal. Retrieved 31 March 2026 from https://www.justice.govt.nz/tribunals/human-rights/.
90	Protective Security Requirements – Roles and Responsibilities. Retrieved 31 March 2026 from https://www.protectivesecurity.govt.nz/about/roles-and-responsibilities.

91	National Cyber Security Centre – Minimum Cyber Security Standards. Retrieved 31 March 2026 from https://www.ncsc.govt.nz/protect-your-organisation/minimum-standards/.
92	OPC – *Privacy Act 2020 turns 5 – changes are needed*, 1 December 2025. Retrieved 31 March 2026 from https://www.privacy.org.nz/tuhono-connect/statements-media-releases/privacy-act-2020-turns-5-changes-are-needed/.
93	EU General Data Protection Regulation, Article 83. Retrieved 31 March 2026 from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#tit_1.
94	Office of the Australian Information Commissioner – Chapter 7: Civil penalties. Retrieved 31 March 2026 from https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-7-privacy-assessments.
95	OAIC – Australian Clinical Labs ordered to pay penalties in relation to Medlab Pathology data breach, 9 October 2025. Retrieved 9 April 2026 from https://www.oaic.gov.au/news/media-centre/australian-clinical-labs-ordered-to-pay-penalties-in-relation-to-medlab-pathology-data-breach-in-first-for-privacy-act.
96	HNZ Health Information Standards Organisation. Retrieved 31 March 2026 from https://www.healthnz.govt.nz/about-us/who-we-are/expert-groups-and-networks/expert-groups/health-information-standards-organisation.
97	RNZ - Private healthcare provider IntraCare hit by cyber breach, 27 March 2026. Retrieved 15 May 2026 from https://www.rnz.co.nz/news/national/590751/private-healthcare-provider-intracare-hit-by-cyber-breach.
98	RNZ - MediMap hack: Pharmacists implement manual system to maintain safe care levels, 25 February 2026. Retrieved 15 May 2026 from https://www.rnz.co.nz/news/national/587924/medimap-hack-pharmacists-implement-manual-system-to-maintain-safe-care-levels.
99	Digital Identity Services Trust Framework Act 2023. Retrieved 31 March 2026 from https://www.legislation.govt.nz/act/public/2023/13/en/latest/#LMS459583.
100	MMH Scenario Risk Matrix.pdf, 2026
101	20260102 initial Action plan MMH .pdf, 01 February 2026
102	Termination of Manage My Health Patient Practice Portal Agreement, 11 December 2024
103	DM6_1_MMH User Record Account Types.pdf, 22 March 2026
104	Draft Remediation Tracker Manage My Health, 21 October 2024
105	Situation Report #21 21 Jan 2026.pdf, 21 January 2026
106	national-resilience-system-handbook-may2025.pdf, May 2025

*** Note:** Hyperlinked sources have been checked and are correct as at the publication date of this report.

Appendix C: Terms of Reference

Purpose

1. A cyber breach attack on Manage My Health Limited (MMH) occurred on or around 29 December 2025. Health NZ became aware and activated a response on 30 December 2025.

2. MMH is a private company that provides an online portal that gives patients access to their own health information shared with them by their health provider or GP. Patients can email and communicate with their doctor through the MMH portal by agreement with both parties.

3. Health NZ Northland have an agreement with MMH to support the distribution of patient documents to streamline discharge processes.

4. The cyber breach has exfiltrated a large number of patient health documents, including a large number transferred to MMH by Health NZ Northland (current estimate is that c. 385,000 HNZ documents were exfiltrated). Affected patient documents may include health information about a hospital admission, together with other personal information such as the patient's name, address, NHI and medical history.

5. Health NZ has a responsibility to securely protect patient information, and it is accountable for meeting that responsibility. To date, the Ministry of Health and the Office of the Privacy Commissioner have announced inquiries into the MMH cyber breach which will include investigations into Health NZ's compliance with the Privacy Act 2020 in connection with the information that it provided to MMH and the adequacy of its response to the cyber-incident.

6. The Chief Legal Officer of Health NZ has commissioned an independent investigation by Deloitte (the Reviewer) in order to gather the information necessary to enable Health NZ's legal team (in-house and external) to respond to regulatory investigations and enforcement and any claims arising out of the MMH cyber-incident. The Reviewer will investigate how its responsibility to protect patient information has been met in relation to the Health NZ information transferred to MMH, how this cyber incident and its impact on Health NZ was responded to, to identify any shortcomings that should be addressed and any lessons learned that apply more broadly to Health NZ.

7. All information, documents, communications, records, work product, memoranda, notes, analyses, reports, findings, and materials of any kind created, obtained, prepared, or exchanged in connection with this investigation will be legally privileged.

Scope

8. The Investigation Report is expected to traverse the following areas:

a. Background: What is the nature / history of Health NZ's relationship with MMH? What service does MMH provide to HNZ that is relevant to this cyber breach and what security and privacy obligations and supporting processes are in place for that service in Health NZ and MMH? Any other context that is relevant to the Investigation Report.

b. MMH Cyber Breach: What was the timeline and the specifics of the breach and the response by Health NZ? What is Health NZ's understanding of how the cyber breach occurred including how root cause was determined; the adequacy of security and data privacy protections that were in place (to the extent that Health NZ patient information was compromised or at risk); and the impact of the breach on Health NZ services, patients and the wider sector.

c. Other Health NZ impacts: Were any other non-MMH systems or processes compromised in the cyber breach and what is the adequacy of the security and data protections that relate to those systems?

d. Incident Response: What was Health NZ's role in supporting the incident response, and how effective was the support from Health NZ to that response? How has Health NZ obtained confidence that the incident has been contained, and that the root cause and contributing factors have been identified and been mitigated? If not yet contained or mitigation actions yet to be completed, how is Health NZ supporting the response and maintaining oversight?

e. Cyber Security and Privacy: What relevant security and privacy requirements were in place by MMH in relation to HNZ information and how much involvement did HNZ have in setting these requirements? How has Health NZ assured itself that these requirements were being appropriately met by MMH both when Health NZ established the relationship with MMH and ongoing? Has Health NZ been notified by MMH of any cyber incidents or material vulnerabilities or privacy concerns prior to this incident occurring?

f. Looking beyond MMH: What regulation, standards and policy/processes apply to cybersecurity and data privacy generally in NZ? To what extent are these formally prescribed versus industry good practice? What is the role of the HISO function in Health NZ defining these and how should HNZ assure itself that these requirements are appropriately met by third party suppliers?

g. For each scope item, the Reviewer is expected to identify where Health NZ and MMH have acted appropriately, where shortcomings are identified and what remedial actions are recommended and what lessons learned should be applied more broadly by Health NZ to improve cybersecurity, data protection and privacy.

Additional information

9. The Reviewer is expected to interview and/or collect information from the following areas (full list TBC):

a. Health NZ Northland District- Details removed for privacy (GDO, Commissioning)
b. PFO Primary Care – Details removed for privacy reasons (Director Living Well, (Planning, Funding, Outcomes) Primary Care

c. Digital Services - [redacted], (CIO), and [redacted], (Head of Digital Applications and Products)
d. Cyber Security - [redacted], (CISO)
e. Privacy Officer - [redacted], (Privacy Officer)
f. Communications - [redacted], (Chief Communications & Government Services Officer)
g. Incident and Crisis Management - [redacted] (Crisis Manager/ Incident Controller) and [redacted] (Incident Controller)
h. Any other person the Reviewer considers may be able to provide relevant information such as from ManageMyHealth, Office of the Privacy Commissioner, and other parties undertaking reviews.

10. Any information the Reviewer requires will be provided by Health NZ. The initial point of contact will be [redacted], Chief Legal Officer.

11. Other than expressed above, the manner in which the investigation occurs will be totally at the prerogative of the Reviewer with a view to conducting a thorough, but expeditious investigation while complying with the principles of natural justice, good faith, and the obligation to act fairly and reasonably.

12. It is acknowledged that the scope of the review may be varied during the course of the review. Such variations could include the review being expanded to look at other specific matters if information comes to light (including through the Reviewer's investigations) that warrants further investigation or a change in phasing of the work. It is expected that as the response to the cyber breach is continuing that the review will initially focus on the aspects of the review that do not involve the response.

Deliverables

13. A draft report outlining findings and specific recommendations (if any) will be addressed to and provided to the Chief Legal Officer.

14. Once Health NZ has provided input into the Reviewer's draft report, the Reviewer will consider that input, make any changes they feel appropriate, and send the Final Report to the Chief Legal Officer.

15. Health NZ will determine how it will use the Final Report at its sole discretion.

Approach

We will perform the review over approximately 10 weeks, in four phases:

- Phase 0: Planning and mobilisation
- Phase 1: The incident and surrounding context
- Phase 2: Broader lessons learned – for Health NZ and the sector
- Phase 3: Report and refine

This timeline and approach attempts to balance the need to be expeditious with the need to be thorough, and reflects that the response is still ongoing, new facts will be coming to light, and other reviews are concurrent and may be needed to provide inputs to our review. We will be pragmatic with our review to ensure the breadth and depth of our work is appropriate, and any important insights and findings are provided promptly rather than wait for the final report to be released.

Over the course of our review we will hold weekly progress meetings with you, supported by brief one-page progress updates which we will provide in advance.

Phase 0: Planning and mobilisation (1 week)

The purpose of this phase is to successfully mobilise the review team, establish secure document sharing arrangements, request documents, and schedule interviews and working sessions over the review period.

Phase 1: The incident and surrounding context (3 weeks)

We will review materials, conduct interviews, and hold working sessions to build up an understanding of the role of ManageMyHealth, the relationship between Health NZ and MMH, the nature of the incident and its scope & extent, the information that was affected, and the details of the response. A primary activity during this period will be to document the detailed timeline of the incident, while also reviewing the contextual artefacts such as policies, procedures, contracts, standards and communications between the various parties.

It will be important for us to have access to documentation around the affected systems, security & controls, architecture and design, as-built documentation and the outputs from the cyber response and/or forensic analysis that has been conducted, for us to form a view on questions within our review scope. Where possible we will rely on work and outputs already prepared rather than repeat work that has already been done (unless this cannot be provided to us).

Where we are asked to identify other non-MMH systems or processes compromised in the incident (scope item c), we will focus primarily on directly-impacted systems and processes. If during our review there are significant indirectly-impacted systems, such as those that rely on MMH or other impacted systems to be the authoritative source of data through interfaces, or systems that use data derived from MMH or other impacted systems for critical business processes (such as enrolment, payment, or providing services) we will discuss these with you and agree how to manage scope in this context.

The outputs of this phase will be a summary of the facts primarily in relation to scope items a – e listed above.

Phase 2: Broader lessons learned – for Health NZ and the sector (3 weeks)

We will assess the facts from phase 1 in relation to the documented expectations (for example, regulation, standards, policies and processes) and with reference to industry good practice particular in relation expectations of the health sector in New Zealand.

For each scope item, we will then identify where Health NZ and MMH have acted appropriately, where shortcomings are identified and what remedial actions are recommended and what lessons learned should be applied more broadly by Health NZ (and the wider health sector) to improve cybersecurity, data protection and privacy. We will also use this phase to pick up on any clarification or refinement of the facts, or updates based on anything that has emerged as the incident and response has unfolded in parallel with our review.

The outputs of this phase will be primarily in relation to scope items f – g listed above.

Phase 3: Report and refine (3 weeks)

We will take approximately 2 weeks to complete the draft report which will be provided to you for a page-turn walk through of our insights, findings and recommendations. You will previously have had the opportunity to review the detailed timeline and summary of facts from phase 1, so this will primarily focus on the additional insights gained from phase 2 and any recommendations we make.

The outputs of this phase will be a draft review for page-turn and management responses, followed by a final report. Where possible, if earlier draft(s) can be provided to Health NZ this will facilitate review and finalisation of the report and associated findings.

Deloitte.