Briefing for information

Action plan for the 'Manage My Health Cyber Security Breach Review'

Date due to MO:	14 May 2026	**Action required by:**	N/A
Security level:	IN CONFIDENCE	**Reference:**	H2026081778
To:	Hon Simeon Brown, Minister of Health		
Consulted:	Health New Zealand: ☐		
Proactive release:	This **title** is proposed by the Ministry of Health for proactive release: ☒		

Contact for telephone discussion

Name	Position	Telephone
Celia Wellington	Deputy Director-General, Corporate Services	s 9(2)(a)
Quin Carver	Group Manager, Data and Digital Services and Chief Information Officer	

Minister's office to complete:

☐ Noted ☐ Seen

☐ Needs change ☐ Withdrawn

☐ See Minister's Notes ☐ Overtaken by events

Comment:

Briefing for information

Action plan for the 'Manage My Health Cyber Security Breach Review'

Security level:	IN CONFIDENCE	**Date:**	14 May 2026
To:	Hon Simeon Brown, Minister of Health		

Purpose of report

1. This briefing seeks your feedback on the action plan outlining the Ministry of Health's (Ministry's) implementation of the recommendations from the review into the Manage My Health cyber security breach.

Summary

2. The Ministry's review into the Manage My Health cyber security breach is nearing completion. The review was commissioned following one of the most serious cyber incidents experienced in New Zealand and has now produced a clear set of actions to strengthen the protection of personal health information and reduce the likelihood and impact of similar incidents in the future.

3. The Ministry has consolidated 26 recommendations from both phases of the review into a single, prioritised action plan (included as **appendix 1**). These actions focus on strengthening system stewardship, clarifying expectations for supplier security, improving incident preparedness and notification practices, and lifting assurance and oversight of high-risk third-party providers across the health sector.

4. Respective owners for each action are identified, and these actions have been shared with Health New Zealand and Manage My Health.

5. Early next week (week of 18 May 2026) you will receive the final public-facing report ahead of the proposed release on 21 May 2026. We will work with your office to develop communications material to support the release.

Recommendations

We recommend you:

a) **Provide** feedback on the Ministry's action plan outlining implementation of the review's recommendations as at **appendix 1**.

b) **Note** that in addition to the review into the Manage My Health cyber security breach, the Ministry is actively engaged in a number of cross-agency work programmes with the aim of improving cyber security.

Celia Wellington
Deputy Director-General
Corporate Services
Date: 14 May 2026

Hon Simeon Brown
Minister of Health
Date:

Action plan for the 'Manage My Health Cyber Security Breach Review'

Context

The review is nearing finalisation

6. A review was initiated in January 2026 following a cyber security breach of the Manage My Health (MMH) patient portal, notified to Health New Zealand (Health NZ) on 30 December 2025. The breach involved unauthorised access to sensitive clinical and personal health information at a scale that makes it one of the most serious cyber incidents experienced in New Zealand.

7. On 5 January 2026, you commissioned the Ministry to undertake a formal review. The purpose of this was to assess the causes of the incident, the adequacy of data protections, and the effectiveness of the response, and to identify actions to reduce the risk of similar incidents in the future.

8. Early in the review process, the Ministry separated the work into two distinct phases to allow urgent technical risks to be identified and acted on quickly, while still enabling a deeper, system-level assessment to follow. This approach allowed the Ministry to move at pace on immediate cyber security issues without waiting for a longer, more complex review to conclude.

9. Bastion Security Group was engaged for phase 1, with the report provided on 12 March 2026 [H2026079338 refers], and Cyber CX has conducted phase 2 on behalf of the Ministry.

10. This review is near completion, with the Ministry undertaking a final consultation process with both MMH and Health NZ to ensure there are no factual inaccuracies in the Phase 2 report and to provide them the opportunity to respond to the findings.

11. At the time of writing the Ministry has received constructive and positive feedback from Health NZ on the review report. This is being considered by CyberCX ahead of the final report being released. The Ministry has not yet received comment from Manage My Health – this is expected by Friday 15 May.

Cause of the incident and identified gaps to address

12. The MMH cyber security breach occurred through a relatively straightforward but high-impact chain of events. An attacker used stolen login credentials from a legitimate user to access the MMH portal. Once inside, they exploited a flaw in the system's Application Programming Interface (API) that allowed access to other patients' documents, enabling the large-scale extraction of sensitive data without breaching core systems.

13. The breach resulted from multiple weaknesses rather than a single failure. s 6(c)

s 6(c), s 9(2)(b)(ii)

14. At a system level, governance arrangements were also weak, with expected security standards not being consistently met, and oversight relying too heavily on self-assessment rather than independent assurance.

15. The review reflects core shifts are needed: strengthen technical controls (e.g. MFA, secure APIs, monitoring); rigorously fix known vulnerabilities through regular independent testing; and tighten system-level oversight of suppliers with stronger assurance and enforcement.

Recommendations for action

Cyber CX have outlined twelve recommendations for the health sector

16. The Phase 2 review by Cyber CX identifies 12 recommended actions to strengthen prevention of similar incidents and minimise the impact of future incidents across the health sector.

17. These recommendations call for stronger system stewardship, clearer expectations for supplier security, improved incident preparedness, and more robust assurance and oversight of high-risk third-party providers within the health sector.

18. Particular emphasis is placed on improving notification processes, enhancing assurance of high-risk suppliers, and ensuring the Health Information Security Framework is applied in practice, rather than relying on supplier self-attestation.

19. These recommendations (refer **appendix 1**) are assigned to categories based on potential to reduce overall risk, with timeframes estimated according to the expected resolution of each issue.

There are also 14 recommendations from Bastion Security's phase 1 report

20. Phase one of the review, led by Bastion Security, also issued 14 recommendations to the sector with respect to addressing the technical issues discovered in the desktop assessment. The Ministry has included these additional recommendations in the action plan and indicated how these should be addressed in the context of the phase two findings.

21. The Ministry considers that the findings of the second phase report are consistent with, and reinforce, the conclusions reached in the first phase report.

22. This therefore provides clear direction on the key issues regarding the security of health information, and the areas requiring remediation by health entities.

The Ministry has consolidated the 26 recommendations into an action plan

23. The Ministry has a key system stewardship role in responding to these findings, including setting clearer expectations for Health NZ's oversight of suppliers, seeking

assurance where risks are highest, and supporting a more consistent, sector-wide approach to third-party cyber risk management.

24. The recommendations outlined in **appendix 1** are intended to reduce the likelihood and impact of similar incidents in future, while strengthening public trust in how personal health information is safeguarded across the system.

25. To ensure clarity about what needs to happen moving forward, the Ministry has identified the proposed owner for each recommendation as well as the status and next steps. In some cases, recommendations have already been actioned or are underway with respective owners.

Reconsidering policy settings for cyber security and privacy

The Ministry continues to engage across government on cyber security

26. The Ministry is actively working with agencies across the public service to strengthen safeguards for New Zealanders' information and data, to maintain system integrity and public confidence, including measures such as enhanced enforcement and investigative powers for regulators.

Privacy Commissioner Inquiry into Manage My Health

27. The Ministry has engaged constructively with the Office of the Privacy Commissioner (OPC) throughout its inquiry into the MMH incident, providing timely information, clarifying the Ministry's system monitoring role, and supporting alignment of recommendations with existing health sector governance arrangements.

28. The Ministry agrees with the intent of the OPC's recommendation to strengthen assurance of key health sector suppliers, while clearly signalling that implementation will need to align with established roles and responsibilities, including operational assurance functions held by Health NZ.

29. The Ministry remains committed to working collaboratively with the OPC as its phase one report is finalised for 21 May and related policy work progresses.

s 9(2)(f)(iv)

s 9(2)(f)(iv)

[redacted]

In light of the cyber security breach and the review's recommendations, the Ministry is considering options to strengthen policy settings

35. The current levers available with respect to private companies are limited. Advice is underway to consider the policy, regulatory and/or legislative settings that influence the management, storage and protection of New Zealanders' health information.

36. This will include looking at the development of an accreditation framework for third parties seeking access to personal health information to supply services to the health system.

37. This advice is expected to be with your office by June 2026.

Next steps

38. The OPC is planning to release their inquiry on Thursday 21 May, and the Ministry plans to follow on the same day.

39. The Ministry is finalising the review in light of feedback from Health NZ and MMH. We expect to provide your Office with a copy of the final 'public-facing' report, with advice on the public announcement and proactive release of material in the week beginning 18 May 2026. We will also work with your office to develop communications material to support the release.

40. Progress on delivery of action will be updated through the weekly report.

ENDS

Appendix 1: Summary of Review Recommendations and Ministry of Health's Action Plan

CyberCX / Bastion	Review Reference	Recommendation	Owner	Rating / Timeframe	Action & Next Steps
Complete (3 recommendations)					
Bastion	B09	Advise s 6(c), s 9(2)(b)(ii) of the series of security vulnerabilities passively observed by Bastion within their respective patient portals.	MoH	High / Within 2 months	Complete MoH met with each of the providers and engaged Bastion to share their findings from the desktop assessment of vulnerabilities.
Bastion	B02	Recommend s 6(c), s 9(2)(b)(ii) investigate and remediate exposed s 6(c), s MMH credentials identified within Bastion's research.	MoH / MMH	High / Within 6 months	Complete MoH met and briefed MMH 18 March 2026 on this recommendation. MMH committed to address this, and MoH will complete follow up testing after 6 months.
Bastion	B01	Undertake an independent secure design practice and source code review of s 6(c), s 9(2)(b)(ii) MMH Application and API(s).	HNZ	Medium / 6–12 months	Complete Addressed by actioning REC12.
Actioned (5 recommendations)					
CyberCX	REC03	HNZ to seek further clarification of any critical services provided to MMH by third-party suppliers, to ascertain the nature of the contract in place, and patient data accessible to third-party suppliers.	HNZ	High / Within 3 months	Actioned MoH briefed HNZ on 7 May 2026 and supplied a copy of the review. MoH to seek assurance the recommendation has been completed by August 2026.

Bastion	B14	Require patient portal providers to uplift incident response capabilities and practices.	HNZ	Medium / 6–12 months	Actioned Addressed by the action taken in REC01 below in meeting with HNZ, .
CyberCX	REC12	HNZ to seek assurances from Manage My Health (MMH) of the data management practices, aligned to HISF requirements and best practice, including details of user onboarding and offboarding processes, data retention periods, data access audit methodologies and whether patient data is accessible to any of MMH suppliers or related parties.	HNZ	Medium / 6–12 months	Actioned MoH met with Health NZ on 6 May 2026 to describe this finding. Requested that HNZ seeks the assurance from MMH as the contracted supplier of services.
CyberCX	REC01	HNZ to undertake regular tabletop incident response exercises with critical suppliers that hold sensitive health data, to practice and better define incident roles and responsibilities and ensure alignment across the sector.	HNZ	Medium / 6–12 months	Actioned MoH briefed HNZ on 7 May 2026 and supplied a copy of the review. MoH regularly monitor Health NZ's progress with regular tabletop incident exercises and ensure this is 'business as usual' by 2027.
CyberCX	REC05	HNZ to develop a plan to engage with the sector to drive better third-party security assurance outcomes across the health sector, in line with HISO and HISF requirements.	HNZ	Low / 12–24 months	Actioned MoH briefed HNZ on 7 May 2026 and supplied a copy of the review. MoH will regularly seek assurance that HNZ is regularly engaging with the sector.

Underway (12 recommendations)					
CyberCX	REC04	HNZ to comprehensively review and uplift its third-party risk management practices in-line with recommendations in the s 6(c), s 9(2)(b)(ii)	HNZ	High / 6-12 months	Underway A comprehensive review of Health NZ third-party risk management practices is underway by Health NZ's internal Cyber Security teams. MoH to seek assurance the recommendation is well underway by November 2026, and complete by May 2027.
CyberCX	REC09	The Ministry (MoH) as the health system monitor, defines thresholds and attributes for 'high-risk' suppliers to the health sector; and regularly receives assurance from entities that hold contracts with 'high-risk' third-party suppliers regarding their security status and HISF compliance.	MoH	Medium / 6–12 months	Underway Policy advice underway, with first briefing due to the Minister of Health in June 2026.
Bastion	B10	Develop and implement a companion high impact systems security assurance monitoring regime.	MoH	Medium / 6–12 months	Underway Aligned to REC09. Policy advice underway, with first briefing due to the Minister of Health in June 2026.
Bastion	B03	Require greater cyber security governance, supplier oversight, and incident-response capability maturity across all patient portal providers.	MoH	Medium / 6–12 months	Underway Addressed by work proposed in response to REC09 above.
Bastion	B06	Introduce a continuous security assurance monitoring programme to oversee all patient portal providers.			

Bastion	B07	Mandate the uplift of credential hygiene across all patient portal service providers.			
Bastion	B08	Mandate the treatment of patient portal credential exposure as a high-impact security event.			
Bastion	B11	Require all patient portal providers to implement platform-wide remediation of any identified access control weaknesses.			
Bastion	B12	Require the strict control of any Internet-exposed non-production environments associated with any patient portal.			
Bastion	B13	Require all patient portal providers to implement detection and alerting capabilities for abnormal API behaviour and bulk downloads.			
CyberCX	REC10	MMH to undertake further security reviews (penetration tests) and/or purple/red team activity on the MMH web and mobile applications. The results of this review should be shared with HNZ.	MMH	High / Within 3 months	Underway MoH briefed MMH (8 May 2026) on the review findings and formally requested that further security reviews and penetration tests are performed.
CyberCX	REC11	MMH to undertake a full external assessment of HISF compliance by a provider conversant with the HISF framework. The output of this should be provided to HNZ as a contract holder and MoH as the health system monitor.	MMH	High / Within 3 months	Underway MoH briefed MMH (8 May 2026) on the review findings and formally requested that a full external assessment of HISF compliance is undertaken.

Planned (6 recommendations)					
CyberCX	REC06	MoH, in their role as health system monitor, write to HNZ (and other contract holders) to confirm how they manage HISF compliance and what actions have been taken in cases of non-compliance.	HNZ	High / Within 6 months	Planned MoH will write to HNZ to formally request that this action is completed along with a summary report of the outcome by November 2026.
CyberCX	REC07	HNZ to consider measures to strengthen HISF compliance among suppliers to the health sector, in particular suppliers that hold sensitive health information.	HNZ	High / Within 6 months	Planned MoH will write to HNZ to formally request that this action is completed, with a report back to MoH by November 2026. We understand this is underway, HNZ has developed an information sharing security awareness campaign with sector engagement to commence in early June.
CyberCX	REC02	MoH and HNZ to better define process and procedures for patient notifications in the event of data breach involving data held by a third-party supplier, with defined roles and responsibilities set.	HNZ / MoH	High / Within 6 months	Planned MoH to request HNZ's documented notification process for review and feedback.
Bastion	B04	Require all digital health service providers to comply with HISO 10029.4:2025 and regularly produce evidence to verify this compliance.	HNZ	High / Within 6 months	Planned Will be actioned through MoH activity outlined in REC06 above.
Bastion	B05	Update and reissue HISO 10029.4:2025 to now formally designate digital healthcare service delivery platforms (patient portals and practice management systems) as high impact systems requiring mandatory implementation of specified privacy and security controls.	HNZ	High / Within 6 months	Planned Addressed by work proposed in response to REC07 above.

CyberCX	REC08	HNZ and other health sector entities to maintain registers of their suppliers that store or process sensitive health information, tiered by risk factors (including volume of records, sensitivity, criticality to care delivery).	HNZ	Medium / 6–12 months	Planned MoH as monitor to engage health sector entities in August 2026 and outline this request, seeking assurance it has been completed within 12 months. Health NZ will define a standardised approach for identifying, recording and monitoring registers of those digital suppliers that store, hold, or process sensitive health information.