Briefing for decision

Public release of 'Manage My Health' cyber security breach review

Date due to MO:	21 May 2026	**Action required by:**	27 May 2026
Security level:	IN CONFIDENCE	**Reference:**	H2026082779
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☐ Needs change ☐ Withdrawn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 decision

Public release of 'Manage My Health' cyber security breach review

Security level:	IN CONFIDENCE	**Date:**	21 May 2026
To:	Hon Simeon Brown, Minister of Health		

Purpose of report

1. This briefing provides you with the public-facing review into the 'Manage My Health' cyber security breach and seeks your agreement to release this in alignment with the Privacy Commissioner's inquiry on Wednesday 27 May 2026 (tentative). It also provides you with a draft letter to your Cabinet colleagues sharing the final report.

2. Attached are:

   a. Appendix 1: Manage My Health cyber security breach review – public release
   b. Appendix 2: Draft letter from Hon Simeon Brown to Cabinet colleagues
   c. Appendix 3: Draft letter from Acting Director-General of Health to colleagues
   d. Appendix 4: Ministry of Health's Action Plan: Responding to the Manage My Health Review Recommendations
   e. Appendix 5: Manage My Health cyber security breach review – fulsome version (not for further distribution)

Summary

3. Recent incidents across both the public and private sectors have reinforced that cyber security is no longer solely an information technology issue, but a core component of system resilience, public trust, and service continuity. For sectors such as health, where large volumes of sensitive personal information are held and shared across complex delivery arrangements, cyber risk has become an issue requiring whole-of-system action.

4. The Manage My Health breach is one of the most serious cyber security events experienced in New Zealand. The breach was not caused by a single mistake, but by a combination of gaps in system security, monitoring, and oversight over time. This independent review undertaken by the Ministry of Health sits within a broader cross-government programme of work responding to the increasing scale, sophistication and impact of cyber security threats facing New Zealand.

5. The findings of the review, conducted by Cyber CX, reinforce the need for stronger cyber governance, assurance and accountability settings across the health sector and its third-party suppliers. The review issues 12 recommendations in response to the breach which, along with the findings, will be released publicly on Wednesday 27 May 2026.

6. The Ministry is intending to proactively release supporting documentation to the review at the same time the review findings are released. We are working with your office on this [H2026082779 refers].

7. Taken together, this review and the Government's broader cyber security work programme underscore the urgency of moving from reactive responses to a more proactive, risk-based approach that recognises cyber security as essential to protecting individuals, maintaining public confidence, and enabling the safe delivery of public services in an increasingly digital environment.

Recommendations

We recommend you:

a)	**Note** the Privacy Commissioner will be releasing their independent inquiry into the Manage My Health incident first on Wednesday 27 May 2026.	**Noted**
b)	**Agree** to the public release of the Manage My Health cyber security breach review on Wednesday 27 May 2026, following publication of the Privacy Commissioner's independent inquiry.	**Yes / No**
c)	**Write** to your Cabinet colleagues confirming the completion of the review and inform them of the upcoming public release.	**Yes / No**
d)	**Note** the fulsome report reviewing the 'Manage My Health' cyber security breach prepared by CyberCX is also attached as appendix 5. This is not recommended for public release.	**Noted**
e)	**Note** that the Ministry will work with your Office regarding the public release of the review and proactive release of the supporting information ahead of Wednesday 27 May 2026.	**Noted**

Celia Wellington
Deputy Director-General
Corporate Services
Date: 21 May 2026

Hon Simeon Brown
Minister of Health
Date:

Public release of 'Manage My Health' cyber security breach review

Context

A review commenced in January 2026 in response to a cyber security breach of Manage My Health patient portal

8. On 30 December 2025, Health New Zealand (Health NZ) was notified of a cyber security breach affecting the patient portal, Manage My Health. The incident resulted in unauthorised access to clinical documents and personal health information from across New Zealand. The scale and sensitivity of the data involved make this one of the most serious cyber security incidents experienced in New Zealand.

9. On 5 January 2026, you commissioned the Ministry to undertake a formal review to assess the causes of the incident, the adequacy of data protections, the effectiveness of the response, and to identify improvements to prevent similar incidents.

10. Phase one of the review commenced on 29 January 2026 and was completed by Bastion Security Group on 11 March 2026 and shared with you for information [H2026079338 refers].

11. The findings from the technical, passive assessment undertaken in phase one revealed systematic weaknesses in security capability, governance and operational maturity within Manage My Health and more broadly, across the sector. The Ministry undertook urgent action to address the most critical privacy and security risks, as outlined in previous advice to you [H2026080142 refers].

Specialist consultant, CyberCX, has completed phase two of the review

12. The purpose of this phase was to undertake a more comprehensive assessment of actions taken pre, during and post incident, informed by interviews and documentation.

13. Phase two included a series of in-person interviews with affected parties, including Manage My Health leadership, the National Cyber Security Centre, Health NZ, Ministry of Health and the New Zealand Police. This review also incorporated the phase one technical report completed by Bastion Security Group as an input to the final review.

14. The independent review was commissioned by the Ministry to provide assurance by:

    a. assessing the cause(s) of the incident,
    b. reviewing the adequacy of the data protections that were in place,
    c. examining the response to the incident, and
    d. recommending any improvements required to prevent similar incidents occurring.

15. The review was completed by 30 April 2026, with consultation and finalisation of the report completed in the weeks following. The Ministry considers that the terms of reference have been met as outlined above.

Ministry's review of Manage My Health's cyber security breach

Assessment, findings and themes

The final report has outlined a number of critical findings

16. The findings can be thematically grouped into key focus areas including,

    a. the scale and sensitivity of the incident
    b. preventable security control failures as root cause
    c. pre-incident systemic weakness in security governance and assurance
    d. challenges in incident scoping, coordination and communication, and
    e. exposure of broader health-sector third party risks management gaps.

17. The reviewers concluded that Manage My Health's weaknesses in cyber security controls and governance contributed significantly to this data breach. While steps have since been taken to strengthen protections, the incident highlights the need for stronger oversight of third-party suppliers and more consistent cyber security practices across the health sector.

18. The reviewers also observed that although Health Information Standards Organisation (HISO) and the Health Information Security Framework (HISF) provide guidance for organisations that handle health information, they currently lack enforcement mechanisms. Improving assurance, accountability, and patient communication is critical to reducing future risk in the collection, storage, access and management of health data.

19. The report concludes that this incident should serve as a 'call to action' for the health sector and New Zealand organisations more broadly, to improve cyber security controls and governance.

Recommendations for action

20. The review has issued 12 recommendations for action by the Ministry, Health NZ and Manage My Health. These are aimed at both preventing similar such incidents and minimising the impact of future breaches within the health sector.

21. The final recommendations are outlined in the report (refer to appendix 1) and have been assigned ratings and timeframes. Ratings are assigned based on potential for the action to reduce risk, and timeframes are estimated on when each recommendation should be completed.

22. Phase one of the Ministry's review, led by Bastion Security, also issued a further 14 recommendations to the sector with respect to addressing the technical issues discovered in the desktop assessment. A number of these were urgently addressed, prior to phase two, given the necessity to remediate these issues [H2026080142 refers]. All 26 actions are included in the Ministry's action plan as referenced in recent advice [H2026081778 refers].

23. As noted, the Ministry considers that the findings of the second phase report are consistent with the conclusions reached in the first phase report, therefore providing clear direction on the key issues regarding the security of health information.

Consultation with affected entities

Meeting with agencies to discuss the finding and recommendations

24. The Ministry met with both Health NZ and Manage My Health executives the week of 4 May 2026, to discuss the findings of the review, the recommendations for action and next steps.

25. The report was provided on 6 May 2026 to both entities to ensure procedural fairness and uphold the principles of natural justice by providing them the opportunity to comment on any adverse findings before the report is finalised. Following the meetings with entities the Ministry asked that they review the report and provide any comment on factual inaccuracies by Wednesday 13 May. This would then be considered prior to the final report being issued.

26. Health NZ and Manage My Health have provided constructive feedback on the review which has been incorporated, where appropriate, by CyberCX.

Next steps

Public release of the summary report

27. The Ministry recognises there is a strong public interest in transparency and accountability in relation to the Manage My Health cyber security incident, given the scale of the breach and the sensitivity of the information involved.

28. The Ministry considers that the countervailing public interest in releasing the full report is appropriately addressed through the proactive release of a public-facing version and other key documents surrounding the review process.

29. The fulsome report contains information provided specifically for the review, which if released in full, could reasonably be expected to prejudice the commercial position of third parties, and the security of health information. Some of the information provided to the review by the entities is also subject to an obligation of confidence and some withheld to protect the maintenance of the law.

30. The Ministry recommends that the fulsome report continues to be withheld, if requested under the OIA, at this stage.

31. Therefore, the Ministry will release a public-facing, summary version as the final report on Wednesday 27 May 2026 [refer appendix 1]. Further information has been provided to your office on the documentation to be proactively released alongside the report [H2026082779 refers].

32. The Ministry has also provided your office with a communications plan and potential press release for consideration. This release will conclude the Ministry's formal review and share the report and link to proactively release information on our website.

Informing government of the review

33. The Ministry recommends you share a copy of the review (under embargo) with your Cabinet colleagues ahead of the public release. A draft letter for your consideration is attached as appendix 2.

34. Similarly, the Acting Director-General of Health will also share an embargoed copy with her colleagues that have either been engaged through the review, or their expertise consulted during the development of the terms of reference. This is included as appendix 3 for your visibility. These agencies include the Public Service Commission, Department of Internal Affairs, Office of the Privacy Commissioner, Government Communications Security Bureau, National Cyber Security Centre, Health New Zealand, Ministry of Justice and the New Zealand Police.

Upcoming advice

35. As a result of the review findings, the Ministry is considering the current levers available with respect to private companies. Advice is underway to consider the policy, regulatory and/or legislative settings that influence the management, storage and protection of New Zealanders' health information. 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. You can expect to receive initial advice on this in June 2026.

ENDS.

Appendix 1: Manage My Health cyber security breach review – public release version **Publicly available via the general Manage My Health release page (see Document 11)**

Appendix 2: Draft letter from Hon Simeon Brown, Minister of Health to Cabinet colleagues Attached and released in full

Appendix 3: Draft letter from Acting Director-General of Health to colleagues **Attached and released in full**

Appendix 4: Ministry of Health's Action Plan: Responding to the Manage My Health Review Recommendations Attached and released with some information withheld under 6(c), 9(2)(b)(ii), and 9(2)(ba)(i) of the OIA

Appendix 5: Manage My Health cyber security breach review – fulsome version (not for further distribution) **Withheld in full under 6(c), 9(2)(b)(ii), and 9(2)(ba)(i) of the OIA**

Hon Simeon Brown

Minister of Health
Minister for Energy
Minister for State Owned Enterprises

Appendix 2: Draft letter from Hon Simeon Brown, Minister of Health to Cabinet colleagues

26 May 2026

Dear Cabinet colleagues

Manage My Health Cyber Security Breach Review

I am writing to inform you that the Ministry of Health's (the Ministry) independent review into the 'Manage My Health' (MMH) cyber security breach is now complete.

Earlier this year I commissioned a review of MMH and Health New Zealand's (Health NZ) response to this incident. I am pleased to share with you a copy of the public report (Appendix 1), which outlines the findings and recommendations of the review. [Note this report is embargoed until 5:00 a.m. on Wednesday 27 May 2026.]

The review examined the circumstances of the breach, the underlying causes, and the system and governance settings that contributed to it. It confirms that the incident resulted from a combination of security weaknesses and inadequate oversight over time, rather than a single failure. The review sets out a clear set of actions to strengthen system security, clarify accountability, improve assurance arrangements, and ensure faster detection and response to cyber incidents.

Recent incidents across both the public and private sectors have reinforced that cyber security is no longer solely an information technology issue, but a core component of system resilience, public trust, and service continuity. For sectors such as health, where large volumes of sensitive personal information are held and shared by a range of entities across complex delivery arrangements, cyber risk has become a material issue that requires co-ordinated, whole-of-system action.

Work is already underway with the Ministry, Health NZ and MMH to address these recommendations, including improvements to technical controls, governance, and ongoing independent assurance (refer to Appendix 2). Health agencies will continue to work with system leads, namely the Ministry of Justice and the Public Service Commission, to support a whole-of-government response to the breach.

Private Bag 18041, Parliament Buildings, Wellington 6160, New Zealand | +64 4 817 6804 | s.brown@ministers.govt.nz

The review report and supporting materials will be proactively released to support transparency and public confidence, as well as a copy of the review report that Health NZ commissioned Deloitte to complete (Appendix 3).

I will keep Cabinet informed of progress as these actions are implemented and as further system-wide improvements are delivered.

Yours sincerely

Hon Simeon Brown
Minister of Health

Appendix 1: Manage My Health Cyber Security Review Phase 2

Appendix 2: Ministry of Health's Action Plan: Responding to the Manage My Health Review Recommendations

Appendix 3: Health NZ Manage My Health Cyber Breach Review

MINISTRY OF HEALTH
MANATŪ HAUORA

Appendix 3: Draft letter from Acting Director-General of Health to colleagues

133 Molesworth Street
PO Box 5013
Wellington 6140
New Zealand
T+64 4 496 2000

26 May 2026

Sir Brian Roche KNZM, Public Service Commissioner
Paul James, Secretary for Internal Affairs, Government Chief Digital Officer
Michael Webster, Privacy Commissioner
Andrew Clark, Director-General Government Communications Security Bureau & Government Chief Information Security Officer, National Cyber Security Centre
Dr Dale Bramley, Chief Executive Health New Zealand
Andrew Kibblewhite, Secretary for Justice
Richard Chambers, Commissioner of Police

Dear colleagues,

Final Report, *Manage My Health Cyber Security Breach Review*

I am writing to update you on the Ministry of Health's (the Ministry's) review into the 'Manage My Health' cyber security breach commissioned by Hon Simeon Brown, Minister of Health earlier this year.

The Ministry sought your engagement in early January 2026 on a 'terms of reference' to guide this review. I am pleased to provide you with a copy of the final public facing report, prepared on behalf of the Ministry by CyberCX. Please note this is embargoed until 5:00AM Wednesday 27 May 2026.

This review has:

- assessed the cause of the incident,
- reviewed the adequacy of the data protections that were in place at the time of the incident,
- reviewed the response of both Manage My Health (MMH) and Health New Zealand (Health NZ) and identified 12 recommendations to prevent similar incidents occurring in the future.

Recent incidents across both the public and private sectors have reinforced that cyber security is no longer solely an information technology issue, but a core component of system resilience, public trust, and service continuity. For sectors such as health, where large volumes of sensitive personal information are held and shared across complex delivery arrangements, cyber risk has become a material issue that requires coordinated, whole-of-system action.

As part of the wider cross-agency work programme on cyber security, the Ministry will leverage the health review findings to support cyber security improvements for the wider government digital system. We may be in touch with your respective agencies as we progress the health sector aspects of this work.

If you have any questions, please do not hesitate to contact my senior management lead, Celia Wellington, Deputy Director-General Corporate Services, or myself directly.

Yours sincerely,

Ruth Isaac
Acting Director-General of Health
Ministry of Health

CC: Hon Simeon Brown, Minister of Health
Celia Wellington, Deputy Director-General, Corporate Services

Appendix 1: 'Public Report - Manage My Health Cyber Security Breach Review'

Appendix 2: Ministry of Health's Action Plan: Responding to the Manage My Health Review Recommendations

Ministry of Health's Action Plan

Responding to the Manage My Health Review Recommendations

As of 20 May 2025

Note: Identifying information relating to the vendor and the report has been redacted to protect commercially sensitive information and information supplied in confidence. If requested under the Official Information Act 1982, the following provisions will apply: sections 9(2)(b)(ii) and 9(2)(ba)(i).

CyberCX / Bastion	Review Reference	Recommendation	Owner	Rating / Timeframe	Action & Next Steps
Complete (3 recommendations)					
Bastion	B09	Advise [**vendors]** 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 [**vendor]** investigate and remediate exposed [**vendor]** and 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 **[vendor]** 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 **[report]**.	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.	MoH	Medium / 6-12 months	Underway Addressed by work proposed in response to REC09 above.
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.