Briefing for information

Preliminary actions post phase one 'Manage My Health' review

Date due to MO:	19 March 2026	**Action required by:**	N/A
Security level:	SENSITIVE	**Reference:**	H2026080142
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, Digital and Information Services	

Minister's office to complete:

☐ Noted ☐ Seen

☐ Needs change ☐ Withdrawn

☐ See Minister's Notes ☐ Overtaken by events

Comment:

Briefing for information

Preliminary actions post phase one 'Manage My Health' review

Security level:	SENSITIVE	**Date:**	19 March 2026
To:	Hon Simeon Brown, Minister of Health		

Purpose of report

1. This briefing updates you on progress with the 'Manage My Health' review (the review) led by the Ministry of Health (the Ministry).
2. Attached are:
    a. **Appendix 1:** Phase One Recommendations and Actions
    b. **Appendix 2:** Letters sent from Celia Wellington to Manage My Health (MMH) and other primary care providers requesting meetings to discuss initial findings from phase 1 of the review
    c. **Appendix 3:** Passive Assessment Brief(s) prepared by Bastion for MMH
    d. **Appendix 4:** MMH Response to Bastion Security Review Findings – External Working Document, 17-03-2026
3. Officials will be able to discuss this further with you at the meeting scheduled for Monday 23 March 2026.

Summary

4. Phase one of the Manage My Health review, completed on 11 March 2026, identified significant cyber security vulnerabilities through a passive desktop and open-source intelligence assessment of MMH and other commonly used patient portals.
5. The findings revealed systemic weaknesses in security capability, governance and operational maturity across the sector, raising concerns about the protection of highly sensitive personal and health information. Bastion's report made 14 recommendations, all of which the Ministry has accepted, and urgent action has already been taken to address the most critical privacy and security risks.
6. The Ministry has engaged directly with MMH and other patient portal providers to ensure awareness of the findings and to encourage remediation, while commissioning CyberCX to undertake a more detailed phase two review, due in May 2026. This work, alongside the Office of the Privacy Commissioner's investigation and wider cross-government cyber security initiatives, will inform consideration of the Ministry's system leadership role and whether further policy or legislative changes are required.

Recommendations

We recommend you:

a)	**Note** that since receiving the final report completing phase 1 of the Manage My Health Review, the Ministry has been engaging with primary care portals to address cyber security vulnerabilities.	**Noted**
b)	**Note** that the Ministry has engaged Bastion Security Group advise portal providers on the actions required to address vulnerabilities, and perform future validation.	**Noted**
c)	**Note** officials will update you following discussions with Manage My Health Chief Executive and Health New Zealand (HNZ) on Monday 23 March 2026.	**Noted**

Celia Wellington
Deputy Director-General
Corporate Services
Date: 19 March 2026

Hon Simeon Brown
Minister of Health
Date:

Preliminary actions post phase one 'Manage My Health' review

Context

The Ministry provided the final phase one report to you on 11 March 2026

7. Phase one of the Manage My Health review (the review) was completed on Wednesday 11 March, at which point the Ministry shared the report with you for your information (H2026079338 refers). This briefing also follows on from information discussed with you and your office on Friday 13 March 2026.

Phase one was a passive desktop review of technical documentation

8. Phase one reviewed the technical documentation provided by MMH and Health NZ and involved Bastion undertaking open-source intelligence to collect and analyse publicly available information.

9. This approach used structured, non-intrusive techniques to map MMH's external digital footprint, including domains, infrastructure references, publicly accessible systems, corporate disclosures and other information intentionally or unintentionally exposed to the public internet.

10. This also included a similar scan of open-source intelligence for some of the other commonly used patient portals in primary care. s 9(2)(g)(i), s 9(2)(b)(ii), s 6(c)

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

Final report from Bastion outlined 14 recommendations to address the vulnerabilities found in their research

12. As noted in the final report (appendix 2 of H2026079338 refers) Bastion's review of the cyber security ecosystems led to the issuing of a number of recommendations.

13. The Ministry has engaged CyberCX to undertake phase two of the review; in part to validate these observations further to ensure any final recommendations are necessary, targeted and effective. However, given the findings to date, the Ministry is clear that urgent action is required now.

Addressing the recommendations from phase one of the review

The Ministry is concerned by the vulnerabilities exposed by Bastion across the patient portals examined in the review

14. The phase one review exposed a lack of cyber security capability, governance and operational maturity that would have been expected of a national-scale digital health service delivery platform handling highly sensitive and personal information.

15. In addition, some of the findings for MMH were found across other commonly used patient portals in New Zealand. In the context of increasing complexity and reliance on digital services, the Ministry has an obligation as system lead to step into the health data ecosystem to ensure patients can trust that their information is protected.

16. However, it should also be noted that there are limited government levers to enforce change or require actions to be taken. New Zealand's patient portal market is general practice led – a private organisation contracting with another.

The Ministry has accepted all 14 recommendations and is progressing actions required for each one, either directly or commissioning other entities

17. Outlined in the table at **Appendix 1** are each of the recommendations, the assigned entity lead, the action(s) required, and the timeframe or next steps needed.

18. A number of the recommendations are dependent on the conclusion of either the Ministry's phase two review and/or the OPC investigation. Importantly, the Ministry has taken swift action to address the most concerning matters that have implications for data privacy, s 6(c)

In response to the review findings the Ministry is meeting with portal providers

19. The intent of these meetings is to ensure a shared understanding of the observations, and the corrective actions each organisation should take to stabilise the security of their platform.

20. Detailed policy work will be required to understand the role and expectations of patient portals and consider how they operate with government in their handling of personal and health information. This will need to be informed by the findings of phase two of the review, and the conclusions of the Office of the Privacy Commissioner's Inquiry.

MMH are actively working to address the issues outlined in the Bastion report and are engaging with officials to ensure findings are considered

21. On Wednesday 18 March officials, including Celia Wellington (SRO) and Quin Carver (SME), met with representatives from MMH s 9(2)(ba)(i) This relates to recommendation number two, as noted in **Appendix 1.**

22. This was a productive engagement in which Bastion briefed MMH on their findings from the passive review of their patient portal system. They were receptive to the findings and keen to improve their practice. MMH provided a document in which they respond to each of recommendations (attached as **Appendix 4**). The Ministry was clear this engagement was to inform and share findings, and it would be for the company to address any vulnerabilities as best they see fit.

23. We will be asking Bastion to repeat their open-source intelligence within 90 days, to understand if the suggestions provided to each patient portal entity, were acted upon. This will be a validation exercise and not include broader testing. Under current system settings this sits outside the Ministry's mandate in relation to private organisations.

s *additional patient portals were reviewed by Bastion to understand the maturity of the national network of providers*

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

25. This letter (example of which is attached as **Appendix 2**) informs of the desktop review findings and seeks a meeting with them and Bastion, to discuss the vulnerabilities discovered. These meetings will be held the week of 23 March 2026.

Cross-Government Workstream to improve cyber security

s 9(2)(g)(i), s 9(2)(f)(iv)

27. Recent incidents such as the Manage My Health and MediMap breaches were not the result of sophisticated cyber-attacks but of basic security controls not being applied. As noted by the NCSC, both incidents could likely have been prevented had fundamental measures such as multifactor authentication been in place, consistent with the NCSC's Essential Controls and standard government practices outlined in frameworks like the New Zealand Information Security Manual (NZISM).

28. Instead, some digital health products have been built and operated at minimal cost, with insufficient investment in secure-by-design principles and low awareness or adoption of established government best-practice controls. This highlights the need for stronger incentives, clearer expectations, and more consistent assurance across third-party platforms handling personal information across government.

Phase two update

CyberCX is underway progressing phase two of the review

Final report from phase 2 is due in May 2026

29. As noted previously (H2026079338 refers) the purpose of this is to undertake a more comprehensive assessment informed by interviews and documentation. This final report will outline the root cause analysis, an assessment of the adequacy of the response, and actionable recommendations to prevent future breaches. We expect this report to be a critical input into both the health and wider government sectors.

30. Following receipt of the final report from CyberCX, the Ministry will need to review the findings and recommendations to determine the actions required by us and the wider sector.

The MMH breach, in conjunction with other recent cyber incidents, have questioned the role of government in the management of personal information held by private organisations

31. Consideration will need to be given to the policy and legislative settings that influence accountability in the management and contracting of data and digital services. Whilst the Ministry has at present limited levers to influence the procurement of services between two private providers (general practices and patient portal providers), there is an element of system leadership, accountability and public expectation to safeguard public information.

32. The Ministry will continue to update you as this policy work is considered in light of the reviews including the Ministry's, Health NZ's, OPC's, review of the Privacy Act 2020 and cross-government enhancement of cyber security practices.

Next steps

33. Officials will discuss the recommendations and the Ministry's actions in more detail with you at the meeting on Monday 23 March.

34. The Ministry will also continue to work with Bastion on informing providers following phase one of the review. Concurrently, phase two will progress with CyberCX, noting interviews are currently underway with those involved from MMH and Health NZ. We will update you regularly as this proceeds.

ENDS.

Appendix 1: Phase One Recommendations and Actions

No.	Recommendation	Proposed Owner	Action required	Next steps / timeframe
1	Undertake an independent secure design practice and source code review of s 6(c), s 9(2)(b)(ii) MMH Application and API(s).	MMH	Ministry to advise MMH of this recommendation.	Awaiting phase 2 completion – it is likely additional findings and actions will be recommended for MMH to action.
2	Recommend s 6(c), s 9(2)(b)(ii) investigate and remediate exposed s 6(c), and MMH credentials identified within Bastion's research.	Ministry of Health	Provide Bastion's findings to s 6(c), s 9(2)(b)(ii) with the expectation of addressing the vulnerabilities within 90 days.	Part 1 - Completed. Ministry met with MMH on 18 March 2026 to inform them of findings. Part 2 – Ministry has commissioned Bastion to repeat their open-source intelligence review to confirm vulnerabilities are closed by 18 June 2026.
3	Require greater cyber security governance, supplier oversight, and incident-response capability maturity across all patient portal providers.	Ministry of Health	Await OPC report and findings for system wide implications and recommendations.	The OPC investigation commenced 28 January 2026, with phase 1 expected by 30 April 2026. The scope and timing of phase 2 is yet to be confirmed.
4	Require all digital health service providers to comply with HISO (Health Information Standards Organisation) 10029.4:2025 and regularly produce evidence to verify this compliance.	Health NZ	Set expectations with all purchasers of digital services to request evidence at the next contract renew cycle.	Health NZ and the Ministry jointly wrote to all providers on 2 March 2026 setting this expectation. The Ministry to consider what advice is needed regarding monitoring and/or regulatory levers to require and validate evidence of compliance.

5	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.	Ministry of Health / Health NZ	Ministry to request HNZ to review HISO and provide advice regarding levers to mandate compliance and levers to direct all holders of health records to formally advise of their compliance.	Ministry to request Health NZ by 30 March 2026, response and assessment by 30 April 2026.
6	Introduce a continuous security assurance monitoring programme to oversee all patient portal providers.	Ministry of Health / Health NZ	s 6(c), s 9(2)(f)(iv)	Await the outcome of the cross-government work programme.
7	Mandate the uplift of credential hygiene across all patient portal service providers.	To be determined by the policy advice (refer recommendations 4 & 5)	Mandate required via HISO designation change.	As per actions 4 & 5, Ministry to request that Health NZ review Health Information Security Framework (HISF).
8	Mandate the treatment of patient portal credential exposure as a high-impact security event.	To be determined by the policy advice (refer recommendations 4 & 5)	Mandate required via HISO designation change.	As per actions 4 & 5, Ministry to request that Health NZ review HISF.
9	Advise s 6(c), s 9(2)(b)(ii) of the series of security vulnerabilities passively observed by Bastion within their respective patient portals.	Ministry of Health	Ministry to meet with each provider to discuss the findings of Bastion's review.	Ministry met with MMH 18 March. Ministry has written to the other s primary care provider portals referred to in Bastion's report and sought meetings the week beginning 23 March 2026.

10	Develop and implement a companion "high impact" systems security assurance monitoring regime.	Ministry of Health	Ministry to determine a 'monitor' for this regime.	Following actions taken for recommendations 4, 5 & 6, Ministry advice will examine remaining gaps to inform mandate and assurance options.
11	Require all patient portal providers to implement platform wide remediation of any identified access control weaknesses.	Ministry of Health	Ministry to await policy advice requiring mandates on private organisations.	Following actions taken for recommendations 4, 5 & 6, Ministry advice will examine remaining gaps to inform mandate and assurance options. In addition, the outcome from the OPC investigation be considered.
12	Require the strict control of any Internet-exposed non-production environments associated with any patient portal.	Ministry of Health / Health NZ	Further direction subject to recommendations 4 and 5.	Dependent on system settings and policy advice referred to in recommendations 4 and 5.
13	Require all patient portal providers to implement detection and alerting capabilities for abnormal API behaviour and bulk downloads.	Ministry of Health / Health NZ	Further direction subject to recommendations 4 and 5.	Dependent on system settings and policy advice referred to in recommendations 4 and 5.
14	Require patient portal providers to uplift incident response capabilities and practices.	Ministry of Health / Health NZ	Further direction subject to recommendations 4 and 5.	Dependent on system settings and policy advice referred to in recommendation 4 and 5.

Appendix 2: Letters sent from Celia Wellington to Manage My Health (MMH) and other primary care providers requesting meetings to discuss initial findings from phase 1 of the review

Appendix 3: Passive Assessment Brief(s) prepared by Bastion for MMH

Appendix 4: MMH Response to Bastion Security Review Findings – External Working Document, 17-03-2026

Note: Appendix 3 and Appendix 4 withheld in entirety under sections 6(c), 9(2)(b)(ii), and 9(2)(ba)(i) of the OIA

MINISTRY OF HEALTH
MANATŪ HAUORA

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

18 March 2026

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

Ministry of Health Cyber Security Review

As you will be aware, the Manage My Health patient portal system in New Zealand was recently subject to a cyber security breach compromising patient privacy and trust in the system.

On 4 January 2026, the Minister of Health, Hon Simeon Brown asked the Ministry of Health to commission an independent review of the incident. A 'Terms of Reference was issued, scoping the purpose and timing of this review. Further details can be found here https://www.health.govt.nz/strategies-initiatives/programmes-and-initiatives/manage-my-health-data-breach.

As part of this review, we commissioned an exploration of whether vulnerabilities found in Manage My Health are present across other patient portals. The Ministry of Health has now received the phase one report from Bastion Security Group, and we would like to discuss the findings with you. Some of these may require urgent action from you.

I would like to formally invite you to a meeting during the week beginning 23 March 2026 with representatives from Bastion Security Group and Ministry of Health officials. At this engagement, the reviewers from Bastion Security Group will provide an overview of the key findings, methodology and identified themes in relation to , your patient portal system.

The intent of our meeting will be to ensure a shared understanding of the observations, and the corrective actions your organisation should take to stabilise the security of your platform for all New Zealand patients.

Please let us know your availability as soon as possible, and who from your organisation should also attend. If you have any questions or concerns, please contact me directly either via email or on s 9(2)(a)

Yours sincerely,

Celia Wellington
Deputy Director-General of Health
Corporate Services
Ministry of Health

CC: Hon Simeon Brown, Minister of Health
Audrey Sonerson, Director-General of Health
Dr Dale Bramley, Chief Executive, Health New Zealand

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