Briefing for information

Manage My Health interim review and next steps

Date due to MO:	11 March 2026	**Action required by:**	N/A
Security level:	SENSITIVE	**Reference:**	H2026079338
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	

Minister's office to complete:

☐ Noted ☐ Seen

☐ Needs change ☐ Withdrawn

☐ See Minister's Notes ☐ Overtaken by events

Comment:

Briefing for information

Manage My Health interim review and next steps

Security level:	SENSITIVE	**Date:**	11 March 2026
To:	Hon Simeon Brown, Minister of Health		

Purpose of report

1. This briefing provides you with a copy of the interim review of the Manage My Health (MMH) Cyber Security Breach (attached as **appendix 2**) and updates you on the Ministry of Health's (Ministry's) next steps.

2. Attached are:

   a. **Appendix 1:** Terms of Reference – Ministry of Health Review of the Manage My Health Cyber Security Incident 22 January 2026

   b. **Appendix 2:** *Manage My Health Cyber Security Review* report prepared by Bastion Security Group (Bastion)

   c. **Appendix 3:** Letter from Sir Brian Roche (22 January 2026) and response from the Ministry of Health (3 February 2026)

3. Officials will discuss the findings and recommendations of phase one with you at the meeting scheduled for Monday 16 March 2026.

Summary

4. Bastion has completed the phase one report of the MMH Cyber Security Breach review, s 9(2)(g)(i)

5. The interim report contains key findings and 14 specific recommendations and will be used as a key artefact to inform phase two. Phase two will increase the scope of the overall review from a purely desktop exercise to a more comprehensive assessment. Ultimately the aim is to prevent similar breaches occurring in the future.

6. The final report is expected in May 2026, at which time officials will provide you advice on implementing the proposed recommendations and next steps.

Recommendations

We recommend you:

a) **Note** the interim review has been completed by Bastion Security Group on behalf of the Ministry of Health and is attached for your information. **Noted**

b) **Note** phase two of the review of the MMH cyber security breach has commenced, with CyberCX engaged to act on behalf of the Ministry. The final report is due in May 2026. **Noted**

c) **Note** officials will discuss the findings of the phase one report and give an update on phase two with you at the meeting scheduled for 16 March 2026. **Noted**

Celia Wellington
Deputy Director-General
Corporate Services
Date: 11 March 2026

Hon Simeon Brown
Minister of Health
Date:

Manage My Health interim review and next steps

Context

Manage My Health was subject to a cyber security data breach compromising patient privacy and trust in the system

7. On 30 December 2025 Health New Zealand (Health NZ) was notified of a cyber security breach of the patient portal system Manage My Health, owned by Cereus Health Group. This incident resulted in authorised access to the clinical documents and personal health information of over 120,000 individuals across New Zealand.

8. On 4 January 2026, you commissioned the Ministry to undertake a formal review of the incident. A 'Terms of Reference' (**Appendix 1** refers) scoped the review with the purpose of assessing the cause(s) of the incident, reviewing the adequacy of the data protections and the response to the incident. Ultimately the review will recommend any improvements that may be required to prevent similar incidents occurring in the future.

Phase One of the Review

Bastion has provided their final report completing phase one of the review

A desktop review of technical documentation was undertaken for phase one

9. The purpose of phasing into two parts allowed the Ministry to begin the review whilst the response to the incident by MMH and Health NZ was ongoing. This protected those involved, allowing them to focus on protecting New Zealanders' information.

10. Bastion was engaged by the Ministry to undertake this 'desktop' review of the technical cyber security and patient portal landscape in which the breach occurred. They assessed MMH against the security controls prescribed within the 'HISO 10029: 2022 Health Information Security Framework (HISF)' using available documentation, publicly known incident details and open-source intelligence gathering.

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)

The review recommends 14 actions to address the immediate risks associated with MMH and remediate data weakness across the system

13. Overall, the Ministry is comfortable and broadly agrees with the recommendations provided by Bastion. Of the 14 recommendations, two are specific to MMH, whilst the remaining recommend changes at the system level to uplift the necessary assurance and oversight.

14. The recommendations are a combination of both technical and generalist actions. For example, the technical actions, recommend requiring controls and certain capabilities specific to good data management practice. Whilst others, such as the requirement for 'greater cyber security governance, supplier oversight and incident-response maturity,' seek to improve the cyber security system.

15. A full list of the recommendations in the phase 1 report are included on page 6 of **Appendix 2**.

Phase Two of the Review

This phase of the review has commenced and the expected timeframe for a final report is May 2026

16. As of Monday 2 March 2026, the Ministry has engaged CyberCX (a specialist cyber security consultancy) to undertake a comprehensive assessment informed by interviews and documentation. CyberCX will outline the root cause analysis, an assessment of the adequacy of the response, and actionable recommendations to prevent future breaches.

17. For this phase to successfully draw accurate, evidence-based conclusions, full cooperation is required by all parties involved in the breach. Audrey Sonerson, Director-General of Health, wrote to Dr Dale Bramley, Chief Executive Health New Zealand and Vino Ramayah, Chief Executive MMH, outlining government's expectations and next steps for the review (2 March 2026).

Wider government response to the cyber security breach

Safeguarding the integrity of public information and data

18. In response to the breach, the Public Service Commission undertook a stocktake of all government departments, their crown entities and wider supply chains, to seek assurance on the integrity of public information they hold.

19. The Ministry responded outlining the arrangements for managing, protecting and overseeing personal information (**Appendix 3**). This also included an initial assessment of the data handling processes and protections in place within the monitored health Crown entities.

s 9(2)(g)(i)

21. We will continue to work with the Public Service Commission, the Government Chief Digital Officer (GCDO) and the National Cyber Security Centre, as government considers its role in overseeing all public information held by private entities across New Zealand.

Next steps

The Ministry will provide advice on all recommendations at the conclusion of the review

22. The Ministry will provide fulsome advice on the full suite of recommendations issued following completion of phase two in May 2026.

23. Advice will outline the key findings and actions required for the sector and provide advice on the ownership, feasibility and timing of each recommendation including, if required, any options for your consideration.

24. Public release of the review findings will not occur until the final report is completed in May. However, the interim report will be provided to the Office of the Privacy Commissioner to inform their own statutory inquiry underway under section 17(1)(i) of the Privacy Act 2020.

ENDS

Appendix 1: Terms of Reference – Ministry of Health Review of the *Manage My Health Cyber Security Incident 22 January 2026*

Appendix 2: Final Report – *Manage My Health Cyber Security Review* prepared by Bastion Security Group

Appendix 3: Letter from Sir Brian Roche (22 January 2026) and response from the Ministry of Health (3 February 2026)

Notes:

Appendix 1: Publicly available via www.health.govt.nz/system/files/2026-01/manage-my-health-review-terms-of-reference.pdf

Appendix 2: Withheld in full under section 6(c), 9(2)(b)(ii), and 9(2)(ba)(i) of the Act

Appendix 3a: Letter from Sir Brian Roche (22 January 2026) is publicly available via www.publicservice.govt.nz/assets/DirectoryFile/Letter-to-Public-Service-CEs-Safeguarding-the-integrity-of-public-information-and-data_.pdf

Appendix 3b: Response from the Ministry of Health (3 February 2026), attached and released in part

Appendix 3b: Letter from the Ministry of Health

MINISTRY OF HEALTH
MANATŪ HAUORA

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

3 March 2026

Sir Brian Roche KNZM
Te Tumu Whakarae mo Te Kawa Mataaho
Public Service Commissioner | Head of Service

Dear Sir Brian

Safeguarding the integrity of public information and data in the health system

Thank you for your letter dated 22 January 2026, requesting confirmation of the Ministry of Health's (the Ministry) arrangements for managing personal information across the wider health supply chain. Your correspondence follows the recent 'Manage My Health' (MMH) data breach and reflects your expectation that government agencies safeguard the integrity of public information held across the sector.

Ministry of Health response to data breach

Earlier this year, the Hon Simeon Brown, Minister of Health, commissioned the Ministry to lead a review of the MMH data breach. This review will assess the adequacy of the data protections that were in place at the time of the incident, the responses of both MMH and Health New Zealand (Health NZ), and identify any recommendations to prevent similar incidents occurring. I can confirm this work is underway, with the phase one interim report due in the next fortnight.

Lifting public assurance

I acknowledge your comments regarding the need to lift the level of assurance public sector agencies have in the integrity of how people's personal information and data are managed. This not only includes information collected, processed or shared directly by agencies, but extends to those third-party providers across the wider health system whose practices and controls have a direct impact on public trust and outcomes.

Notwithstanding the outcome of the Ministry's review into MMH and the independent inquiry by the Privacy Commissioner, the Ministry has limited oversight and few levers to influence the management of health information and patient data across the breadth of the health sector. I strongly support the view that further work is required to review and strengthen the current policy and operational settings. I look forward to working with Paul James and public sector colleagues on this matter.

Response to your request

As requested, I have attached information pertaining to your request. This outlines the Ministry's arrangements for managing, protecting and overseeing personal information, and provides my initial assessment of how these are handled by third parties across the health sector. We have collected information from the Crown entities we monitor and, based on the responses received, assessed the level of risk. Please note that this information has not been independently verified, nor has any deeper analysis been undertaken at this stage.

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

Yours sincerely,

Audrey Sonerson
Director-General of Health
Ministry of Health

MINISTRY OF HEALTH
MANATŪ HAUORA

Appendix 1: Information Request
Arrangements for managing personal information across the health supply chain

Ministry of Health's collection and management of information

Summary
Overall, our assessment indicates s 9(2)(g)(i) in the Ministry's arrangements for managing, protecting and overseeing personal information and data, both internally and through the third-party suppliers contracted by the Ministry.

Assessment
We have conducted a preliminary assessment of information held by third-party suppliers that provide specialist services to identify how information is collected, held and the controls put in place during the procurement process. This assessment included both suppliers who deliver a digital service to the Ministry (e.g. SaaS/PaaS, Assisted Dying Service), and third parties who are contracted to perform an operational function (e.g. The New Zealand Institute for Public Health and Forensic Science, various 'health committees'). We have also reviewed the 'terms and conditions' in the Ministry's standard contracts to confirm they meet information security requirements.

Findings
We have two key findings from our internal assurance exercise:

1. In review of the Ministry's outsourced services (both digital and operational delivery aspects), s 9(2)(g)(i) in the arrangements and controls we have in place to manage personal information.

2. A number of digital systems that collect personal information are 'owned' by the Ministry but are hosted on Health NZ platforms. Whilst the Ministry has full accountability, it has limited control over the settings, management and control processes.

Next Steps
We are reviewing the Ministry's contract management, procurement practices and general information services to ensure adequate controls are in place to mitigate any risks of data breaches involving information collected by the Ministry or its third-party suppliers.

Crown entities' collection and management of information

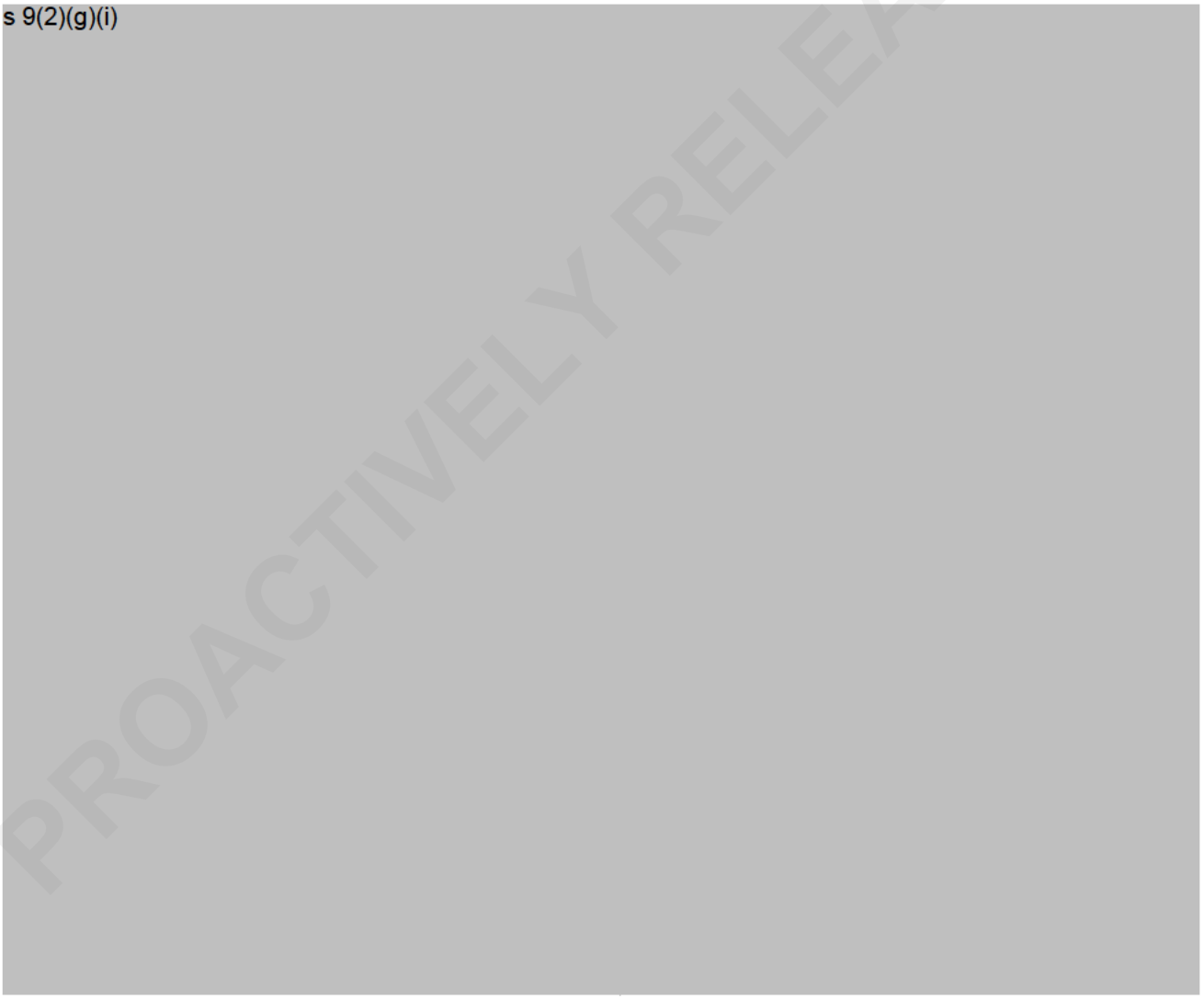
Summary
Across the Crown entities within our sector for which we are responsible, our level of confidence is mixed and varies by agency. Many of the smaller entities have a narrow remit and manage limited amounts of personal health information. s 9(2)(g)(i), s 6(c)

Assessment
The Ministry wrote to all health sector Crown entities regarding the importance of trust as a foundation of the public service future digital strategy and operating model. As part of this, we requested a high-level self-assessment and summary of each entity's arrangements for collecting and managing personal information, both internally and through third-party providers.

It should be noted that the Ministry's interim assessment is based solely on the information provided by the Crown entities and has not been independently verified.

Findings
There are seven health Crown entities monitored by the Ministry, each performing a distinct role within the health system. Arrangements differ widely based on the entity; some with a limited role in personal information, others with an extensive remit.

s 9(2)(g)(i)



[1] Confidence rating is given through the Ministry's initial assessment of the agency's arrangements for managing, protecting and overseeing personal information and data, and arrangements for data held by third parties across the supply chain. This rating is informed by the information provided by each agency and has not been validated.

Health Sector

The health sector includes a wide and diverse range of providers, from government agencies to non-governmental organisations, public and private hospitals, general practices, physiotherapists, aged residential care, dentists, opticians, naturopaths and many more. The Ministry has limited visibility and few levers for how personal information and data are managed across this wide range of providers.

Any decision to increase the assurance and controls over personal and health related information, will require a strengthening of current policy and operational settings governing how third parties collect, manage and protect this data s 9(2)(g)(i) [redacted]

Conclusion

This assessment identifies a generally sound foundation within the Ministry and parts of the Crown entity group but also highlights material risks, s 9(2)(g)(i), s 9(2)(b)(ii), s 6(c) [redacted]

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