5.2 Operational issues

5.2.1 Update on Ministry review – ManageMyHealth cyber security breach [Sensitive]

This item provides an update on the Ministry's review, which you commissioned into the ManageMyHealth (MMH) cyber security breach.

Background

On Monday 5 January 2026, you commissioned a Ministry led review of MMH's and Health NZ's handling of the cyber security incident, to commence no later than Friday 30 January 2026. The review focuses on understanding the cause of the breach, the adequacy of protections in place, and the effectiveness of the incident response. The scope and Terms of Reference were developed in consultation with the Government Chief Digital Officer and the National Cyber Security Centre and are published on the Ministry's website.

Update

Bastion Security Group has been engaged to deliver Phase one of the review, which commenced on Thursday 29 January 2026. An interim report is due on Friday 27 February 2026.

Phase one will assess MMH's capability to operate a critical health platform, compare its published security standards with actual practice, and consider relevant frameworks such as the Health Information Security Framework. It will analyse incident response material, conduct a passive technical review of the MMH portal, and provide a high-level scan of risks across other patient portals.

The Ministry has requested specific information from Health NZ and MMH, which was provided during the week commencing Monday 2 February 2026.

Next steps

Planning for Phase two procurement is underway, noting that Phase one findings will inform Phase two.

Ministry lead	Celia Wellington, Deputy Director-General Corporate Services, s 9(2)(a)

5.2 Operational issues

5.2.1 Update on Ministry review – ManageMyHealth cyber security breach [Sensitive]

This item provides a further update on the Ministry's review into the ManageMyHealth (MMH) cyber security breach. This follows the previous update provided to you in early February 2026 [Weekly Report for the week beginning Monday 9 February 2026, item 5.2.1 refers].

Initially the interim report from Bastion Security Group (Bastion) was due to the Ministry on Friday 27 February 2026. We now expect the interim report no later than Friday 13 March 2026. Primarily this is because both Health NZ and MMH continue to operate in a 'response mode' to address the impacts of the breach. Delays in information being provided by MMH has meant that Bastion has not had timely access to the documentation required to undertake a fulsome analysis and provide their opinion. It is important that phase one is thorough, as this will inform the scope of phase two.

Next steps

You can expect to receive an update following receipt of the interim report of the phase one review. Additionally, procurement for phase two commenced last week (Wednesday18 February 2026). We will update you further on scope, deliverables and expected timeframes, when phase two is underway.

Ministry lead	Celia Wellington, Deputy Director-General Corporate Services, s 9(2)(a)

MINISTRY OF HEALTH
MANATŪ HAUORA

1 Ministerial priorities

1.1 Progress with the Manage My Health review [Sensitive]

Context

This item updates you on the Ministry of Health's (the Ministry's) progress with the review into the Manage My Health (MMH) cyber security breach. This follows previous written updates to you in the weekly reports of 9 and 23 February and briefings of 11 and 19 March [weekly reports for the weeks beginning Monday 9 and 23 February 2026 refer, and items 5.2.1 refer, and briefings H2026079338 and H2026080142 refer].

Actions following phase one review

As you will be aware, the initial phase one report from Bastion Security Group (Bastion) recommended 14 actions in response to the findings of systemic weakness in security capability in the patient portal sector. Following receipt of this report, the Ministry has undertaken urgent action to address the most critical privacy and security risks [H2026080142 refers].

The Ministry has engaged directly with the other patient portal providers referred to by Bastion in its 'desktop analysis' of the sector. s 9(2)(ba)(i) These meetings were positive, and each provider was interested to understand the specific vulnerabilities detected and undertake corrective action.

Additionally, some providers shared their experiences and concerns with the current policy and operational settings in place. For example, they too were concerned that without accreditation/standards (or something similar), practices will continue to look for the lowest cost option available on the market, compromising the protection of personal information.

Progress with phase two review

CyberCX is on track with progressing the phase two review and final report into the breach. At present, it is undertaking a number of key stakeholder interviews and will be meeting with the Ministry to share initial insights. This remains on track for final delivery in May 2026.

Improving government policy settings to protect personal information

In response to the recent health sector data breaches, cross-government workstreams have been initiated to better protect New Zealanders personal information. s 9(2)(ba)(i), s 9(2)(f)(iv)

Next steps

The Ministry has requested Bastion repeat its open-source intelligence scans against the MMH service within 90 days (by Tuesday 9 June 2026) with the purpose of understanding if the recommended corrective actions were addressed. We will update you following this validation exercise.

The final report from CyberCX remains due in May 2026. We will provide you a copy once finalised, and any advice on next steps.

Contact	Celia Wellington, Deputy Director-General Corporate Services, s 9(2)(a)