Privacy Commissioner
Te Mana Mātāpono Matatapu

Inquiry into the cybersecurity breach affecting the Manage My Health Limited patient portal

Phase one report

25 May 2026

Executive Summary

The breach and this inquiry

1. On 1 January 2026, Manage My Health Limited ("MMH") notified the Office of the Privacy Commissioner ("OPC") that threat actors ("hackers") had managed to steal large amounts of health information from MMH's patient health portal. Subsequent investigations found that valid stolen patient credentials had been used by the hackers to enter the portal. Those credentials were then used to access and copy documents from thousands of other patients' accounts.

2. Information in the MMH portals is stored in various separate sections. Only one of those sections was compromised (the "My Health Documents" module), but 99,416 patients were affected (revised down from the initial estimates of 126,000). This makes it one of New Zealand's largest known breaches of sensitive personal information, and it has caused serious distress to many affected patients.

3. Around 91% of affected patients appear to have been in Northland. This was the result of a unique agreement between the Northland District Health Board (now Health New Zealand) and MMH to make certain types of Northland hospital records available to patients through the MMH portal. This project started in around 2019, was piloted in 2021 and was more widely rolled out between 2023 and 2025.

4. Given the seriousness and the scale of the breach, the Privacy Commissioner publicly announced an inquiry on 21 January 2026 and issued terms of reference on 27 January 2026. The inquiry is being conducted under section 17(1)(i) of the Privacy Act 2020. The inquiry is in two phases.

5. This report covers **Phase 1**. It looks at whether MMH and Health New Zealand ("Health NZ") had adequate security safeguards in place to protect health information in the patient portal, as required by Rule 5 of the Health Information

Privacy Code 2020 ("the Code"). It also comments on the security safeguards that general practices are expected to have in place when they engage health portal providers to communicate with their patients.

The value of patient health portals

6. The Ministry of Health has long recognised the value of patient health portals as part of its digital health strategy. As reflected in the 2017/2018 report by the Office of the Auditor General, the Ministry has actively encouraged the take-up of patient portals in the health sector. Health portals have also had the support of general practitioner organisations including the Royal New Zealand College of General Practitioners, as they are a practical and efficient way to provide patient services and information.

7. This inquiry is not a signal that OPC is opposed to patient portals. On the contrary, done well, we consider that these tools can enhance privacy by providing better access for patients to their own information and better control over that information. They can also improve efficiency in the health sector.

8. However, to achieve those benefits, it is essential that patient health portals are secure, and that patients can trust them to operate in a privacy-protective way.

Overall findings

9. Our inquiry has concluded that both MMH and Health NZ failed in their responsibilities to have reasonable security safeguards in place and therefore that they breached Rule 5 of the Code.

Findings about Manage My Health

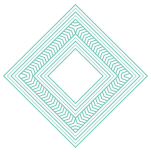
10. MMH's entire business focuses on handling and storing sensitive health information in a secure and trustworthy way. As a result, while it is a small

company, Rule 5 of the Code still requires it to have very strong technical and operational security safeguards in place.

11. We have concluded that this security breach was not the result of a single failure. Instead, it involved a combination of factors. If those safeguards had been operating more effectively at the time of the incident, it would have been less likely that the breach would occur at all, and the impact would have been reduced.

12. In particular:

- Multifactor authentication was available within the platform but was not required for all users. It was only an optional feature.
- Web security controls were in place but were not sufficiently effective.
- Identity and access management controls were also in place but not sufficiently effective. A valid but stolen patient account was able to be used to access and extract information relating to thousands of other patients.
- Earlier testing had revealed recurring themes relating to access control and application security risks. While the precise sequence of events may not have been specifically anticipated, the themes identified by the testing were not adequately addressed at the time of the breach.
- We had concerns about whether some security testing and assurance activities were sufficiently effective to identify and mitigate the relevant risks prior to the incident.
- There were deficiencies in the company's data leak protection settings and in its ability to detect incidents and take action to intervene. MMH's own systems did not detect the presence and actions of the hackers: it first became aware of the problem when it was alerted by Health NZ.



- While risk management processes existed at the time of the incident, they were not sufficient to ensure that safeguards relating to health information were working.

13. MMH has informed us that it has already taken steps to address these deficiencies and that the platform is secure. The steps that MMH states that it has taken include requiring multifactor authentication for all users and fixing the particular vulnerability that the hackers used. It is also taking steps to update its contracts and policies, and to boost its governance arrangements. However, we have not yet independently validated that the changes address all the issues raised by this inquiry, or that the stated controls are in place and operating effectively.

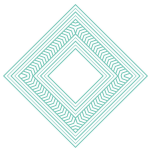
14. We therefore intend to issue MMH with a compliance notice under section 123 of the Privacy Act. This notice would direct the company to take steps to ensure that the deficiencies identified in Phase 1 of this inquiry are addressed, and to demonstrate that it now complies with Rule 5(1)(a) of the Code.

Findings about Health NZ

15. The decision by Health NZ in Northland to routinely send certain hospital-related documentation to patients through MMH's health portal resulted in large amounts of sensitive information being stored in patient accounts that would not otherwise have been there. Health NZ also actively encouraged and supported patients and their GP practices to sign up to MMH so that they could receive their hospital documents.

16. It is clear that Health NZ was trying to improve patient services as well as improve efficiency for the hospital. This was a novel – and potentially precedent-setting – digital project.

17. The novelty and scale of the project created very strong obligations on Health NZ to ensure that patient information would be properly protected. While it did

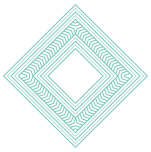


not have direct visibility of or control over MMH's technical security settings, Health NZ needed to meet very strong standards for due diligence, contract drafting, governance, risk management and ongoing assurance.

18. We have concluded that Health NZ did not always do so and that these failures amounted to a breach of Rule 5(1)(b) of the Health Information Privacy Code.

19. In particular:

- Health NZ did not conduct sufficient due diligence over MMH before it decided to engage the company as its design partner and supplier. The result may have been the same, since MMH was an obvious partner for the project, but decision makers would have been better informed.
- There were serious problems with the quality of the privacy risk assessments, though things improved somewhat in the later stages of the project.
- The way in which the MMH system would manage the hospital information was insufficiently understood and key technical issues were not identified.
- The Health NZ project team appear to have relied too much on the security and privacy of information provided by MMH, rather than taking a more independent view.
- While there was an active project steering group, with senior leadership, that group did not include direct privacy or security representation as would be expected for a project of this novelty, complexity and scale.
- There was also no evidence that the project team received advice from internal privacy or security specialists early enough to properly inform the design of the project (though Health NZ were unable to contact many former staff to check this).



- The contracts between Health NZ and MMH were not fit for purpose and did not contain appropriate protections for patient information.

20. These findings are likely to be largely historic in nature. Health NZ has informed us that a variety of changes have been made, including developing updated digital services contract templates, and making improvements to privacy and security assessment processes with the support of expert central privacy and cyber security teams. However, information from Northland hospitals is still shared with patients through their MMH accounts and Health NZ is still funding licence fees for GP practices to use MMH.

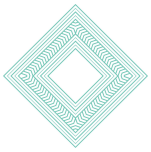
21. We therefore intend to issue a compliance notice to Health NZ under section 123 of the Privacy Act. This notice would direct Health NZ to take steps to ensure that the deficiencies identified in Phase 1 of this inquiry are addressed, and to demonstrate that it now complies with Rule 5(1)(b) of the Code.

Recommendations about general practitioners

22. All information in the My Health Documents module was either placed there by patients themselves, consisted of hospital records that were part of the Health NZ arrangement with MMH, or were copies of referral letters that MMH (not GP practices) had decided to store in that area of the patient portal. Put simply, MMH was not acting on behalf of GP practices when it stored any of that information in the My Health Documents module. GP practices had no control over those arrangements. Nor did GPs have access to the information stored in My Health Documents.

23. As it happens, therefore, we consider that it is unlikely that GP practices were legally responsible for the security of the specific information that was stolen in this cyber security breach.

24. However, in our opinion, it is largely a question of luck that the breach did not involve information for which GP practices were responsible. It is essential that



GP practices are aware that they still have obligations under Rule 5 of the Code to have reasonable security safeguards in place when engaging a patient health portal service provider such as MMH.

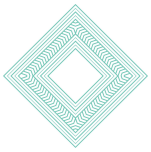
25. It is not possible for this inquiry to review what steps each individual GP practice has or has not taken. There are thousands of general practices in New Zealand, and there will be significant variability in whether they engaged MMH at all, what they contracted MMH to do, what information was stored in the portal, and what patients were told.

26. Instead, we have set out our general expectations for the reasonable security safeguards that GP practices should have in place when engaging a patient health portal. Those expectations will provide a framework for assessing any future complaints about whether GP practices have complied with Rule 5.

27. We expect all GP practices to take this opportunity to review their existing settings and make sure that they are meeting these expectations for engaging with third party providers such as patient health portals. GP practices should undertake this exercise whether or not their patients have been affected by the MMH breach.

Two additional recommendations

28. At the moment, there is no central verification of whether key health sector suppliers such as patient health portals meet the relevant security standards set by the Health Information Standards Organisation (part of Health NZ). The health sector holds some of New Zealand's most sensitive information. Security breaches impact not only the affected individuals but also trust and confidence in the health system as a whole. Simply relying on vendor assurances about their security profile is problematic, as this inquiry shows.



29. To be certain that security is adequate, GP practices or other health providers technically have to check security documentation and contracts, or engage independent advice to assess the documentation that suppliers provide.

30. We consider that the status quo is unrealistic and unnecessarily burdensome. It leads to duplication, uncertainty and unnecessary expense for GP practices or other healthcare professionals, who usually do not have security or legal specialists on staff. Checking by multiple organisations as part of due diligence also increases compliance costs and engagement costs for suppliers.

31. Australia has approached this issue by introducing, amongst other things, a registration system for health organisations who wish to access electronic health records including organisations offering repository or portal services (the "My Health Records" Act). Whether or not the New Zealand government considers that this approach is appropriate, we consider that central government needs to do more to improve security confidence in health sector suppliers who are an increasingly important part of the system.

32. We therefore recommend that the Ministry of Health, as the health sector monitoring agency, should ensure there is a centralised and ongoing programme to verify that key health sector vendors such as patient health portal providers are meeting the relevant security standards.

33. This inquiry is a useful illustration of how the current provisions of the Privacy Act (particularly section 11) work. It has revealed weaknesses in the way in which the Privacy Act allocates legal responsibility for security, in situations where third party providers are involved. We consider that there is an opportunity to simplify the settings and better meet consumer and regulatory expectations.

34. While the inquiry has concluded that MMH is legally responsible under Rule 5(1)(a) of the Code, this has relied on a close examination of how MMH operates. Other patient health portals – as well as other third party health

services – operate differently and a security breach would not necessarily lead to the ability for OPC to take compliance action against that third party under Rule 5 of the Code.

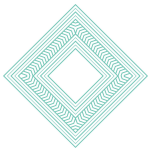
35. It should not be that complicated for the regulator, health consumers or health sector users of these services to identify which service provider or agency is accountable under the Privacy Act or its Codes. We also consider that the existing model, which relies on principal agencies making use of contractual remedies to address failures in security standards, is insufficient.

36. Instead, we recommend that all agencies should have direct liability for their security settings under the Privacy Act, including when they are providing services to others.

37. This would simplify the process for individuals seeking to complain about a security breach. In particular, it would simplify the section 11 analysis as part of an OPC investigation (and any later Human Rights Review Tribunal examination) and therefore improve efficiency.

38. Also it would enable OPC to take direct compliance action against a third party provider that fails to have reasonable security safeguards in place. At the moment, OPC's ability to bring compliance action relies on showing that the third party is using information on its own behalf or engaging directly with consumers, not merely processing information for a client organisation.

39. Finally, businesses – particularly small businesses like many general practitioners – should not have to rely on contractual provisions if the third parties that they engage fail to have reasonable security settings in place. It is unduly burdensome for each business to have to take separate legal action under contract to enforce security expectations. Contracts are important, but businesses should be confident that the Privacy Act itself also requires the third party to have reasonable security settings in place.



40. Again, Australia has also been considering this issue. The review of the Australian Privacy Act has recommended introducing a 'controller' and 'processor' distinction (Proposal 22.1), similar to the structure of the General Data Protection Regulation ("GDPR") in Europe. Under Article 32 of the GDPR, processors are required to have a level of security appropriate to the risk. This proposal was accepted in principle by the Australian Government. We agree that Article 32 is a useful model.

41. We therefore recommend that the Ministry of Justice, as the government agency responsible for Privacy Act policy, should seek amendments to the Act to ensure that third party service providers are directly liable under IPP5 for ensuring reasonable security safeguards are in place for personal information, even when they are collecting, storing and processing information on behalf of a principal organisation.

Next steps

42. Both MMH and Health NZ have told us that they have already made changes to better protect patient information. However, we intend to issue compliance notices under section 123 of the Privacy Act to both MMH and Health NZ, to independently check that those steps have in fact been taken and to check that the changes fix the breaches that this inquiry has identified. It is important that patients can be more confident that their information will be properly protected from now on.

43. We will also consider any complaints that affected people may make about this breach if they consider that the breach has caused them harm.

44. Finally, we will start Phase 2 of our inquiry shortly and will report on our findings later in 2026. That phase will consider issues such as:

- whether patients were properly asked for authorisation before a MMH account was established for them and information was stored in that account
- whether patients received adequate information about how the portal would be used
- how information in the portal was retained and deleted: for instance when a primary health practice ceases to use MMH; when a patient moves between practices; and when an account has been inactive or the patient has died
- the quality of communications about the breach
- whether the notifications to OPC and to affected patients met the requirements of the Privacy Act
- any aspects of these issues that are particularly relevant for Māori, especially Northland Māori
- whether any additions need to be made to the compliance notices to address other breaches of the Code.