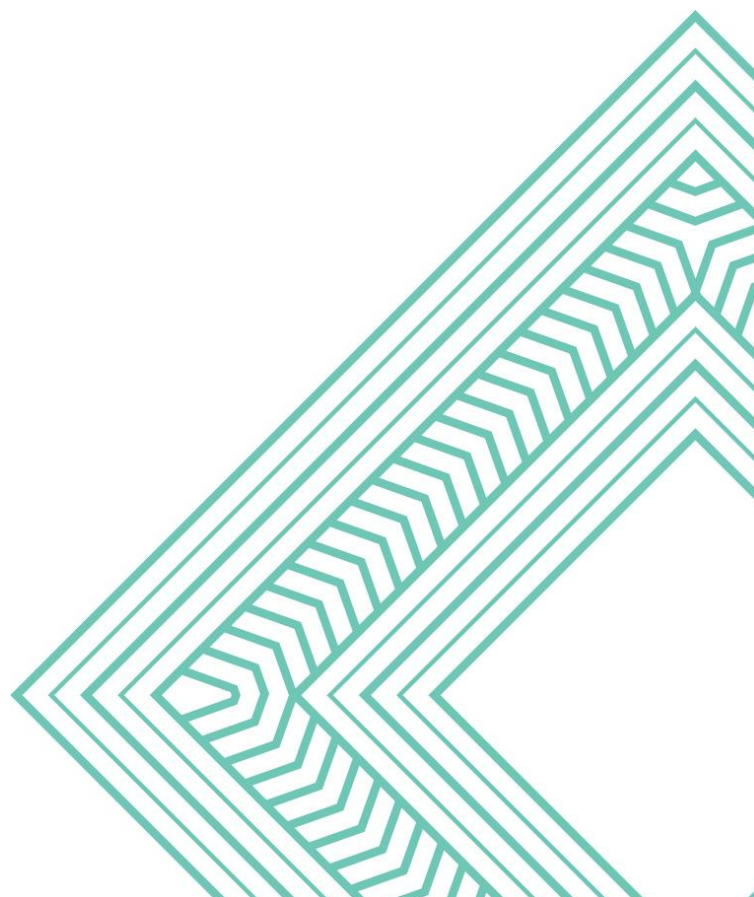


Executive summary: Inquiry into the cyber security breach affecting the Manage My Health Limited patient portal



Phase two report

27 October 2026



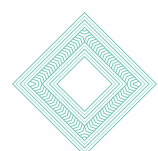
1 Executive Summary

The breach and this inquiry

1. Our Office has undertaken an inquiry under section 17(1)(i) of the Privacy Act 2020 into the cyber security breach of Manage My Health's patient portal at the end of 2025. The inquiry has been conducted in two phases.
2. Our [report into Phase 1](#) of the inquiry was published on 27 May 2026. That report contains a full description of the breach, the timeline, and our conclusions. We also issued compliance notices to [Manage My Health Limited](#) ("MMH") and to [Health New Zealand](#) ("Health NZ"). [Further information](#) can be found on our website.
3. This document is our report into Phase 2, which concludes the inquiry.

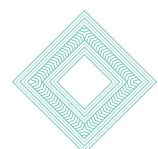
What this report covers

4. Phase 1 of the inquiry focused on security and legal accountability. Phase 2 therefore focuses on the remaining aspects of how patients came to be affected by the breach and what the impact of the breach was, both on affected people and on their wider communities.
5. We specifically comment on issues relating to:
 - authorisation for portal accounts to be set up
 - authorisation for detailed patient information to be stored
 - the quality of the information that users received about the portal
 - retention of accounts and information in the portal
 - breach notification and quality of communications.



The impact on people and their communities

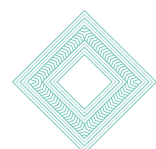
6. This breach affected many people around New Zealand. However, around 91% of affected people were Northland hospital patients: a massive majority. No other hospitals in New Zealand were sharing information through MMH. In fact, the only other patients affected appear to have been those who had uploaded their own records to MMH.
7. This means that, while the incident has created significant anxiety and difficulties around the country, it is the people of Northland and the GP practices that support them that have borne the brunt of the fallout. Inevitably, therefore, there has been a disproportionate impact on Māori patients, whānau and health services. We have actively considered those impacts under section 21(c) of the Privacy Act (“the Act”) which requires us to take into account cultural perspectives on privacy when performing statutory functions or exercising statutory powers. Here, the relevant cultural perspective is a Māori perspective.
8. Our consideration goes beyond mere numbers of affected people: there are features specific to that region that aggravated the impacts, especially for Māori. Some key comments made to us were that, as well as creating the distress experienced by many patients affected by the breach, it also:
 - exacerbated existing problems in Northland, especially existing distrust of health and government systems among already marginalised whānau
 - was not simply a stand-alone event, but added to the cumulative experience of systemic failures in the region
 - taxed the resilience of whānau, who are “sick of being resilient”
 - undermined the reliance that Northland patients and health practitioners need to be able to have on digital and virtual services, to cope with resource constraints



- extended beyond health portals into other unrelated areas of healthcare
- made government services harder to deliver in non-health fields such as emergency response.

Findings about Health NZ

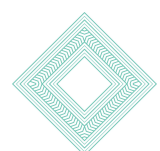
9. On 27 May 2026, Health NZ [announced](#) that it had cancelled the contract to supply hospital information to patients through MMH. It has temporarily reverted to supplying information in paper form (except for laboratory test results which are not supplied but held within the hospital).
10. Subsequently, on 24 July, Health NZ published its [action plan](#) to respond to the OPC inquiry and additional independent reports. As part of that action plan, Health NZ intends to roll out a new vendor-agnostic digital solution. Initially that solution will be offered in Northland. If successful, it might then be extended to other areas of the country.
11. We consider that this proposal creates both a challenge and an opportunity. The success of any new solution is likely to depend in large part on rebuilding trust in health services in general, and public health services in particular. To rebuild trust, it will be important to both hear and acknowledge the hurt experienced by the Northland community, and to ensure that the community has full input into the design and implementation of the new solution. This is particularly important if Health NZ is to support the Crown's commitments under the Treaty of Waitangi/Te Tiriti o Waitangi and fulfil its statutory responsibilities in relation to Māori health.
12. We recommend that Health NZ ensures that direct engagement with the Northland community and health providers is a central aspect of its action plan. This includes direct engagement with Māori (both end users and Māori health providers).



13. We also recommend that Health NZ should expressly include Māori data governance considerations as part of its procurement processes and in the terms of any contracts that it enters into with vendors who want to offer health portal services in Northland as part of the new solution.

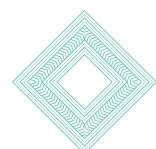
Findings about MMH

14. It has been apparent from the start of this inquiry that large numbers of patients were unaware that they had an MMH account at all, or that MMH still maintained an account for them despite the fact the patient had moved practices or their practice had ceased to use MMH. They were therefore taken entirely by surprise to find that they were affected by the breach.
15. We have investigated how MMH accounts came to be created and how information came to be saved into those accounts. Our key findings are as follows.
16. Many people had active MMH accounts and were aware that their health information was stored there.
17. However, some Northland hospital information was saved into accounts that patients had never activated. As we commented in our phase 1 report, we consider this to be the result of a flaw in the technical ‘match’ process that both agencies should have known about. That flaw was corrected in January 2026, when MMH amended the match criteria so that hospital information would only be imported into activated accounts.
18. Another flaw in the match process resulted in Northland hospital information being saved into the portal in situations where patients did not have an account at all. Instead, it imported information when the hospital details matched patient records that had been set up to transfer shared electronic healthcare records (“SEHR”) between health practitioners, or to enable patients to use the Easy Booking service. Health NZ did not ask for hospital information to be matched



against such records, as patients would not be able to view the information in the portal. By making a decision to include these records in the match criteria, MMH was therefore legally acting on its own account and needed to comply with the collection rules in the Health Information Privacy Code 2020 (“the Code”). While we accept that MMH did not use the information in any way, we consider there was clearly no valid purpose for importing information into the portal when patients could not access the records, and we also consider that MMH did not have consent of patients to do so. We have therefore found that it collected information in breach of rule 1 and 2(1) of the Code.

19. We were aware that MMH had already deleted all Northland hospital discharge information in non-activated accounts. However, it was not initially clear whether MMH continued to hold other types of information (including other hospital information such as lab test results) in any situations where information had been imported as a result of a match against SEHR or Easy Booking records. MMH formally confirmed to us that all information has been deleted except information held in activated accounts. This includes deleting the information from backups and storage systems. We are therefore satisfied that MMH has fully remediated the problem.
20. Some patients had activated their accounts at one time but had since forgotten that they had the account. Others had moved to a GP practice that did not use MMH or were enrolled with a GP practice that stopped using MMH, and did not realise that their account would remain live.
21. At the time of the breach, MMH only triggered a “dormant account” process after 24 months of inactivity. We have found that this is too long a period, and that it breached rule 9 of the Code. MMH is not required to retain information under the Health (Retention of Health Information) Regulations 1996, and there was no ongoing purpose for retaining the information for that length of time.
22. The problem has been partially remediated. MMH has already taken the initiative to improve its process for managing “dormant” accounts for patients



who are not with medical centres that are MMH users (“active practices”). It has reduced the time to 12 months before contacting patients to see whether they still want to maintain their account. We support this improvement.

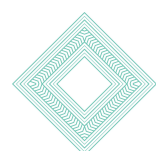
23. However, MMH still has a 24-month dormant account process for patients that are registered with active practices. While we acknowledge that not all patients would visit their GP during a year, we consider this is too long for health information to remain on the system without patients being given a choice about whether they wish to maintain an account.

24. In addition, we consider that MMH retains contact and other details in non-activated accounts for too long. Patients should have a reasonable opportunity to decide whether to activate their accounts, with a couple of reminders, but if the account is not activated after three months, we consider that it should be deleted.

25. We recommend that MMH’s ‘dormant’ account process for patients attached to an active practice should be reduced to 12 months, to match the process for other dormant accounts and to comply with rule 9 of the Code.

26. We also recommend that MMH implement a process to remove any non-activated accounts after three months (using a process similar to the ‘dormant account’ process), to comply with rule 9 of the Code.

27. At the start of phase 2 of our inquiry, there was no readily accessible information for representatives of people who have died about how to find out about and manage their MMH accounts. We recommended that MMH needed to update its information for representatives, including ensuring that they can access records in MMH accounts if required, as they are legally entitled to do. It accepted our recommendation. MMH has now provided additional information in its privacy policy for representatives of deceased people (see para 3.10), allows access to representatives (para 9.1) and has a process to delete information within 30 days of becoming aware that a person is deceased.

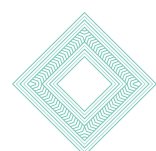


28. MMH updated its terms of use, privacy policy and business terms and conditions in June 2026. On our recommendation, it has made further amendments which were published on 30 September 2026. We agree that these amendments have improved the documents and have addressed the points we specifically mentioned. However, we have not reviewed the rest of the documents more thoroughly or provided further comments, as it is not our role to provide ongoing advice.

29. Instead, we recommend that MMH does full user-testing with patients and practitioners to ensure that the documents now provide clear information about people's rights and obligations.

Breach notification

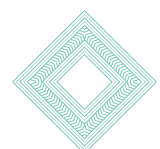
30. We consider that both MMH and Health NZ met their obligations under section 114 of the Act to notify our Office about the breach. MMH notified the Office within our expected timeframe of 72 hours of discovering the breach had occurred, and Health NZ also notified our Office as soon as practicable once it realised that the Northland hospital information had been affected by the breach.
31. While MMH did in fact notify our Office, it initially categorised the breach as not involving serious harm. MMH told us that this was an administrative error and it was promptly corrected after advice from our Office that this was clearly a breach that met the serious harm threshold.
32. We have reservations about the length of time that it took to notify some individuals, as required by section 115 of the Act. Final notifications were not completed until March.
33. The timeframe for notification ("as soon as practicable") is based on what a reasonable agency in this situation should have been able to do, not only on what the agency found itself able to do. Here, if contact details had been more



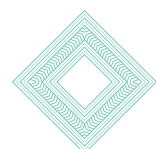
readily available and if the agency systems, processes, contracts and breach planning had been better, we consider it should have been possible to notify some individuals more quickly. However, this does not automatically mean that MMH or Health NZ breached the Act, especially as notifications were completed at different times. Whether any delay in notification in fact resulted in a breach of section 115 would have to be determined in the context of an individual complaint.

Recommendations for wider agencies

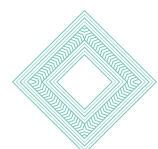
34. Every major breach creates lessons that other agencies can and should learn from. The MMH breach is an excellent example. We highlight the following points that others may find useful.
- a. The MMH and Health NZ compliance notices provide valuable information to all agencies about our regulatory expectations for security. We advise agencies to review them for points that are relevant to them.
 - b. If an agency which is processing information on behalf of another agency makes a design decision that goes beyond its instructions, it will be seen as acting on its own account (whether or not it actively uses the information) and will be independently liable under the relevant privacy principles.
 - c. If a customer does not complete a registration process (for instance by setting a password or activating their account), they have not authorised any further collection and storage of information in that account.
 - d. GP practices and specialist health practitioners should take this opportunity to check that patients are properly informed about how the SEHR system operates and, where necessary, obtain patient authorisation to transfer information.



- e. GP practices should also check that they have accurately specified the age at which MMH should de-link a child's portal accounts from the account belonging to their parents or guardians (at the latest at age 16, unless there is ongoing legal authority to keep the accounts linked). This will ensure that parents or guardians do not have unauthorised access to the health records of young people.
- f. All agencies that operate customer accounts should have a process to identify and manage 'dormant' accounts. What that process is, and whether information can be kept will vary between agencies. It will be determined by any laws that require retention of information, and by any lawful ongoing purpose for retaining it. Unless there is a specific law or reason requiring retention, we consider it is general best practice to check in with an account holder after 12 months of inactivity to see whether they wish to retain the account.
- g. Any agency that is relying on authorisation as a legal basis for collecting, using or disclosing personal information should ensure that information provided to individuals is clear and precise so that they fully understand what they are being asked to agree to.
- h. Agencies should have a clear process for personal representatives to follow when an account holder has died, and should make sure that representatives can find information about what to do.
- i. All agencies should have a proper breach (or crisis) management plan in place that includes:
 - whether they have ready access to contact details for people whose information they hold, and if not, who would have those details
 - how to distribute information (for example, anticipating that they will need to partner with client agencies that have a direct relationship with affected people)



- who will handle media and regulator queries
 - how they will ensure that public statements or messages to affected people are accurate, or be clear when they have only incomplete information and when a clearer picture might emerge
 - how they will ensure that communications are focused on the harm the breach has caused affected people, even when the company's staff are under significant stress and themselves feel victimised by the breach
 - having good internal processes to report breaches up to appropriate staff quickly so that those breaches can be promptly assessed, managed and notified to OPC and to affected people as soon as practicable (failure to have good processes to identify affected people and assess and manage breaches is not a 'reasonable' excuse for delaying notification)
 - making sure key people can be contacted at all times including over holidays
 - ensuring that the agency can scale up legal and technical support if required to manage a major breach, including having external support available
 - ensuring the agency has planned access to support services which can assist affected people (e.g. call centre support, health and wellbeing services, identity protection services and so on), including culturally relevant support where needed.
- j. Agencies should consider whether proposals or breach responses may have a particular cultural impact, and ensure that that impact is properly assessed. For projects, direct engagement with affected communities will provide valuable insights, and techniques such as completing Māori data



governance assessments can also assist. For breach responses, direct engagement can restore trust and confidence more quickly and effectively than dealing exclusively at arm's length.

- k. Agencies should ensure that their contracts do not contain clauses that purport to oust or limit liability for compensation under the Privacy Act, or that purport to limit Privacy Act liability if personal information held by the agency has been compromised by criminal activity. Any liability or remedies in such circumstances will be determined by the normal application of the Act (or applicable Code).

Next steps

- 35. We have issued compliance notices to MMH and Health NZ following our findings in Phase 1 of this inquiry. These will be managed as stated in the notices. We have also received around 50 complaints, which we will also manage as part of our normal dispute resolution processes.
- 36. However, this Phase 2 report now concludes the inquiry itself, and the inquiry is now formally **closed**.

