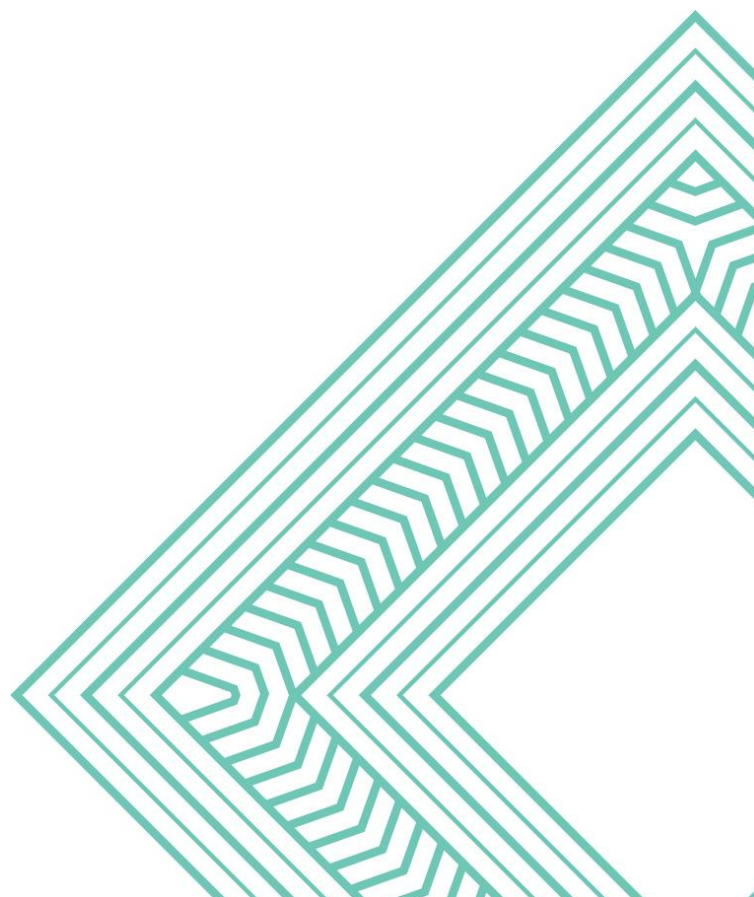


Inquiry into the cyber security breach affecting the Manage My Health Limited patient portal



Phase two report

27 October 2026



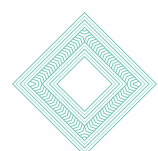
1 Executive Summary

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.

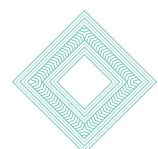
What this report covers

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

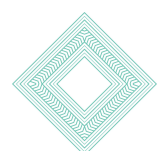
6. This breach affected many people around New Zealand. However, around 91% of affected people were Northland hospital patients: a massive majority. No other hospitals in New Zealand were sharing information through MMH. In fact, the only other patients affected appear to have been those who had uploaded 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

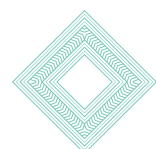
9. On 27 May 2026, Health NZ [announced](#) that it had cancelled the contract to supply hospital information to patients through MMH. It has temporarily reverted to supplying information in paper form (except for laboratory test results which are not supplied but held within the hospital).
10. Subsequently, 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.

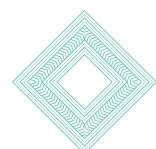
Findings about MMH

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.

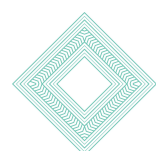
23. However, MMH still has a 24-month dormant account process for patients that are registered with active practices. While we acknowledge that not all patients would visit their GP during a year, we consider this is too long for health information to remain on the system without patients being given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

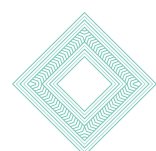


28. MMH updated its terms of use, privacy policy and business terms and conditions in June 2026. On our recommendation, it has made further amendments which were published on 30 September 2026. We agree that these amendments have improved the documents and have addressed the points we specifically mentioned. 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

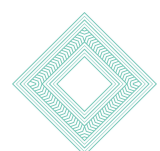
30. We consider that both MMH and Health NZ met their obligations under section 114 of the Act to notify our Office about the breach. MMH notified the Office within our expected timeframe of 72 hours of discovering the breach had occurred, and Health NZ also notified our Office as soon as practicable 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



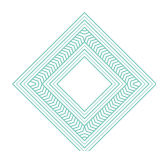
readily available and if the agency systems, processes, contracts and breach planning had been better, we consider it should have been possible to notify some individuals more quickly. However, this does not automatically mean that MMH or Health NZ breached the Act, especially as notifications were completed 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

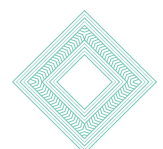
34. Every major breach creates lessons that other agencies can and should learn from. The MMH breach is an excellent example. We highlight the following points that others may find useful.
- a. The MMH and Health NZ compliance notices provide valuable information to all agencies about our regulatory 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

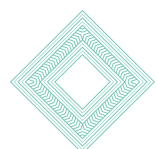


governance assessments can also assist. For breach responses, direct engagement can restore trust and confidence more quickly and effectively than dealing exclusively at arm's length.

- 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**.

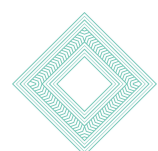


2 The inquiry so far, and the scope of Phase 2

37. Phase 1 of the inquiry described the nature and scope of the breach and came to conclusions about its causes. It explained the relationships between the different agencies (MMH, Health NZ and GP practices) and made findings about which agencies bore responsibility for the security of the information that was affected by the breach.
38. It is not necessary to repeat all those details here. However, it is useful to provide a brief summary of the breach, the findings of Phase 1 and what has happened in the intervening months, as background for our Phase 2 findings.

The breach

39. MMH operates a long-standing New Zealand patient health portal. On 30 December 2025, MMH discovered that the “My Health Documents” module in the portal had been infiltrated by criminal threat actors (“hackers”) and copies of a large number of patient health documents had been stolen. Other areas of the MMH portal were not affected by the breach.
40. Around 100,000 patients were affected, and approximately 91% of them were from the Northland region. This was because of a unique arrangement between the Northland District Health Board (now Health NZ) and MMH to supply hospital discharge documentation to patients who had accounts with the portal. All these documents were stored in the “Health Documents” module that had been compromised by the hackers. The remaining affected documents had been uploaded by patients themselves.
41. MMH and Health NZ both notified our Office about the breach at the start of January 2026. As a result of the scale of the breach and the sensitivity of the information that was compromised, the Privacy Commissioner opened a formal inquiry under section 17(1)(i) of the Privacy Act. The inquiry was announced on 21 January 2026, and [Terms of Reference](#) were issued on 27 January 2026.

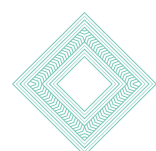


The Phase 1 findings

42. Our report on Phase 1 of the inquiry was concluded on 25 May 2026, and published on 27 May. Key findings were:

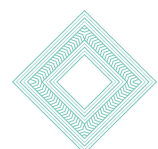
- MMH was acting on its own behalf rather than on behalf of Health NZ in relation to the information that was affected by the breach. A key to that finding was that MMH had a clear and direct relationship with the patient. It therefore ‘held’ that information and was directly responsible for its security. We found that MMH did not have reasonable security settings to protect the information, and that it had therefore breached rule 5(1)(a) of the Code.
- Health NZ was the original source of the Northland hospitals’ discharge information. It also designed and implemented the project to supply that information to patients through MMH, including paying the licence fees for Northland GP practices that were engaged in the portal project to sign up with MMH. We found that Health NZ had failed to ensure that there were adequate security safeguards in place as part of the design and implementation of the project. We therefore found Health NZ had breached rule 5(1)(b) of the Code. However, we found that it did not “hold” the hospital information once it was stored in the MMH portal. It could neither view that information nor directly control what happened to it. The actual security settings in the portal were MMH’s responsibility.

43. Primary healthcare providers – including GP practices – did not supply any of the information that was stored in the “My Health Documents” area of the portal. They also had no ability to view or control that information in that section either on their own behalf or on behalf of their patients. As it happens, GP practices were therefore not responsible for the security of the information that was affected by the breach and did not breach rule 5 of the Code in relation to that information. However, if the hackers had accessed information in any other area of the portal, this could have been different. The phase 1 report therefore took the opportunity to highlight the responsibilities that GP practices have to



protect the security of patient information that they supply to health portals, including MMH. Responsibilities include undertaking due diligence, training staff and ensuring the systems are properly used.

44. We recognised that it is not feasible or efficient to expect each individual GP practice to separately assess technical security issues for health portals (or other key health system vendors) that support multiple businesses in the sector. Instead, they should be able to rely on a central security accreditation programme. We recommended that the Ministry of Health should ensure that a programme was established to verify that portal providers and other key health service vendors meet appropriate security standards.
45. At present, section 11 of the Act insulates agencies that are merely processing information on behalf of others from liability under the Act for their security settings. Instead, the agency procuring their services needs to enforce any security clauses or warranties in the contract. This is not reasonable or efficient in our modern digital environment, particularly for small businesses (like many GP practices) that have little or no ability to influence or check security clauses in contracts or get effective assurance about security settings. Instead, vendors should always be directly responsible under the Act for the security of their systems, regardless of whether they are acting on their own behalf or processing or storing information for others. While principal agencies have their own obligations under Information Privacy Principle (IPP) 5(1)(b), we therefore recommended that the Ministry of Justice should support an amendment to the Act to ensure that all agencies that process information on behalf of others are legally responsible for their security settings.



What has happened since Phase 1 finished

46. Several important things have happened since Phase 1 concluded.

OPC has issued compliance notices

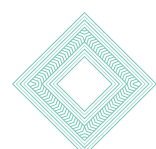
47. We issued compliance notices [to MMH](#) and [to Health NZ](#) requiring them to take specific steps to rectify the breaches of rule 5 of the Code that our inquiry had identified. MMH and Health NZ had already made some improvements to their security practice and governance and had planned or were in the process of making other improvements. The compliance notices now legally require them to take the remaining steps that we consider necessary.

48. Importantly, compliance notices do not provide a guarantee that all aspects of the respondent agencies' practices are now fully compliant with the law. Compliance notices can only address the breaches of the law that we identified during the inquiry – that is, those that were relevant to this particular cyber security breach.

49. Also, complying with a notice still only gives a snapshot of an agency's practice at a particular point in time. Future breaches – even breaches of the same or similar type – may still happen if agencies fail to maintain the security and privacy controls that they put in place to meet the requirements of the notice. Agencies need to ensure that they maintain those controls, as repeat breaches are likely to attract further regulatory attention from the Privacy Commissioner.

50. These compliance notices have no legal effect on other agencies. However, they are a strong indication of our regulatory expectations for what is required to comply with rule 5 of the Code.

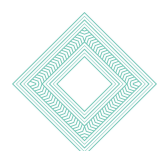
51. We therefore advise all agencies to review the MMH and Health NZ compliance notice requirements and use any criteria that are relevant to assess aspects of their own systems and see where they may have gaps. They should also



ensure that all controls are properly maintained to reduce the likelihood of further breaches.

Health NZ has stopped sharing with MMH but is planning a new digital solution

52. On 27 May 2026, Health NZ [announced](#) that it had stopped sending hospital information from its Northland sites to patients through MMH. It cancelled that contract with MMH and reverted to providing all patients with discharge documentation in paper format. It has also cancelled the arrangement to pay MMH licence fees for Northland GPs engaged in the portal project (the cancellation takes effect in late November 2026).
53. However, the benefits of the digital project for hospital documentation were strong enough that Health NZ is taking new steps to enable patients to get documents in digital format again. Health NZ's [action plan](#) in response to the inquiry and reviews (24 July 2026) records that it intends to implement a vendor-agnostic digital solution for the provision of hospital discharge information. It will initially roll the solution out in Northland. Decisions on whether there would be any wider roll-out will be made after that. The indicative timeframe for delivery is Q3 (January-March 2027).
54. The compliance notice to Health NZ requires OPC to be consulted before the solution is implemented.
55. However, we consider that direct engagement with people in Northland, including a range of Northland Māori representatives (both end users and Māori health providers), will also be essential, to start to restore the trust that was lost as a result of the breach. The success of the project depends on it. Some of our hui participants suggested that co-design would be an appropriate approach, particularly given Health NZ's obligations to support the Crown's commitments under the Treaty of Waitangi/Te Tiriti o Waitangi. Digital services have a real potential to alleviate some of the inequities for people in areas such as Northland (while acknowledging that there is still a major digital divide).



However, it is apparent from discussions with affected people during this inquiry that Health NZ and relevant portal vendors cannot simply assume that the Northland population will be willing to adopt a new solution.

56. We therefore recommend that Health NZ ensures that direct engagement with the Northland community and health providers is a central aspect of its action plan.

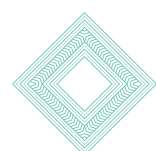
57. We also recommend that Health NZ should expressly include Māori data governance considerations as part of its procurement processes and in the terms of any contracts that it enters into with vendors who want to offer health portal services in Northland as part of the new solution.

58. A useful approach would be to complete a Māori data governance assessment as part of the Health NZ review of any new proposed solution, with the assistance of either internal or external Māori data specialists.

59. Health NZ's action plan also records that it has developed a broad programme of work to improve security and privacy across its systems, including in areas such as risk management standards, contracting and delivery governance. Some of that work is already under way. This programme aims to respond both to the findings of Phase 1 of our inquiry, and also to the other independent cybersecurity reports that were published on 27 May 2026: the [report from CyberCX](#) commissioned by the Ministry of Health, and the [report from Deloitte](#) that was commissioned by Health NZ itself. Our compliance notice to Health NZ will ensure that the delivery timeframes for some of these critical changes are met.

MMH has been working on security improvements and has updated its documentation

60. MMH has been heavily focused on improving its security settings over the last few months. It is also involved in assessment against the Health Information Security Framework, as required by the central government health agencies.



61. On 25 June 2026, MMH published new versions of its terms of use, privacy policy and business terms and conditions. These were meant to clarify some aspects of the relationships and relative responsibilities between MMH and its users (both GP practices and individuals). After some feedback from us, MMH has made further amendments which were published on 30 September 2026.

Complaints

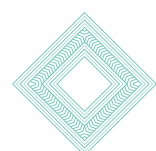
62. We have received formal complaints from around 50 people about the effect that the breach has had on them. The conclusion of the inquiry does not affect the process of resolving those complaints, which will be managed as usual by our Office. If a resolution is not achieved, complainants would then have the right to take a case to the Human Rights Review Tribunal for assessment and potential financial damages or other remedies.

Ministry of Health

63. The Ministry of Health has accepted the recommendation made in our Phase 1 report that it should establish a more centralised and ongoing approach to assuring that patient portal providers and other relevant vendors meet appropriate security standards. The shape of that approach is still to be determined. It is currently exploring options for strengthening sector-wide assurance arrangements, including the role of central oversight, accountability, and regulatory settings.

Ministry of Justice

64. As noted in a [recent report of the Petitions Committee](#) (August 2026), and the [Cybersecurity Action Plan](#), the Ministry of Justice will seek decisions from Ministers in due course on options to incentivise the protection of personal information from cyber threats, including changes to the Privacy Act.



What's in this report – the scope of phase 2

65. Phase 1 of the inquiry focused on security considerations and legal accountability. Phase 2 of the inquiry considers the remaining aspects of the breach.
66. First, it explains what we have learned about the impacts on people affected by this breach, particularly in Northland and particularly for people and their whānau who are Māori.
67. Recovery from a breach starts with acknowledgement of the harm that affected people have suffered. The effect this breach has had on people is also a useful signal to other agencies about the importance of managing privacy well. There is often a tendency to look at security and privacy purely through a technical or process lens. However, this inquiry shows that there is a very real human cost when things go wrong, and it is essential for agencies to take a person-centred approach to their risk management, project or product design and processes including service delivery from third parties.
68. The report then considers what this breach can tell us about:
- patient authorisation for collection, storage and use of their information
 - what to tell people about how their information will be collected, stored and used
 - issues relating to retention of information
 - lessons for breach response and communications.
69. In doing so, it is not merely focused on assessing whether MMH or Health NZ were legally at fault for what they did, or what they failed to do. More importantly, it uses this breach as a detailed case study that illustrates OPC's regulatory expectations. Again, other agencies therefore can, and should, use this as an opportunity to review and improve their own systems and processes.



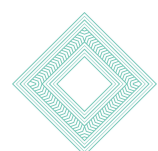
Methodology

70. As with Phase 1 of the inquiry, we collected information from Health NZ, MMH, general practitioners and affected people. That information was provided in a variety of ways:

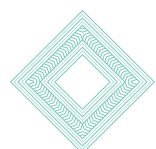
- as part of the original mandatory breach notification process under the Privacy Act
- in response to statutory information demands under the Privacy Act and meetings or follow-up questions
- through meetings with GP representative organisations and PHOs
- through a hui in Northland hosted by Ngāti Hine Health Trust
- through correspondence from affected people, including people making enquiries or formal complaints.

71. Our principal reference point for our analysis has of course been the requirements of the Code and the Act. However, we have also built on the Office's own previously published regulatory expectations set out in [Poupou Matatapu: Doing Privacy Well](#).

72. In addition, because the breach has had such a significant effect on Northland – and therefore an inevitably disproportionate effect on Māori – we have also referred to Te Kahui Raraunga's [Māori Data Governance Model](#), to help us identify and articulate what more should be done to address Māori concerns over their data in the context of a digital project such as this and to provide guidance about ways in which trust might be gradually restored. The effect on Māori goes beyond numbers of affected people: Māori may experience disparate effects, relating to breaches of Treaty principles, tikanga and values. Socio-economic conditions in Northland and regional disparities in health funding and service provision can also lead to effects that other populations would not experience.



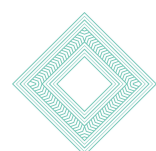
73. We also acknowledge the assistance of our Māori Reference Panel, Te Ranga Tautiaki. They have helped us to articulate our findings more clearly than we would otherwise have been able to do.
74. MMH, Health NZ and GP representative organisations (the Royal College of General Practitioners, GP Aotearoa and General Practice NZ) have had an opportunity to comment on aspects of the findings that are relevant to them. We have taken those comments into account in this final report.



3 The impacts on people

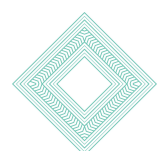
The effect goes beyond the immediate breach

75. Many people across New Zealand have been affected in one way or another by the MMH breach. As with any major privacy breach, that impact goes beyond the 100,000 people whose information was stolen by the hackers. In particular, it is evident that there has been a broader (though potentially temporary) loss of confidence and trust not only in MMH and Health NZ themselves but in other health practitioners and digital health providers. As an example, GP practices, PHOs and GP peak bodies from around New Zealand have reported that some patients have started requesting physical rather than digital copies of information. Some patients are also now more wary of using portals or other digital technologies, even if they were not themselves impacted by the breach.
76. This is why it is so important that MMH and Health NZ complete all required steps to address the flaws that led to the breach so that patients can continue to use their services with confidence. It is critically important that patients feel able to seek help from GP practices, specialists and hospitals without worrying about what is happening with their information. Patient health portals are a small but important part of the modern health information environment. As long as they are safe and well managed, they provide a valuable and effective service for patients and enable greater efficiencies for GP practices.
77. Other health agencies also need to learn lessons from the breach, so that they can provide assurances to their patients. This includes ensuring that government agencies follow through on their intentions to support and enforce better security of health information right across the sector. The MMH incident has proved to be a useful – and necessary – wake-up call for health authorities, health practitioners and health information service providers alike.



The harm suffered by affected people

78. As we recorded in paragraphs 59-63 of our Phase 1 report, it was immediately clear that the theft of both medical and non-medical information (including identity or location-related information) had caused many people substantial distress and uncertainty. All health information is sensitive, and this degree of distress is entirely understandable.
79. As required under section 21(c) of the Act, we have specifically considered cultural perspectives on how this breach has affected people, most obviously Māori people in Te Tai Tokerau (Northland). From a Māori perspective, the breach has led to “hara” – an injury that diminishes the mana of all involved. That impact is experienced holistically: it can be physical, mental, spiritual or social. A person’s data is an extension of themselves. A breach affects tapu (or the human dignity of the person), mauri (life force) and mana (right to authority and control of one’s own information). It is important to restore balance and correctness in order to heal and move forward, for example through a hohou te rongo (tikanga-based restorative justice) approach.
80. Out of the approximately 150 people who originally contacted us to register concern about the breach and how it was being managed, around 50 have since chosen to make formal complaints to the Office. Those complaints will continue to be managed using our normal processes.
81. This is obviously a tiny proportion of the overall number of affected people. However, it would be wrong to use this small figure to downplay how much people care. In fact, based on our experience of other significant breaches, it is unusual to get even this number of complaints. Typically, many affected people simply want the breach to be properly addressed and feel satisfied when OPC takes action and holds agencies to account, as we have done through this inquiry. To have this number of people who wish to take the time to bring formal complaints says a lot about the harm that people feel that they have suffered. In addition, Māori may be less likely to complain to government agencies. As

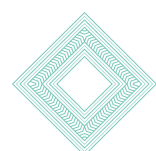


OPC's [most recent survey](#) shows, Māori have significantly less trust in government agencies than others (21% vs 31%).

82. The broader impacts on people have also become even more apparent during our Phase 2 discussions. We have listened to what people have to say, not only through ongoing correspondence with complainants but also through various meetings with GP practices and peak bodies who reflected what they have heard from patients. In addition, some members of our inquiry team travelled to Whangārei to hear directly from Northland primary health providers and affected people at a hui on 13 July 2026 hosted by Ngāti Hine Health Trust.

The particular impact on Northland

83. All affected people and their privacy are equally important to our Office, wherever they live and whoever they are.
84. However, it is important for us to recognise that, in many important ways, this breach is not in fact a nationwide event. Around 91% of affected people were Northland hospital patients: a massive majority. No other hospitals in New Zealand were sharing discharge information through MMH. In fact, the only other patients affected appear to have been those who had uploaded their own records to MMH.
85. This means that, while the incident has created significant anxiety and difficulties around the country, it is predominantly the people of Northland and the GP practices that support them that have borne the brunt of the fallout.
86. Section 21 of the Act requires us to take account of cultural perspectives when exercising statutory functions or powers. In this situation, relevant cultural perspectives were obviously those of Northland Māori.
87. Given our time and resourcing limitations, it has not been possible to consult a statistically representative sample of affected people (including a statistically representative sample of Māori). However, the hui in Whangārei, hosted by

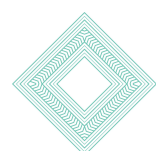


Ngāti Hine Health Trust, provided valuable qualitative insights into the experiences, concerns and expectations of Māori patients and whānau, healthcare providers and their communities.

88. Attendance was lower than anticipated due to unexpected commitments on the day, including two significant tangi. However, the value of the hui should not be assessed solely by the number of people present. Participants brought a range of relevant experiences and perspectives including direct experience of the breach and knowledge of the experiences of patients and healthcare providers across the region. Participants included respected Māori health providers. The hui also needs to be understood in its cultural context. In keeping with the principle of whanaungatanga, participants drew on their relationships with patients, whānau, GP practices and wider community networks to inform the discussion. This enabled them to contribute perspectives extending beyond their individual experiences. While these contributions cannot be assumed to represent all Māori or affected people, they provided important insights into the wider context in which the breach occurred and its potential implications for patients and communities.
89. In our view, contributions were informed, thoughtful and constructive. Rather than focusing solely on assigning blame, participants considered what could be learned from the incident and how the response could support improved privacy practices, strengthen safeguards and rebuild or maintain patient trust in health services.
90. Importantly, the themes raised at the hui were also consistent with concerns and perspectives emerging from other engagement undertaken as part of the inquiry including discussions with GP representative groups, complainants and other affected people and their healthcare providers.

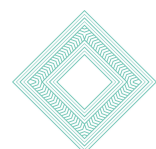
The impacts on Northland patients and their whānau

91. First, affected patients in Northland reported the same feelings of harm and

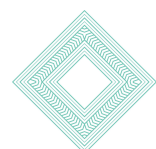


distress that other affected people experienced.

92. While any redress under the Act is limited to distress caused by the actual loss of personal information, we acknowledge that the distress that people suffered goes beyond the documents that were compromised. For example, patients who had highly sensitive information in the portal (including records of sexual assault, family harm and justice involvement) were at risk of re-traumatisation as a result of the breach, even though in many cases the information itself turned out not to be stored in the “My Health Documents” section of the portal and was therefore not stolen. In addition, the initial uncertainty about what had and had not been accessed by the hackers in itself created distress.
93. As well as distress caused by the loss of medical information, identity theft was a key concern for hui participants or their patients. This is because in some cases names, addresses, photos and contact information were exposed. There was a real concern about the potential for fraudulent activity, or the potential for information to be exposed to abusers.
94. Secondly, however, while some of the harm is common to people around the motu, some issues raised at the hui were more specific to Northland itself.
95. A key theme was the extent to which the breach had exacerbated existing problems in the Northland region, including among Māori. In particular, it had compounded existing distrust of health and government systems among already marginalised whānau, including those involved with Corrections, ACC sensitive claims (that is, survivors of sexual abuse) and unconsented dwellings.
96. Participants in the hui recognised that patient distress was not always proportional to the sensitivity of the actual information disclosed. Instead, it was often about the cumulative experience of systemic failure in the region and what the breach meant for personal identity, autonomy and safety. Participants noted that whānau were resilient, but this was framed as a concern rather than a strength to rely on. As one participant said, “we’re sick of being resilient”.



97. It was also clear that the impact on the Northland region goes beyond the simple statistic that the majority of people affected by the breach live in that region. This is because Northland has a particularly strong reliance on digital and virtual health services, driven by resource constraints. This makes portal use – and trust in portals – particularly critical in that region.
98. This reliance on digital health services is why Health NZ's project to deliver patient records was such a valuable idea and why that was a useful region in which to offer the new service. Done well, it had the capacity to reduce health inequities (which the Health NZ documentation has clearly demonstrated was one of its prime intentions). Prior to the breach, the project also appeared to be reasonably successful. It met the consumer demand that Health NZ and the Northland Health Consumer Council had identified. Patient take-up of the services had increased significantly, from around 19% at the start of the pilot in 2020 to around 40% by the time the full project got under way in 2023, with more coming on board during the project itself (potentially influenced by the choice to pay licence fees for project participants as well as intensive communication efforts). Supplying documents in digital form through the portal seemed to work well for patients who elected to use it, and reduced administrative burdens on both the hospitals and GP practices.
99. The breach has frustrated that intention, and instead appears to have significantly damaged many people's trust in portals. Even more importantly, health practices reported to us that damage to trust also extends beyond the digital environment into other (apparently unrelated) areas where health practitioners are trying to support their communities. An example provided was immunisation coverage – already a trust-sensitive area. This was cited both by participants at the Northland hui and some other primary care providers as a domain where portal distrust now compounds existing hesitancy.
100. It appears that the problems have even extended beyond the health field. Workers supporting whānau after recent flooding noted that data collection was



already a fraught trust-building exercise, and the breach made future data sharing more difficult.

Experience of the way in which the breach was managed

Effect on practices

101. GP practices around the country had to respond immediately to the breach.

This was particularly evident in Northland, where the majority of affected patients lived. In some cases, staff were brought back from summer holiday leave so practices could have "all hands on deck".

102. Because of the nature of the breached information (including hospital discharge records), it was not unusual in Northland for staff to have to manage patient responses to the breach when their own information had also been stolen.

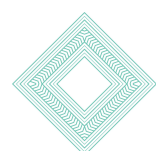
Responsibilities for providing information about the breach

103. Responsibility for information provision to patients was an area of real uncertainty and tension between practices and MMH. GP practices and PHOs, including in Northland, felt that there was no clear guidance on who was responsible for doing what. MMH initially told practices not to notify their own patients directly; instead, communications had to come centrally through MMH itself. For doctors, this created tensions with the clinical duty of care, particularly for patients who were more vulnerable.

Uncertainty about who was affected and how many people were affected

104. The number of affected individuals changed rapidly and repeatedly. Patients themselves reported that messaging from MMH was inconsistent: some were told they had been breached when they had not, and vice versa. Many people reported being confused about what was going on.

105. The problems also affected information given to practices. For example, one Northland practice reported initially being told it had a small number of affected



patients to being told it had more than a thousand. GP practices that had set up a way of dealing with the breach were unable to scale the response up to meet the larger numbers (e.g. an initial process to hold individual conversations with affected whānau was not going to be feasible once the numbers became so large). Such discrepancies are not necessarily unusual while the scale and effect of a breach is being assessed. However, this shows the importance of forward planning and clear communication, which we discuss later in section 5.

Difficulties with identifying and informing vulnerable people

106. Similarly, agencies that hold information about people who are considered vulnerable (for example because of health condition, age or capacity) need to think particularly carefully about how to identify them, and whether – and if so how – any communications about a breach will be provided to those people.
107. Again, this was a source of frustration for GP practices. It took some time for MMH and Health NZ to provide advice about this issue. Even then, there was a perception amongst some GPs in Northland that notification criteria for "high vulnerability" were expedited for political rather than clinical reasons. We have seen no evidence that that perception was correct, but it is unfortunate that some were able to interpret the situation that way. The main point was that the criteria were reported as being poorly defined. Again, defining vulnerability is an example of something that can be worked out in advance.
108. Practices then felt pressured to have GPs contact vulnerable patients directly without adequate information or clinical context. Some practices and PHOs pushed back, noting risks of inadvertently disclosing sensitive information (such as mental health or sexual health status) to parents of young people. There were also concerns about notifying patients in situations where an abuse perpetrator might still be in the house.



The actual information was not always appropriate or enough

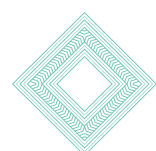
109. One large Māori health practice chose not to rely on official MMH or Health NZ communications, citing a lack of manaaki in the messaging. Instead, staff stayed past midnight calling patients individually, with clinical staff assessing each person's likely response before making contact.

110. Another large Māori health practice relied heavily on its PHO for guidance. It reported that it could offer patients little beyond advice to change their passwords.

111. A variety of examples were provided about how the breach response had in some cases led to greater confusion and distress:

- One patient described receiving only a generic notification email with no guidance from their GP, and having to independently seek out a nurse for reassurance.
- Another patient described being unable to get clear answers from anybody; they ultimately stopped use of Manage My Health entirely.
- One community worker described a whānau member who had no GP, and could not get answers from MMH to basic questions, such as: where did the information go; how long was it held before the breach; and what could be done about it.
- Concern was raised about notifications reaching households where young people had sensitive health information (mental health, reproductive health) that they did not want disclosed to parents. Participants advocated for Children's Commissioner involvement in notification design.

112. Northland practices also expressed real frustration at what it perceived as Health NZ's absence during the response. To quote hui participants, Health NZ was "nowhere to be seen when it needed to step up."



What will it take to restore trust?

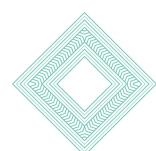
113. In te ao Māori, how a goal is achieved – through proper engagement, consensus and adherence to correct process – is just as important, or more important than, the final result itself. A good result will not save a poor process where it has been conducted with a lack of respect for the dignity, authority and wellbeing of people. To a Māori way of thinking, it is important to avoid mistakes where possible, but where they occur, they must be rectified properly in order to make things right.
114. Hui participants had some useful specific comments about how health portals should operate and the steps they considered necessary to rebuild trust. We have taken these views into account and considered them alongside the Code, our inquiry findings and our regulatory expectations.

Consent and informed engagement

115. First, patients must be genuinely informed about what a portal is, why it is used, where data goes, and what happens when they leave a practice, not simply handed a form to sign.
116. Consent processes should be supported by a trusted navigator, such as a community health worker or kaiāwhina, sitting with whānau and explaining matters in plain language.
117. Data should be deleted when it is no longer needed, with patients understanding the full data lifecycle from the outset.

Culturally responsive support

118. Digital tools must be supported by people from the community, "supported by people who've grown up like us." Face-to-face and phone-based support must remain available alongside digital options, since one-size-fits-all digital approaches exclude many whānau.
119. Again, navigator roles are critical to helping whānau access systems and



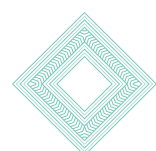
require proper resourcing and recognition.

Standards, accountability and governance

120. The hui supported the approach we recommended in Phase 1 of having centralised, independent verification that portal providers meet relevant cybersecurity standards. Hui participants considered that standards should be actively monitored and enforced rather than simply published, and suggested that the Ministry of Health consider funding independent organisations with appropriate cybersecurity assurance capability to undertake this work.
121. Data sovereignty and governance were framed as priorities, with stewardship of health data needing to include Māori governance frameworks such as the Te Kāhui Raraunga Māori Data Governance Model.
122. Hui participants also said that commercial portal providers' business models should be subject to contractual conditions that prioritise patient welfare over commercial interests.

Regional breach response playbook

123. A regional crisis response playbook was proposed, modelled on civil defence and flood response frameworks, with coordinated, pre-agreed roles and clear communication chains extending down to practice level, including a flowchart for who to call, what to say, and when numbers are confirmed.
124. Breach communications can usefully be outsourced to a skilled contact centre (as MMH did here) but with Māori kaiāwhina or navigators, modelled on Healthline, Whakaruruhau, and COVID-19 response infrastructure. Key points included:
- A single, consistent message to whānau is essential; multiple contradictory emails caused confusion and eroded trust.



- Mental health and social work support should sit alongside IT helpdesk support.
- Practices should not be left to independently verify patient lists or manage communications without support.
- A structured debrief culture was recommended after each crisis; participants noted that in this case, "we just moved on to the next thing."

Restorative justice

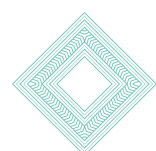
125. A restorative justice component was proposed. Whānau want to hear from the agencies themselves in order to reach closure, not simply see compliance notices issued. There needs to be both demonstrated improvement and personal acknowledgement of how the breach has affected Northland communities.

126. This aligns with the approach proposed by our Office and the Independent Police Conduct Authority as part of the [joint inquiry into police conduct when photographing members of the public](#) (see in particular paras 598-602).

127. As with that inquiry, we therefore recommend Health NZ and MMH hold hui kanohi ki te kanohi (face to face) with the Northland community to discuss issues raised by the breach. This would enable them to better understand the impact of the breach on the community and the wider implications felt by whānau. It would allow whānau to see and feel the intent of the apologies provided and would allow the agencies to directly acknowledge the hurt felt. This would reflect tikanga, and would help balance to be restored to move forward from the breach.

Foundational work before further digitisation

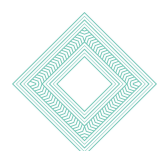
128. There was strong consensus that foundational issues, forms, consent processes, and privacy arrangements must be resolved before expanding digital health infrastructure at pace. The pace of government digitisation was a



real cause for concern; the health sector was not seen as ready for a "big digital one-stop shop." AI was flagged as an emerging risk that could amplify existing vulnerabilities if governance frameworks are not strengthened now.

129. We have already strongly recommended to Health NZ that it needs to engage directly with the community and ensure that the proper foundations are in place before implementing its new vendor-neutral digital solution for health portals in Northland. We reiterate that recommendation here, and note that we received feedback that co-design with Māori would be particularly beneficial. There is a specific opportunity to conduct this engagement as part of Health NZ's action plan, and Health NZ should ensure that it is done.

130. We also recommend that Health NZ should expressly include Māori data governance considerations and assessments 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.



4 A key problem: patient knowledge about the portal

The relevant law

131. Any health agency that collects health information needs to comply with rules 1-4 of the Code.

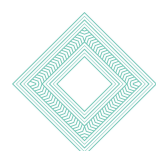
132. Rule 1 states that health information must not be collected by a health agency unless:

- (a) The information is collected for a lawful purpose connected with a function or activity of the health agency; and
- (b) The collection of the information is necessary for that purpose.

133. Rule 2 requires health agencies to collect health information directly from the individual concerned, unless one of the exceptions applies. The only potentially relevant exception to the collection of information in the portal at or before the time of the breach would be rule 2(2)(a) which allowed indirect collection if the individual concerned has authorised the collection of the information from someone else, having been made aware of the matters in rule 3(1). This does not exactly equate to the Māori data governance principle of free, prior and informed consent (for example because it focuses on the individual rather than including the collective). However, the way in which rule 2 is worded comes close.

134. Rule 3(1) requires an agency to take any steps that are reasonable in the circumstances to ensure that the individual concerned is aware of:

- (a) the fact that the information is being collected; and
- (b) the purpose for which the information is being collected; and
- (c) the intended recipients of the information; and
- (d) the name and address of—

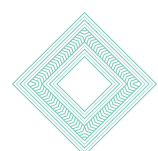


- (i) the health agency that is collecting the information; and
- (ii) the agency that will hold the information; and
- (e) whether or not the supply of the information is voluntary or mandatory and if mandatory the particular law under which it is required; and
- (f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and
- (g) the rights of access to, and correction of, health information provided by rules 6 and 7.

135. Rule 9 of the Code is also relevant. It states that:

- (1) A health agency that holds health information must not keep that information for longer than is required for the purposes for which the information may lawfully be used.
- (2) Subrule (1) does not prohibit any agency from keeping any document that contains health information the retention of which is necessary or desirable for the purposes of providing health services or disability support services to the individual concerned.
- (3) This rule applies to health information obtained before or after the commencement of this code.

136. Any agency or individual that is defined as a “provider” is also governed by the Health (Retention of Health Information) Regulations 1996 (“the Regulations”). These regulations require any providers (including health practitioners) to retain patient health information for a minimum of 10 years from the date of last contact with the patient. Where the Regulations apply, therefore, they provide a clear definition of how long health information must be kept for under rule 9 of the Code.



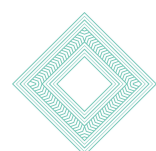
137. However, we have confirmed with the Ministry of Health that MMH is not considered to be a “provider” as defined in clause 4 of the Regulations. The services that it is providing only relate to the management of health information. In contrast, the services that are referred to in clause 4(k) of the Regulations relate to the provision of health or disability advice and support. MMH explicitly does not provide health or disability advice, treatment or support.

138. This interpretation is supported by the fact that the purpose of the retention provision in the Regulations is to ensure that health information is available when it is needed for patient care. MMH only stores a permitted snapshot of information that is held by GP practices or, in the case of the Northland information, by the relevant hospital. That snapshot differs from practice to practice and is provided for the convenience of patients. The MMH information is not a ‘source of truth’ for health practitioners to use when providing advice or treatment to patients; health practitioners look to their own, more complete records. It therefore does not in any way frustrate the purpose of the Regulations if information is deleted from a patient’s MMH account (as MMH has permitted patients to do for a long time).

Many people were fully aware of MMH

139. The most common process to create an MMH account is through the patient’s GP practice. Briefly, it works as follows:

- The patient enrolls in a GP practice that is a licensed MMH user. Information about MMH is included in the enrolment form or package, or is provided in separate communications with patients. The GP practice conducts any necessary patient identity checks at the time of enrolment.
- An authorised person in the GP practice creates a patient account in MMH. The patient information in this basic account is: email address, first and last name, date of birth, NHI (optional but usual), practice name, the type of



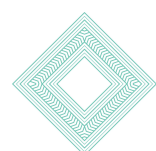
identification sighted by the medical practice (eg a passport or drivers licence) and number. At this point, the account is classified as “**registered**”.

- The creation of the basic account triggers an automated message from MMH to the patient’s email address or phone inviting the patient to activate their account, and explaining how to do this.
- If the patient wishes to use the MMH portal, they activate their account by verifying their details, accepting the terms of use and privacy policy, and setting a password and any multifactor authentication credentials (which were optional before the breach and are now mandatory). At this point, the account is classified as “**registered and activated**”.
- MMH can see whether a patient has activated their portal account. The GP practice can also see this, as the MMH logo on the GP practice management system changes from yellow to green.
- A patient cannot view any information in their account until they have activated that account.

140. GP practices that join MMH can bulk-enrol their existing patients. In such cases, the GP practices would have to send a specific communication to patients, with an explanation about the portal so that patients are aware of what is happening. However, the information supplied to MMH and the activation process is the same.

Enrolment during Health NZ’s Northland project

141. Early in the project, particularly at the pilot stage, a dedicated staff member at the hospital was available to support patients to self-register with MMH while they were still on the wards that were being used for the pilot. This included answering any questions the patient had about the service, providing a pamphlet about the portal, and encouraging them to activate their account. The staff member would assist with activating the account if the patient had their

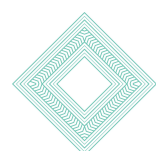


device with them in hospital. At this time, MMH did not run a match between the hospital information and existing portal accounts: instead, the staff member had administration rights (similar to those that GP practices have) to link the patient account to the new “Northland Hospitals MMH” practice. (If the patient also had an account registered through their GP practice, their MMH account would display information for both practices). Linking the account to the Northland Hospitals MMH practice enabled their information to be transferred through to the portal.

142. However, routine 1:1 support became unsustainable once the project was rolled out to more wards in the hospital, though it still happened from time to time. Pamphlets were also provided to patients and informational posters were on display to advertise the portal service. Some staff instructions and training were provided in case patients had questions. An important technical change was also made at the ‘back end’ of the system. Northland hospital information was forwarded to an MMH storage repository, which then ran a match against patients with MMH accounts. If a match was found, the information would be automatically imported into the patient’s account in the portal. As we will discuss in the next section, there were unfortunately some significant flaws with the match process that resulted in information being stored in the portal even when patients had not activated their accounts, or – in some cases – did not have accounts at all.

143. Health NZ paid the MMH licence fees for all Northland GP practices that were involved in the portal project to become or to remain MMH users, so that GP practices would enlist their own patients into the portal. Health NZ then actively promoted the service to GP practices and to patients.

144. We have viewed substantial amounts of information that Health NZ supplied about the project and about the MMH portal. This includes regular updates on what was happening, information about MMH and the portal, a presence at roadshows and so on. Primary healthcare providers, including Māori, were also

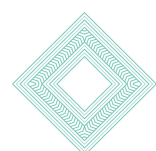


represented at the governance level on the project.

145. We accept that the small team in charge of this project at Health NZ made a significant and good faith effort to ensure practices were aware the service existed. We also accept that they did their best to provide information to enable GP practices to offer their patients an informed opportunity to engage with it, and actively considered issues relating to equity.
146. However, the reaction to the breach shows that there was still a significant knowledge gap about the portal and how it operated. As part of its action plan to roll out a vendor-neutral digital portal solution in Northland next year, Health NZ might therefore usefully consider engaging a navigator to work with Northland practices and whānau, to explain how the solution works and what their rights are. Particularly in a region such as Northland with a very high Māori population, such an approach might better fit with the Māori data governance model (particularly requirements for free and informed consent) and would be a practical and positive way to rebuild trust in health portals.

Self-registration

147. At the time of the breach, MMH enabled patients to self-register for the portal. Patients had to supply their email address, first and last name, date of birth and mobile number. They also had to identify the health facility to which they are attached. They then received an activation offer from MMH (as detailed above) and could proceed to activate their account.
148. MMH does not conduct any separate identity verification if a patient self-registers. Its control for identity verification is the fact the patient has to identify the health facility to which they are attached. MMH relies on the practice to notify it if the patient is not in fact enrolled or if the patient's identity cannot be established. If a patient does not identify a health facility, or if a practice cannot confirm that the patient is registered with them, the portal account cannot be activated.



149. Prior to the breach, patients could also self-upload documents into their MMH portal account. In fact, many thousands of affected patients had done so. The ability to self-upload documents was removed on 3 June 2026, as part of the remediation programme following the breach.

150. As a result of these standard processes, many people who were affected by the breach were aware that they had an MMH account and were current users.

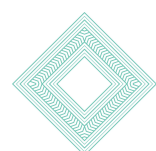
- They had been signed up through the normal process with their knowledge and agreement by their GP practices or had self-registered (either independently or with the assistance of hospital staff)
- They had activated their accounts.
- In doing so, they had at least received and acknowledged the information provided about the portal (though, as with any 'click to accept' process, there is no guarantee that they had read it).
- They then continued to use the portal to access their own information, access health-related resources or link with their health professionals. 8,566 affected people had also uploaded their own information into MMH, which demonstrates they were active users at least at one time.

151. Issues about whether that authorisation was fully informed, and issues about retention of information may still have arisen for those people as a result of the lack of clarity about the terms and conditions on which the portal operated. The discussion and recommendations below are therefore still relevant.

152. However, we focus first on the many people who had no idea that they had an MMH account, and therefore who had no ability to make informed choices or exercise control over their information.

Many people were taken by surprise

153. Early in the inquiry, it became obvious that many thousands of patients



appeared to have no idea that they still had – or, in a large number of cases, that they had ever had – an MMH account or record against which their information might be stored. This lack of awareness has been confirmed by our subsequent discussions with complainants, our Northland hui and other GP practices and representatives, as well as through media or online commentary. For example, several GP practices wrote to tell us that they had no idea how information about their patients could still have been stored in MMH when the practice had not used MMH for years.

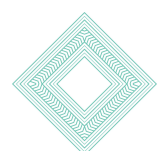
154. It is not possible to put an exact figure on how many people may have been taken by surprise, but the fact that MMH did not appear to have contact details for around 47,000 affected people suggests that at least that number are likely to have been unaware of their accounts. All people with activated accounts have, by definition, provided their contact information.

155. This is an extremely large number, particularly as the whole purpose of the MMH portal is to enable people to access their own information. If people do not know they have an account or are unable to access it, that purpose is frustrated. For Northland patients in particular, the whole point of Health NZ's project was to enable people to access their hospital information through the portal.

Why people were unaware

156. There appear to be several common reasons why patients were taken by surprise:

- a. They had received an invitation at one time to activate their account with MMH but had never done so, and thought no more about it.
- b. They had never known that any information about them was stored in the MMH portal.
- c. They had activated their account at one stage, but had not used it for a long



time, and had either forgotten about it or thought it had lapsed.

- d. They had moved practices, and their new practice used a different portal to MMH – the patient did not realise that their information would still be in MMH.
- e. Their practice had stopped using MMH and was now using a different service – again, the patient did not realise that their information would still be in MMH.

157. Each of these scenarios raises questions about the extent to which patients authorised the initial creation of their account, and the ongoing collection and storage of their health information in that account. We deal with them in turn below.

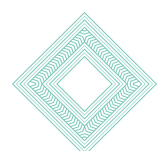
Scenario (a) – patients who had never activated their account

158. As highlighted in Phase 1, there was a flaw in the match process that MMH conducted when Health NZ forwarded hospital information for processing. That information was imported not only into activated patient accounts, but also into registered but non-activated accounts. This meant that many patients were affected by the breach without ever having activated their accounts.

159. MMH remediated this flaw in January 2026, by updating the match criteria to only import information into activated accounts. This was a responsible thing to do, but it was too late to protect people who had been affected by the breach. The share of hospital information also stopped altogether in late May 2026, so there are no chances that the problem is continuing.

160. We have already found Health NZ at fault under rule 5(1)(b) of the Code because it should have had stronger risk management processes that expressly considered the match criteria. Having specific contractual terms would also have helped.

161. We have received assurances from both MMH and Health NZ that MMH has



now deleted all Health NZ hospital discharge information from non-activated accounts. We are satisfied with the evidence provided.

162. However, we also consider that one of the lessons we can learn from this incident is that there is no ongoing purpose to maintain registered but non-activated accounts at all, once patients have had a reasonable opportunity to decide whether to activate them. It is our view that keeping accounts past this point would be a breach of rule 9 of the Code. As this breach demonstrates, even holding the relatively small amounts of personal information in ‘stub’ accounts awaiting activation can create privacy risks if there is a breach of the portal. Some affected patients were more concerned by the loss of their name and contact details than they were about the loss of their relatively innocuous medical information.

163. We therefore recommend that MMH implement the following process to delete any non-activated accounts, in order to fully comply with rule 9 of the Code:

- if a patient has not responded to an activation email within a month, MMH must send them a reminder; and
- if the month elapses without the patient activating the account, MMH must notify the patient that the account will be securely deleted at the end of a further month unless they take action.

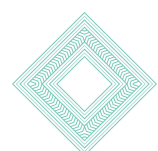
164. This process would mean that information would not be held in non-activated accounts for more than three months. It mirrors the process MMH has established for dormant accounts, as discussed below. It should therefore be practical and straightforward to implement.

165. We also recommend that Health NZ should pay particular attention to account creation and activation as part of its roll-out of its new solution during 2027. While Health NZ stopped sending hospital information to patients through MMH in May this year, it is important that lessons are learned from what happened so that that these types of issues will not recur.

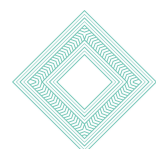


Scenario (b) - patients who never had an account

166. Even more pointedly, the inquiry has shown that many patients never had an actual account in the MMH portal at all - not even a 'registered' but unactivated account. This was another flaw in the match process that MMH conducted when Health NZ forwarded hospital information for processing.
167. The patient portal is not the only service that MMH offers to health facilities and patients. For instance, MMH also provides an IT system to transfer electronic healthcare records between practitioners. This is known as the shared electronic healthcare records system, or "SEHR". This transfer does not require the patient to have an account: if they do, the information may be visible through their portal, but for others, it simply operates as an IT pipeline. However, to enable the transfer to happen accurately, the MMH system needs to hold the patient name, NHI, and details of the sender and recipient health facilities, so that SEHR information is associated with the right person and is transferred to the intended healthcare professional.
168. No patient email is associated with these records: there is therefore no means of MMH contacting the patient to let them know the information has been transferred. MMH relies entirely on the health practitioners to provide information to patients about the SEHR service and gain any necessary patient authorisation.
169. Whether this always works successfully is an important privacy question, but it is outside the scope of this particular inquiry as SEHR records themselves were not affected by the breach.
170. However, we recommend that GP practices and specialist health practitioners take this opportunity to check that patients are properly informed about how the SEHR system operates and, where necessary, obtain patient authorisation to transfer that information.



171. Similarly, patients can use MMH to book appointments with their GP through the Easy Booking service. In the past, this did not require the patient to have an MMH portal account (this was changed at the end of 2024). However, basic patient information needed to be stored so that the patient's appointment request could be transferred to the right GP practice, and the patient could be told of the time and date of their appointment.
172. MMH – understandably – does not classify these patient records as portal 'accounts'. A portal account exists to make information available to the patient but the purpose of these services is different. The patient may not know MMH records any SEHR information about them at all, and may not know what MMH holds as a result of the Easy Booking service. In relation to SEHR records, they are not provided with MMH's terms of use or privacy policy and are not asked to agree to them. The patient also cannot see the records if they have not activated their account. The same was true for Easy Booking records prior to the change at the end of 2024 which required users to have an account.
173. If a patient does not have an activated MMH account, no detailed information or documents should be stored on the portal at all. Such collection and storage clearly exceeds anything that the patient could have been said to authorise. The information should simply be transferred to the clinician's patient management system as usual.
174. Here, when MMH was processing the hospital information on behalf of Health NZ, the process not only matched the patient details on the hospital information against actual patient accounts (both activated and non-activated), but also matched them against any patient details that had been set up to enable SEHR transfer or Easy Booking. If the patient details were on the system, the hospital information was imported into the portal and was stored in the My Health Documents module.
175. We consider that this was a fundamental mistake. The information should not have been imported into the portal simply because it matched an SEHR or



Easy Booking record. This was inconsistent with the purpose for which those records were created and resulted in the information being held in the portal, where it was subsequently accessible to the hackers.

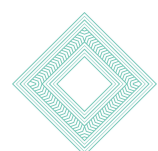
176. We have found that Health NZ had no knowledge that hospital information was being matched against patient records created for the SEHR and Easy Booking services and cannot be said to have agreed to it. If Health NZ had properly considered the match process and match criteria, it should have identified the problem, but, again, that falls within matters that were already addressed in phase 1. For the purposes of this part of the inquiry, it is enough to say that we consider that MMH made the decision to match and import information based on the SEHR or Easy Booking records.

177. There is no suggestion that MMH used the information in any way – we accept that it did not. But taking this decision meant that MMH was acting on its own account in terms of the Code. It was therefore directly responsible under the Code for the collection of that information.

178. There was no legitimate purpose for MMH to import Northland hospital information into the portal as a result of matching it against SEHR records or Easy Booking records that were not associated with activated accounts. The point of the portal project was to make information available to patients. That is only possible if the patient has activated their account (or, here, has an account to activate). We therefore consider that importing that information using SEHR and Easy Booking records as match criteria was a breach of rule 1 of the Code.

179. In addition, MMH was collecting information from a source other than the patient themselves. None of the rule 2 exceptions apply here. In particular, we consider that it cannot be asserted that a patient authorised MMH to collect their Northland hospital discharge information when there was no activated account.

180. In coming to this conclusion, we have drawn a distinction between the two



points in the portal creation process at which patient authorisation can be said to occur. This distinction will be useful to note for other agencies that operate in a similar way.

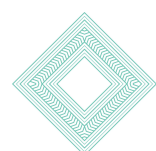
Initial “in principle” authorisation

181. Normally MMH, quite reasonably, relies on the frontline healthcare practitioner (whether a GP practice or the hospital), to have an initial conversation with the patient about whether they wish to use the MMH portal and what information will be sent through to it. MMH has no contact with a patient at that point. It can, and does, provide information that the healthcare practitioner can supply to patients; for example, it collaborated with Health NZ on the messaging to be given to patients. But any initial authorisation to set up an MMH account needs to be obtained by the health practitioner.

182. However, we consider that this is only an ‘in principle’ authorisation and it does not extend to collecting detailed medical information in the portal. It can only be said to extend to authorisation to supply the patient’s name, contact details and medical centre information to MMH to set up the ‘stub’ account that will then trigger an invitation to activate the account. Clauses in the documentation provided to users that state that users are solely responsible for gaining patient consent are therefore not completely correct (see for instance clause 9.3 in the new [business terms and conditions](#)). It is a shared responsibility.

Lack of activation is lack of authorisation

183. This is because the second point of authorisation – activation – is entirely controlled by MMH. This is when patients first see and have to agree to the terms of use and privacy policy (the documents that are supposed to provide the information required by rule 3(1) of the Code (or, since 1 May 2026, by rule 3A(1) of the Code). The contents of the terms of use and privacy policy are determined by MMH; health practitioners have no control over them.



184. So while the patient might have given their GP or hospital staff member an initial indication that they might be happy to have a portal account, we consider that it is only when they receive and agree to MMH's terms and then activate their portal account that they can be said to have fully authorised the collection and storage of further information into that account.

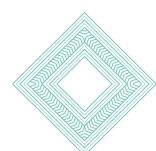
185. This second, and key aspect of consent was missing when MMH matched the hospital information against SEHR and Easy Booking records that were not associated with activated patient accounts. We therefore consider that it breached rule 2(1) of the Code.

186. MMH has formally confirmed that all Northland hospitals' information that is not associated with an activated account has been deleted. This occurred before the end of May 2026. MMH has therefore fully remediated the issue and we do not need to take further action.

Scenarios (c) - (e): the patient was unaware that they still had an account

187. It appears to have been common for patients to be entirely unaware that their MMH portal account would persist even if they moved to a GP practice that used a different portal, or if their existing GP practice stopped using MMH and switched to a different provider. Our discussions with GP practices and peak bodies also suggest that GPs were also often unaware that their patients would continue to have an MMH account even when the practice as using a different portal provider. For example, after we wrote to affected GP practices to let them know that they did not need to individually notify our Office about the MMH breach, some told us they did not know how patients could have been affected since the practice had not used MMH for several years.

188. MMH does provide detailed information in its terms of use, privacy policy and business terms and conditions. For example, at the time of the breach, those documents indicated that patient accounts would persist if the patient moved



practices. In particular, clause 3 in the June 2024 terms of use (which applied at the time of the breach) stated that:

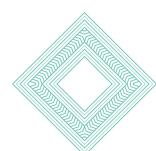
If you change GP practices or otherwise disengage from your GP practice, you will still remain registered with ManageMyHealth™ and you will still be bound by these Terms of Use. You may use ManageMyHealth™ in connection with any new GP practice you register with, if that practice also uses ManageMyHealth™

189. MMH's consistent position – as also evidenced from its discussions with Health NZ and its privacy risk assessments – was therefore that it was clear that only patients could cancel their account, and that they knew this when they stated they accepted the terms of use and privacy policy. The GP practice could not cancel the account for them. If the patient did not cancel the account, it would persist. MMH relied on users reading these documents to understand how the portal operates and what their rights and responsibilities are, including rights about retention of patient information.

190. We had some concerns about the clarity of that information which have now been addressed (at least to a large extent) in further updates made by MMH. However, we accept that MMH's policy that only patients could delete accounts usefully provided patients with control and autonomy over their own information. MMH operates as a separate repository of client information and providing maximum client control is something we support. The problem here is that the breach has demonstrated that the persistence of the account becomes unhelpful – even very risky – if the client does not know, or forgets, that the account continues to exist unless they take active steps to cancel it.

191. This raised two practical and legal questions:

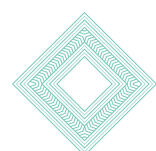
- what happens to accounts that have not been used for a long period of time (“dormant accounts”)
- were the terms of use and privacy policy clear enough to meet the



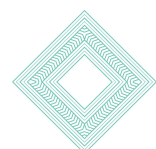
requirements under rule 3(1) of the Code, to give patients the information they needed to understand what they are agreeing to.

Dormant accounts

192. At the time of the breach, MMH had a process to identify dormant accounts where the patients had not signed in for two years. That process involved contacting the patient and asking whether they still wished to have an account or whether they wished to delete it. A reminder would be sent if MMH did not hear back and then the account was supposed to be deleted if the patient still did not respond, or confirmed that they did not wish to have the account any more.
193. It is unclear whether this process always worked successfully. We received anecdotal information from one GP practice that at least some of their affected patients had not used their accounts since the practice moved from MMH on a defined date more than two years previously, and yet their patients had not received any reminder messages from MMH. The number of affected patients who were taken by surprise that their accounts still existed after several years (including those who might have signed up during the early stages of the Northland project, or those who had self-uploaded documents) could also suggest that the dormant account process did not always operate as well as intended.
194. Even if that process functioned perfectly, however, we consider that two years was too long for MMH to continue to hold health information for the purpose of making it available to the patient (which is the sole purpose of the portal). We consider 12 months to be the maximum amount of time an account should be inactive before the patient is asked to confirm whether the account is still needed.



195. We therefore consider that, at the time of the breach, MMH's dormant account process breached rule 9 of the Code.
196. Since the breach, MMH had already independently recognised that two years was too long a time to leave before contacting patients about dormant accounts. It has now reduced that time to 12 months as part of its remediation plan. Its new dormant account process was finally implemented by June 2026 and is now reflected in clauses 3.4 - 3.7 of its new privacy policy (published on 30 September 2026).
197. According to clause 3.6, a patient receives a reminder after 12 months of inactivity where that account is no longer linked to an active practice on MMH. If the patient has not taken action or responded after a further 30 days, MMH sends them a reminder that warns them that unless they confirm they wish to maintain the account within the following month, their account and all the information in it will be deleted. The longest an account will persist when an inactive patient is not attached to a practice using MMH is 14 months.
198. Deleted information is retained in MMH's backups for 14 days and is then overwritten and irretrievable.
199. Also, according to clause 3.4 of the new privacy policy, when a healthcare provider stops using MMH, MMH will let the patient know within 30 days to advise them of the change. That is helpful for patients and would have prevented some of the issues that arose with the breach. However, there are two problems.
200. First, clause 3.4 also states that if the healthcare provider stops using MMH, all health information accessible through MMH will be removed and the patient will no longer have access to it. This appears to remove patients' ability to choose to maintain their MMH account if they wish to do so. Such a clause would be appropriate for a portal that only operates as a look-through system into the GP practice's patient management system. However, MMH operates as a stand-



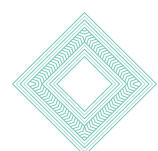
alone store of copies of health information. Patients may like to continue to have easy access to those past records. This particularly applies to information that patients had uploaded for themselves (before the ability to do so was removed). MMH intends to delete that information after a 'sunset' period during which patients will have the ability to access copies of that information for themselves.

201. It is up to MMH what their reasonable terms and conditions should be, provided that they comply with the Code and other relevant legal frameworks. This proposed deletion would do so. Also, since patients can no longer self-upload documents, it will probably be relatively rare in future for patients to be disadvantaged if information is simply deleted. They will still be able to see or obtain all their information through their GP or their hospital (subject to any difficulties in being enrolled in primary care, which is a particular issue in more remote regions such as Northland), or other original information source.

202. The proposed clause does not create issues with Privacy Act compliance. But for whatever time MMH operates as a standalone repository of information, (the purpose of which is to provide the patient with easy access to their information), we suggest that it should consider whether it would be better customer service to offer the patient a choice to retain their account, if they have a reason to do so. An example is lab test results shared by Northland hospitals, which were not necessarily being copied to the patients' GP practices. The decision to remove any information on the grounds that it is no longer necessary or relevant to keep it appears to relate more to the company's desire to reduce its information holdings rather than driven by whether the patient still has an ongoing need for that information.

203. For Māori patients, offering a genuine choice about what happens with their data is also necessary to be in line with the Māori Data Governance Model.

204. Secondly, and more importantly, the process does not apply to accounts that have been dormant for 12 months but where the patient *is* still attached to a



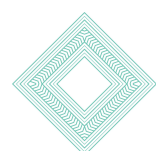
practice that uses MMH. Clause 3.7 of MMH's updated privacy policy states that the period before an account is considered dormant is still 24 months. We consider this is too long. Patients who do not visit their doctor frequently or check their medical records may forget that they have an account and may be unaware what is in it. We consider that *all* patients with accounts that have been inactive for a year should receive a reminder and have the account deleted if they fail to respond or do not choose to maintain it. Annual confirmation that they still wish to maintain an account that contains their sensitive personal health information is a reasonable step to take, in line with rule 9 of the Code.

205. A failure to manage all dormant accounts appropriately is likely to be a breach of rule 9. We recommend that MMH amend its dormant account settings to apply to **all** patients with accounts that have been inactive for a year.

206. Twelve months is still a long time to manage the risk that the patient forgets about the account or no longer wishes to use it. However, on balance, it is probably the most practical option. That time period avoids annoyance to customers by asking them to reconfirm their accounts too frequently and also ensures information is not kept when there is clearly no need to do so. Patients can still ask for deletion of their account at any time if they no longer wish to use it (see clause 3.1 of the new privacy policy).

207. As a wider lesson from this inquiry, the management of dormant accounts is an issue of general importance, beyond health sector providers. It is common for customers to create accounts for specific purposes (eg to buy a product or service). Once that purpose has elapsed, they may forget they have the account.

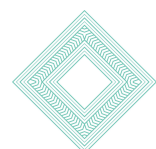
208. All agencies that operate customer accounts should therefore have a process to identify and manage 'dormant' accounts. We would expect this to be standard best practice. What that process is, and whether information can be kept will vary between agencies. It will be determined by any laws that require



retention of information, and by any lawful ongoing purpose for retaining it. However, we consider that in many cases best practice would be to verify annually that the customer still wishes to keep the account.

The terms of use and privacy policy have been updated

209. Before a patient can be said to have genuinely authorised the collection and storage of their information in the MMH portal, they need to have received clear information about how that information will be handled and what their rights and obligations are. This information is set out in rule 3(1) of the Code. The purpose of rule 3 is to promote openness and transparency by enabling individuals to understand how their health information is collected and managed, so they can make informed decisions about their engagement with health services.
210. We commented in our phase 1 report on the fact that MMH's terms of use and privacy policy at the time of the breach were unclear about the uses to which the patient's information could be put. This report has shown that people were not always told that their information was being collected at all or why. The fact that core conditions such as the continued existence of the patient's account were buried in amongst other terms also led to a lot of confusion about what patients' rights were. For patients who had activated their accounts, the documentation technically ticked the boxes in rule 3(1), but it failed to provide actual meaningful information to patients and practices in an accessible way.
211. Agencies that rely on authorisation as a legal basis for collection, use or disclosure of personal information need to be particularly careful to ensure that their terms of use are easy to understand.
212. MMH updated its new [terms of use](#), [privacy policy](#) and [business terms and conditions](#) on 25 June 2026. The timing and content of these changes may indicate that they were, at least in part, intended to address issues identified following the breach, including the management of retention and deletion issues.



213. We advised MMH that that exercise had only been partly successful – for example there was now a specific section on account closure which enabled users to find that information easily. However, we considered that there were still inconsistencies between different clauses in different documents, the documents were hard to navigate and in several instances were unclear (for instance, what information was “practice data” and therefore in the control of the GP practice or other healthcare provider, and what information was “patient data” that the patient could exercise choices over). As part of our consultation with MMH on the draft Phase 2 report, we recommended that it review these documents again, particularly as they purport to be core terms of the contract that users enter into with MMH.

214. MMH has now revised the terms of use, the privacy policy and the business terms and conditions further. Those updated documents were published on 30 September 2026.

215. We agree that MMH has made improvements with the later updates, but we have not considered those documents again in more detail, as it is not our role to provide detailed advice or approval to MMH. The best judges of whether the documents are now sufficiently clear will be the people who have to agree to them.

216. We therefore recommend that MMH conduct a range of user testing on its documentation to check what people understand and what remains unclear. It will then be in a position to amend those documents to work better.

217. Finally, we also recommended that MMH amend clauses in their documentation that attempted to restrict liability for breaches caused by a criminal attack on its systems, for events beyond their control, or for accidental or unauthorised access to the patient’s information. To its credit, MMH accepted our recommendation and removed the clauses from its documentation.

218. This is not the only instance that we have seen where these types of clauses



are included in contracts, and we advise other agencies to review their documentation to make sure that they are not making a similar mistake. Such clauses are legally invalid and misleading in terms of the Act (and therefore may be unenforceable in contract law as well). Whether an agency is liable for a security breach under the Act or the Code depends on whether it had reasonable security safeguards in place as required by IPP5 or rule 5. The fact the attacker was criminally motivated is immaterial. It also does not matter if a customer had supposedly accepted the conditions in these clauses. Agencies cannot 'contract out' of most of their obligations in the Act or Codes of Practice under the Act, including security obligations.

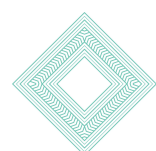
Residual issues – children, young people and deceased people

219. The breach also raised questions about how accounts relating to children, young people and deceased people were handled. Since they do not raise separate issues to the ones already discussed above, we cover them only briefly here, for the sake of completeness.

Children under 16

220. We would not expect children under 16 to be specifically made aware of the portal, as any MMH account will usually be linked to their parent or guardian's account. It is their legal representative who engages with their health information on their behalf, and who would authorise the creation of that account and set up credentials to access it.

221. We know that children's information was impacted by this breach, and we would expect that some parents would have been unaware that the account still existed. As [OPC's Children's Privacy Project](#) makes clear, we expect particular care to be taken with children's and young people's information. Here, the reasons for that lack of awareness, though, are likely to be the same as listed above, and therefore do not raise new issues around consent or transparency.

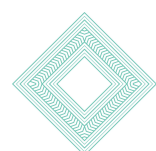


Young people 16 and older

222. Once a child turns 16, MMH's business terms and conditions at the time of the breach required GP practices to de-link the child's MMH account from their parent's account and approach the child to set up a new independent account. MMH has now clarified that there is an automated process to de-link accounts, but this relies on the GP practice noting the age at which the account should be de-linked (in some cases, this may occur at younger ages).
223. We have heard from several GP representatives that it can be difficult to engage with young people to set up a portal account once their child account is de-linked, as it is not top of mind for them. That is an indication that the expected cancellation and re-registration process normally works successfully.
224. Again, we know that many young people over 16 were affected by the breach and some of them will probably have been unaware that they had an MMH account. However, we do not have any evidence that that was because their accounts had not been properly cancelled when they turned 16. If so, that would certainly be a problem.
225. We recommend that GP practices use this opportunity to check that they have accurately specified the age at which a child's account should be de-linked (with the maximum age usually being 16 unless the parent continues to be the legal representative, for instance because of capacity issues). This is essential to make sure that parents do not have unauthorised access to young people's health information once the parent is no longer a legal representative.
226. For the purposes of this inquiry, though, we presume that young people's lack of awareness about their account was likely to be for the same reasons an adult might have been unaware.

Deceased people

227. We do not have any specific evidence that information from deceased persons' accounts was stolen in the breach but given the scale of the information theft, it



would be surprising if that was not the case.

228. One representative of a deceased person contacted us about their concerns with the process to deal with MMH accounts. We therefore asked MMH how it finds out that a person has died, what it does with the information and what support is available for representatives.

229. MMH stated that it becomes aware that an account holder has died when the patient's health centre notes the patient as deceased in its patient management system. The information is then synchronised to the MMH portal, which updates the patient's enrolment status to "deceased".

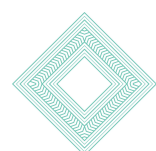
230. It does not appear that MMH takes any active steps to contact the representative of the deceased person (such as the executor, or administrator of the estate). It would not have contact details to be able to do so.

231. However, representatives can contact MMH's customer care team about the patient account. The customer care team confirms identity information for both the patient and the representative, to ensure that the person is entitled to deal with the account. It also verifies the 'deceased' enrolment status with the patient's health centre. Once confirmed, it will take instructions from the deceased person's representative about what should happen with the account, including closing that account if desired. If the representative wants access to the health records, though, MMH directs them back to the health centre, since it is responsible for the patient's clinical record.

232. Alternatively, the representative can simply contact the health centre and ask for the account to be closed through the patient management system. The MMH system allows authorised health centre users to make this change.

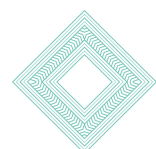
233. While this process sounds simple enough, there were some problems.

234. First, there was no mention in the terms of use, business terms and conditions or privacy policy of what happens when an MMH account holder dies. There



also did not appear to be any information in the FAQs on the website. There was plenty of information about children's accounts, but nothing to help representatives of deceased people. We recommended that MMH should update the documents to address this. They have accepted this recommendation and included information for representatives of deceased people in clause 3.10 of its updated privacy policy. The Accounts and Privacy section of MMH's FAQs now also set out information about deceased account holders.

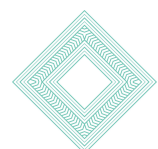
235. Secondly, a representative may never have known – and may never think to ask – whether the deceased person had a health portal account and if so what would happen to it. While the dormant account process would be triggered after 12 months of inactivity, this is a long time for a deceased person's information to remain in the portal without instructions from a representative. We also consider that reminder emails to the deceased person's email account after a year of inactivity would be likely to create distress to surviving relatives (most often a surviving spouse) who have access to that email account.
236. Both problems were avoidable. When a patient's MMH enrolment record notes that the patient is deceased (through the automated synchronising process), this should trigger a query to the patient's health centre, noting that the patient account exists, that it has been suspended pending instructions from a representative, and asking the health centre to inform the representative that the account exists and how to get in touch with MMH.
237. We consider that if the representative has not been in touch with MMH for a period of three months after the person has died, the account should be deleted, provided that none of the information in that account was uploaded by the patient themselves. All other information is merely a duplicate of information that is held on health agency systems and representatives would be able to access the information from there as usual.



238. MMH has now updated its process in response to deceased account holders.

Clause 3.10 of the updated privacy policy states that MMH will permanently delete an account once becoming aware the account holder is deceased, if no representative has contacted it within 90 days.

239. We note in passing that since MMH is a health agency, it is not entitled to decline a request for access to information by a deceased patient's representative. Section 22F(1) of the Health Act 1956 requires all agencies that hold health information to disclose information to the person's representative on request. Once MMH is satisfied of the representative's identity and their ability to represent the estate, it therefore has no lawful basis for declining a request. We encourage MMH to review its access request processes to make sure they are fully in line with the Code and the Privacy Act.



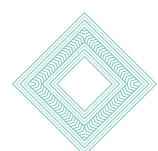
5 Breach management

240. This section of the report focuses primarily on the lessons that other agencies can learn from what happened during the MMH breach. As with many major breaches, the MMH breach presents us with a valuable ‘use case’ that illustrates how the law works and what this Office’s regulatory expectations are for compliance with the Act and the Code. Most importantly, though, it draws on what went right and what could be improved to provide insights on how to manage breaches successfully in future.

Fault is not the point for notification

241. Breaches can be – and often should be – big news, and, where justified, agencies should certainly be held to account. Public coverage is also an important means of getting information to the right people quickly. When a major breach happens, it is also inevitable that public commentators and affected people will focus on whose fault that breach might have been.

242. However, it is important not to jump to conclusions. First, speculation about cause and liability and size of a breach can cause unnecessary anxiety to clients of the affected agency. We recommend that commentators should be sensitive to the impact of any coverage on those people. Secondly, speculation about vulnerabilities in a system can create additional security risks to the information that continues to be held in the system. Cyber security and privacy breaches are an everyday part of our modern digital information environment. Sometimes – as we found in Phase 1 of this inquiry – it transpires that an agency could and should have done more to prevent the breach, and that failing to do so was a breach of the law that caused real harm to people. However, sometimes it turns out that there is nothing else that the agency could reasonably have been expected to do. Breaches can and do happen to agencies with strong security and privacy protections in place. However, the harm to people still exists and needs to be addressed.



243. The Act's breach notification provisions recognise this distinction. The Act's requirements do not depend on whether the agency was or may have been at fault. Instead, the main aims of mandatory breach notification are:

- to make sure that agencies proactively identify and address breaches in a way that prevents or limits further harm to individuals
- to enable people to know when their information has got into the wrong hands so they can take steps to protect themselves (for example, to change passwords, alert their bank to watch for suspicious transactions, be particularly wary about emails, boost physical security, seek help for any trauma the breach may trigger)
- to require agencies to be transparent with affected people, and inform them about what has occurred
- to incentivise agencies to prevent breaches in future
- to enable the Privacy Commissioner to develop a clearer picture of patterns of risk, that may indicate where improvements in privacy practice are needed (not only within an agency, but across a sector or broader aspects of the economy).

The legal requirements

244. As with many other jurisdictions, since 1 December 2020 the Act has required certain types of breaches to be notified to the Privacy Commissioner and – generally – to affected people.

When is a breach notifiable?

245. First, the notification obligation is only triggered when the breach is of a **type specified** in section 112 of the Act. These are largely security-related types of breaches. They either need to involve:

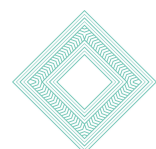


- unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of personal information held by an agency; or
- an action that prevents the agency from accessing the information on either a temporary or permanent basis (typically a cyberattack that locks the agency out of its own systems).

246. In other words, breaches of IPPs involving other aspects of privacy – such as collection, inaccuracy or failure to respond properly to requests for access to personal information – do not trigger the notification requirements. They are still breaches of the law, and the agency must take them seriously, prevent them from recurring and address any harm that affected people may have suffered. Affected individuals can also make complaints to the Privacy Commissioner. However, the agency does not need to separately and pre-emptively notify the Privacy Commissioner that something of that kind has gone wrong.

247. Secondly, the breach is only “notifiable” if it is reasonable to believe that the breach has caused or is likely to cause **serious harm** to the affected person or people. The Act does not define serious harm, but section 113 sets out factors that an agency must consider when it is assessing whether a privacy breach is likely to cause serious harm:

- (a) Any action taken by the agency to reduce the risk of harm following the breach
- (b) Whether the personal information is sensitive in nature
- (c) The nature of the harm that may be caused to affected individuals
- (d) The person or body that has obtained or may obtain personal information as a result of the breach (if known)
- (e) Whether the personal information is protected by a security measure
- (f) Any other relevant matters.



Notifying the Privacy Commissioner

248. If a breach meets the ‘notifiable breach’ definition, section 114 states that the agency **must** notify the Commissioner as soon as practicable after becoming aware that a notifiable privacy breach has occurred.
249. It is a criminal offence under section 118 to fail to notify the Commissioner without reasonable excuse – or to fail to do so as soon as practicable without reasonable excuse – regardless of whether the agency has taken steps in the meantime to manage the breach. The only defence is where it was reasonable in the circumstances for the agency to think that the breach was not notifiable.
250. The maximum penalty for failing to notify the Commissioner is \$10,000. Importantly, this is not a penalty for the breach itself: unlike similar jurisdictions, the Privacy Act does not currently include a civil penalty regime.
251. Section 117(1) sets out what has to be included in the notification to the Commissioner.
252. OPC generally expects that it will be practicable for the agency to notify the Office within 72 hours of becoming aware of the breach. This timeframe refers to actual days not to working days. As the MMH breach shows, breaches also happen at weekends and over public holidays and the risk of harm to individuals needs to be promptly contained. Agencies are therefore expected to have a reasonable degree of cover outside normal working hours to identify, assess and notify breaches quickly.
253. The time starts ticking once any member of the agency – including a staff members or contractor – becomes aware that a notifiable breach has occurred. This wording assumes some degree of assessment of the breach has first been done by a person familiar with the Act. However, in practice, it can be hard for agencies to argue that they are only aware a breach is notifiable once the privacy officer (or other responsible staff member) has had a chance to assess it. The majority of notifiable breaches are self-evidently serious. While there will



be some latitude for more ambiguous breaches, in practice the 72 hour guideline creates a useful bright line that enables agencies to establish sound breach management practices. This includes encouraging staff to report rather than hide breaches, and to make sure that breaches are immediately reported to an appropriate person in the organisation who can assess them and help to resolve them.

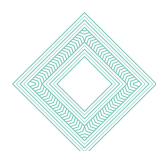
254. 72 hours is a guideline rather than a fixed rule. It gives time for agencies to report breaches up to appropriate staff for assessment and then to notify OPC promptly. However, in some cases, it may be obvious that a breach is notifiable and it may be 'reasonably practicable' to notify the Office on the same day the breach is discovered.

255. It will be relatively rare for a longer period to be appropriate before contacting OPC. Agencies that exceed 72 hours will at least need a solid explanation for the delay (for instance if they have had to make further enquiries to check whether a breach in fact occurred). OPC is clear that not all details of the breach need to be known before the agency notifies – such investigations can take days, weeks or even months. The Act provides for "incremental" notification. Delays can frustrate the policy purposes that underlie notification. The key is whether it is reasonable to believe that there has been a notifiable breach. If in doubt about whether the breach meets the serious harm threshold, OPC advises the agency to notify.

Notifying affected people

256. The Privacy Commissioner is not the only person who is required to be notified. Section 115 requires the agency to notify each affected individual. Section 117(2) sets out what needs to be included in that notification.

257. Again, the notification needs to be made as soon as reasonably practicable. However, that timeframe may well be different from the timeframe for notifying the Commissioner. With large scale breaches in particular, or breaches

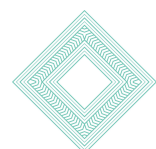


affecting large quantities of unstructured information, it may take longer than 72 hours to identify exactly who has been affected. Rushing notifications can also lead to people being incorrectly notified that they have been affected by a breach, or being provided with inaccurate information. As this breach has shown, this can cause unnecessary anxiety. A calm and measured approach is best, albeit fueled by appropriate urgency, so that people are equipped with the information they need about whether they are affected and what happened.

258. If it is not reasonably practicable to notify the person (for instance because the agency does not have contact details for people), the agency can issue a public notice instead. However, section 115(2) makes it clear that a public notice is a backstop provision only. While it is more time-consuming to do individual notifications, it is also more personal and responsible to communicate directly with people. It provides an opportunity to explain, to apologise and to assist. Direct communication is also far more effective: public notices can be easily overlooked, and also may make people think that their information is affected when it is not.

259. Importantly, a 'public notice' is different from website updates, media statements or other public comments that the agency may make about the breach. With breaches that are publicly known, the agency will have to make such statements in any case, and will need to provide updates and information as things progress. However, the fact the agency has made such statements does not remove the obligation to directly notify affected individuals. A true public notice is a last resort, once opportunities for direct notification have been exhausted and should be a specific communication targeted at the residual group of people.

260. There are some limited exceptions to the obligation to notify affected individuals. These are set out in section 116. An agency is not required to notify affected individuals at all – either directly or through a public notice – if the notification or notice:



- a. would be likely to prejudice New Zealand security, defence or international relations (s116(1)(a))
- b. would be likely to prejudice the ability of a New Zealand public sector agency to maintain the law (s116(1)(b))
- c. would be likely to endanger the safety of any person (s 116(1)(c))
- d. would be likely to reveal a trade secret (s 116(1)(d))
- e. relates to a child under 16 years of age and the agency believes that the notification or notice would adversely affect the child's interests (s 116(2)(a)). However, the agency must consider whether it might be appropriate to notify a representative instead (e.g. a parent, guardian or other person lawfully acting in the child's best interests (s 116(3))).
- f. after consulting with an affected person's health practitioner (where practicable), if the agency believes that the notification or notice would be likely to prejudice the health of the person (s116(2)(b)). Again, the agency must consider whether it might be appropriate to notify a representative instead, taking into account the circumstances of the individual and the breach (s 116(3)).

261. These are the only reasons that an agency can use to refuse to notify individuals. Contrary to popular belief, there is no general catch-all provision that allows an agency to think that notifying would 'cause more harm than good'. Such a provision would be highly subjective, and could too easily be used by agencies to avoid what can be expensive and time-consuming notification processes. If a breach is notifiable, it is already by definition a breach that is at least capable of causing serious harm to a person. The affected person deserves to be told.

262. Section 116(4) allows the agency to delay notifying the affected individual if the agency believes that a delay is necessary because notification could create



risks to the security of the information held by the agency and those risks outweigh the benefit of notifying the individuals. This is not an endless period. As soon as the reason for the delay no longer exists, the notification must be made. Agencies that are using this ground to delay notification must therefore frequently review whether the justification still exists. It also does not operate as a reason to delay notifying the Privacy Commissioner. The Commissioner's statutory secrecy obligations provide the necessary protections for the security of the information.

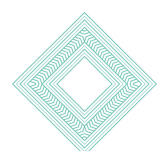
Did MMH and Health NZ meet the notification requirements in the Act?

263. Our inquiry has concluded that both MMH and Health NZ complied with the legal notification requirements in section 114 of the Act. Both agencies did in fact notify the Privacy Commissioner of the breach, and did so as soon as practicable, as required by section 114.

264. MMH notified OPC on 1 January 2026, less than two days after it became aware of the breach. The time in between was focused on fixing the specific breach pathway and making sure that no further information would be compromised. MMH mobilised quickly and well to manage the breach, despite the public holiday, including bringing in external specialist help to supplement its small number of key staff (some of whom were on leave).

265. While MMH successfully met its legal obligations to notify OPC, we note that on 1 January, MMH told our Office that it did not consider that the breach was one that could cause serious harm. This was clearly incorrect from even a brief consideration of the factors in section 115, as MMH was informed by the OPC representative on duty:

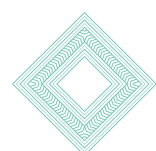
- Health information is inherently sensitive. The starting point would always be to consider that the breach would be capable of causing serious harm, unless other factors suggested that that harm would not eventuate.



- While the exact numbers of affected people and exact numbers of files would not have been confirmed at this very early stage, the hackers plausibly claimed that it was a large-scale breach. The affected area of the portal (My Health Documents) was known to contain large amounts of health documents about large numbers of people.
- Even if the breach had been restricted to the sample of information that the hackers published online, that sample clearly demonstrated that MMH documents containing health information had been stolen.
- That sample of health information was publicly available on the dark web where anyone could access, copy and reuse it without restriction.
- It was not protected by any security measures such as encryption.
- It was obvious that loss of even that sample of health information would cause distress – potentially significant distress – to at least some of the affected individuals.
- All the other information was still in the hands of the hackers who were threatening to expose it on the dark web as well.

266. MMH said this was an administrative error and quickly updated its notification. We accept this explanation. However, we note that MMH is far from the only agency that has made such an error and we recommend that all agencies take this opportunity to review their own understanding about what “likelihood of serious harm” means in the Act.

267. Health NZ notified OPC on 6 January 2026. While Health NZ had informed MMH of the breach on 30 December so were aware there was a problem, its concern related to whether a different service was affected (which it was not). It was not clear for some days that the Northland hospitals’ information had been affected. Once Health NZ became aware of this, it communicated promptly with OPC.



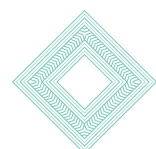
268. MMH notified affected individuals directly, where it had contact details to do so (which it did not, in approximately 47,000 cases. Of those, Health NZ managed to notify 19,497).

269. People whose information was included in the sample dataset published by the hackers on the dark web were specifically told that their information was in that dataset. This was an essential aspect of notification, and we consider that MMH did it well.

270. Other MMH users could log into their MMH portal to see whether they were affected, and also received direct email communications. This was a useful service and a helpful means of communication. However, there are points of improvement that other agencies could usefully bear in mind:

- The breach advice on the portal sometimes changed, which was confusing for people (they were told they were affected and then told they were not, or vice versa).
- The system was overloaded and people had difficulty getting into the portal, or getting hold of MMH. That loading is inevitable when a major breach occurs: a large number of people will need to get information or get into their accounts. Planning for such loading and building in an ability to scale up quickly is therefore critically important. In addition, MMH could have used GP practices as partners to distribute information, rather than informing those practices that they were not permitted to notify individuals or provide information.
- It was not always apparent what information was affected, and some people have had considerable difficulty getting those details. We have a number of complaints where people made information requests to MMH that have still not been adequately answered.

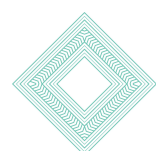
271. It became apparent that there were a large number of people for whom direct notification was not in fact practicable because of a lack of contact details.



MMH used a specific public notice on 4 March 2026 to inform those people of the matters required under section 115. Use of a public notice in those circumstances was acceptable but the need for it was unfortunate.

272. We acknowledge that the agencies spent a great deal of time, effort and money to fix the breach; identify what had happened and why; work together to identify who had been affected; develop communications to affected people, the sector and the public; and provide information and assistance to affected people. Much of this effort occurred in the first couple of weeks after the breach. Much of the effort also fell on a few key staff during a period where at least some of them were on annual leave. Those steps included:

- Engaging the right people to respond to the breach, including a clinical nurse, and people with privacy and security knowledge
- Engaging a public relations and media agency to assist in communication with media and other stakeholders
- MMH and HNZ holding daily coordination meetings with stakeholders and subject-matter experts
- Implementing identity theft and credit monitoring support for affected individuals
- Establishing a dedicated call centre, which provided access to trained health professionals, counselling services, mental health support, wellbeing advice, and crisis support, to address emotional impacts resulting from the breach
- Providing affected individuals and their families access to professional wellbeing and psychological support services
- HNZ making specialist clinical support available to practitioners, to ensure affected individuals could access clinically appropriate support following the breach.



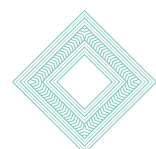
273. MMH also obtained a High Court injunction restricting the dissemination, use, and publication of the breached information, which we consider was an essential step.

274. However, after listening to the experiences of affected individuals and their general practitioners, we consider that it should have been practicable in these circumstances for affected individuals to be notified earlier and more clearly than they were. Final notifications were not completed until more than two months after the breach and we have had many reports of people being unclear about what information was affected, and receiving conflicting information about whether they were affected or not.

275. There were some practical difficulties with these notifications, including:

- the very large number of people affected by the breach
- initial confusion over who was affected and what information was involved
- confusion over whether MMH, Health NZ or GP practices were responsible for the notifications
- the fact that MMH did not hold contact details for thousands of affected Northland patients
- concerns over how to communicate appropriately with vulnerable people, including children.

276. To be clear, we do not expect agencies to rush notifications before they have established the relevant facts. Agencies need sufficient time to understand what has occurred so that they can provide affected individuals with accurate and practical information. Premature or inaccurate notifications can create additional confusion and anxiety, particularly where people are incorrectly identified as affected or provided with incomplete or incorrect information. At the same time, agencies should have processes in place to assess and communicate significant breaches promptly, recognising the practical



challenges that large-scale breaches can present, particularly for smaller agencies.

277. Our point, though, is that some of those difficulties with timeliness were either of the agencies' own making or could have been mitigated by appropriate advance planning. We consider that the phrase "as soon as practicable" should be interpreted in light not only of what the agencies in fact were able to do, but in light of what a reasonable agency experiencing a breach of this type would be expected to do. Notifying individuals is a critically important part of the breach management scheme in Part 6 of the Act. The policy reasons underlying those provisions would be undermined if agencies were allowed to avoid or delay notification because their own systems were not designed to allow them to notify promptly. Delay is also a risk for the agency – a failure to notify individuals as soon as practicable is a ground for an affected individual to make a complaint to the Privacy Commissioner. If the individual was not notified promptly and was adversely affected as a result of the delay in learning of the breach, this raises the potential liability of the agency in the Human Rights Review Tribunal.

Who is responsible for notification?

278. Here, some of the problems would have been avoided with a much clearer understanding about who was responsible for notifications – particularly whether MMH or GP practices would conduct the notifications. Under the law, the legal **holder** of the information is the agency responsible for notifying. However, there may be more than one holder of the information. For instance, for much of the information on the portal (though not the actual information affected by the breach), both the GP practice and MMH may legally be the holder of the information.

279. Decisions about who is responsible for notification become particularly acute when, as here, a service or product vendor experiences a breach that affects information supplied by hundreds of individual customers. Here, there were

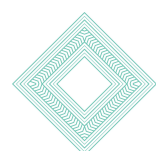


approximately 1,000 GP practices whose patients were affected. If those customers are the legal holders of the information, technically they all need to notify OPC.

280. Multiple notifications can quickly look inefficient and unnecessarily resource intensive for all. Sometimes, though, notifications from clients of a vendor that has suffered a breach may be the first that OPC hears about that breach. There is also a practical value for OPC receiving notifications from a variety of sources, to get a variety of perspectives about what has happened and how it may affect individuals.

281. However, there are also options for OPC to take a practical approach and that is what was done here. On about 7 January, OPC released a public advisory statement to let GP practices know that they did not need to individually notify the breach to OPC, as MMH had undertaken to fulfil the notification requirements in the Act. Health NZ also assisted OPC to get the message out to GP practices that they did not need to make direct contact with OPC. Once MMH provided a list of affected general practices, OPC also contacted them directly (on 9 February) to reiterate that separate notification was not necessary.

282. Another practical point is that the vendor (MMH) may have custody of the relevant information, but the agency that uses their services may have the closest relationship with the affected person and with others who may be concerned about the breach. It is often the agency with the closest relationship with affected people that is in the best position to decide how best to engage with people, particularly in a health context where there is a clinical relationship. For example, it is the GP who may have the best idea of whether talking face to face will be clearer and more supportive or whether written communications are sufficient). It is also the GP who is more likely to be aware of which people are likely to be vulnerable and need extra support. It is also the GP who needs to make a call about whether a person should not be notified of a breach on



grounds of risk to their health.

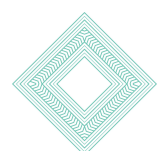
283. Some GP practices told us that MMH directed them not to contact their patients because that was MMH's job. While, as it turned out, that was the *legally* correct answer (because, as we discussed in Phase 1 of the inquiry, GP practices did not 'hold' the information that was breached), in the immediate aftermath of the breach it was not clear which agency was in fact accountable for notification.

284. Another complication here was so many of the Northland patients had not activated their accounts or did not realise that their information was stored on MMH at all. Many had never had a relationship with MMH. Any communication from MMH would therefore come out of the blue. Rather than receiving useful information about how to protect themselves, they would be likely to see an email from MMH as a scam and would – sensibly – either delete the email or not open it. This is why several thousand notifications were done by Health NZ, where Health NZ had contact information for those affected people. Since they had had contact with the hospital in the past, they would be less likely to be taken by surprise.

The need for clear communications

285. We have heard from complainants, enquirers and general practitioners that confused communications added to the anxiety that people experienced, and have undermined trust not only in these particular agencies but across the wider digital health sector.

286. From the start, GP practices that used the MMH portal were fielding calls from their patients asking for information. GP practices in turn were contacting MMH asking for information that they could pass on to patients. MMH was trying to put information together and manage queries from patients, clients and government agencies (including OPC) at the same time as investigating the breach, but this created understandable challenges for a small company. The



resulting information was sometimes patchy and inconsistent. At times, the tone was more focused on the company being the victim of a criminal attack rather than focusing firmly on the harm that had occurred to people whose information had been stolen. While the company properly apologised to its customers, this degree of defensiveness risked undermining the value of that apology.

287. Clear and consistent information provision is clearly important in breach situations, and the agency that has been the subject of a cyberattack or other breach will usually be in the best position to find out and communicate details of what had happened. MMH and Health NZ were unprepared for the situation. The time to work out who should communicate with patients and where the information should come from is before a breach happens (both with clear references in the contract and with practical instructions), not in the immediate aftermath of a breach. It is not possible to anticipate everything with planning, but the basics of breach management should already be in place.

288. This experience shows that how a breach is handled is critical to whether – or how quickly – people feel supported and inclined to continue to trust the company. We therefore recommend that all agencies – especially smaller agencies – should have a plan for what they would do if they had a large scale breach. This goes beyond normal breach management: any agency holding large amounts of personal information should have a crisis management plan in place. For example, they should consider:

- 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

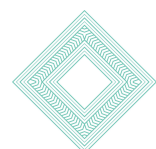


are accurate, or be clear when they have only incomplete information and when a clearer picture might emerge

- 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 quickly assessed, managed and notified to OPC and to affected people as soon as practicable.
- making sure key people can be contacted at all times including over holidays
- ensuring that they can scale up support if required to manage a major breach, including having external support available
- ensuring they have planned access to support services which can assist affected people (e.g. call centre support, health and wellbeing services and so on), including culturally relevant support where needed.

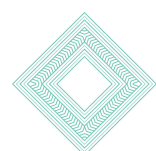
289. This does not mean that each agency needs to develop a crisis management plan independently; that would be unnecessarily resource intensive. Instead, we strongly recommend that industry associations, peak bodies and other formal or informal groupings of businesses or not for profit agencies can play a major part in developing and distributing information and crisis management playbooks for all their members to use.

290. We hope that these recommendations are useful to help all agencies be better prepared for breaches.



Appendix – List of key recommendations

1. Health NZ should ensure 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).
2. 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.
3. Health NZ and MMH should meet face to face with relevant communities and health providers in Northland to discuss the breach, as a way of restoring balance.
4. Health NZ should pay particular attention to account creation and activation as part of its roll-out of its new solution during 2027.
5. 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.
6. MMH should 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.
7. MMH should do full user-testing of its terms of use, privacy policy and business terms and conditions with patients and practitioners to ensure that the documents now provide clear information about people's rights and obligations.
8. GP practices and specialist health practitioners should check that patients are properly informed about how the SEHR system operates and, where necessary, obtain patient authorisation to transfer information.



9. GP practices should check that they have accurately specified the age at which a child's account should be de-linked from a parent's account, unless there is ongoing legal authority to keep the accounts linked.
10. All agencies should:
 - review the MMH and Health NZ compliance notices for points that are relevant to them
 - note that design decisions made other than under instruction may lead to third party providers being liable under the IPPs or Code rules
 - note that if a customer does not complete a registration process, they have not authorised any further collection of information into that account
 - have a process to identify and manage dormant accounts
 - if relying on authorisation as a legal basis for collecting, using or disclosing personal information, ensure that information provided to individuals is clear and precise so they know what they are agreeing to
 - have a clear process for personal representatives to follow when an account holder has died, and ensure representatives can find information about what to do
 - have a proper breach (or crisis) management plan in place
 - consider whether development proposals or breach responses may have a particular cultural impact and ensure that impact is properly assessed
 - ensure their contracts do not include clauses that purport to oust or limit liability for compensation under the Privacy Act or that purport to limit liability if personal information held by the agency is compromised by criminal activity.

