Privacy Commissioner
Te Mana Mātāpono Matatapu

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

Phase one report

25 May 2026

Table of Contents

1 Executive Summary

The breach and this inquiry

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

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

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

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

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

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

The value of patient health portals

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

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

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

Overall findings

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

Findings about Manage My Health

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

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

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

12. In particular:

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

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

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

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

Findings about Health NZ

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

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

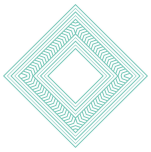
17. The novelty and scale of the project created very strong obligations on Health NZ to ensure that patient information would be properly protected. While it did

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

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

19. In particular:

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



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

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

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

Recommendations about general practitioners

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

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

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

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

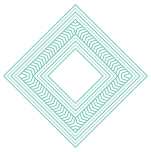
25. It is not possible for this inquiry to review what steps each individual GP practice has or has not taken. There are thousands of general practices in New Zealand, and there will be significant variability in whether they engaged MMH at all, what they contracted MMH to do, what information was stored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

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

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

Two additional recommendations

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



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

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

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

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

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

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

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

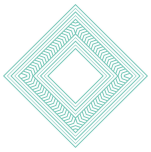
35. It should not be that complicated for the regulator, health consumers or health sector users of these services to identify which service provider or agency is accountable under the Privacy Act or its Codes. We also consider that the existing model, which relies on principal agencies making use of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

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

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

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

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



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

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

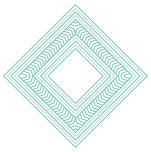
Next steps

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

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

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

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



2 An introduction to the inquiry

The breach

45. On 1 January 2026, MMH notified OPC that it had become aware of a cyber security breach ("the breach") affecting MMH's patient portal, in which a large amount of information had been extracted by criminal threat actors.

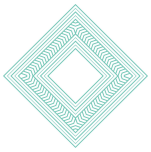
46. A general timeline of the breach is as follows:

- On or around 21 December 2025, hackers known as Kazu gained unauthorised access to the patient portal, using stolen patient user credentials.
- The credentials were then used to exploit a security weakness. That weakness enabled the hackers to systematically gain access to other patient accounts, and patient files were copied and extracted. This activity continued over several days.
- On 29 December 2025, the hackers uploaded a sample of stolen patient information to a dark web leak site. Users of that site were able to view and copy that patient information.
- The following day, 30 December 2025, the hackers advertised on an online channel that the data was available.
- Later that same evening, MMH was contacted by Health NZ, which had identified through its own monitoring that MMH information was being offered for sale by the hackers.
- Shortly afterwards, MMH received direct contact from the hackers, who demanded a 'ransom' payment of US$60,000 to prevent the sale of all the remaining stolen information.

- MMH started formal incident response activity in the early hours of 31 December 2025 and took immediate containment action. MMH also engaged forensic investigators later that day and remediated the specific vulnerability.
- On 1 January 2026, MMH made external notifications to relevant parties, including legal advisors and regulatory and law enforcement entities, including OPC.
- In the days that followed, additional response and monitoring activities were implemented, including ongoing monitoring of external sources for data exposure.
- Further forensic and remediation activities were also completed, including retesting of remediated controls.
- On 5 January 2026, MMH obtained an injunction from the High Court prohibiting unauthorised access to or disclosure of the stolen information.
- Initially, it was not apparent that Health NZ records had been affected. However, this was revealed during the forensic analysis. On 6 January 2026, Health NZ notified OPC that information from Northland hospitals stored in the MMH portal had been affected by the breach.
- Patient notifications started during January. MMH has said that those notifications were completed on 18 March 2026.

Numbers of affected people

47. Estimates of affected people have varied widely during the course of the breach investigation. This is not uncommon in the early days of a breach, but it has created some complexity for all parties with communicating about the scale of the event.



48. According to the most recent figures received from MMH in May 2026, 99,416 patients were affected in total, and 90,644 of those people were Health NZ patients in Northland (that is, around 91%).

49. The reason why so many people are affected in Northland is because of the unique arrangement between MMH and Health NZ to enrol patients into MMH and make certain types of hospital documentation available through the portal.

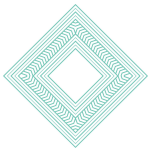
50. Almost 40% of people in Northland are Māori, which is significantly higher than the national average. While neither Health NZ nor MMH have been able to supply ethnicity figures for affected people, we therefore consider that it is a reasonable presumption that the breach has had a disproportionate impact on Māori.

The stolen information

51. Information in the MMH platform is organised into several separate areas or "modules". This enables patients to find the information they are looking for, or find a service that they need. For example, there are separate tabs under a module called "My Health Records" that stores shared electronic health care documents, vaccination and lab test results. Other modules allow patients to book appointments, ask for repeat prescriptions, or access health tips that they may be interested in.

52. All the stolen information was stored in a specific module called "My Health Documents". There is no evidence that any of the other information in the MMH platform was affected. For example, hospital lab test results were not affected, because they were stored under My Health Records which is a completely separate module. GP patient management systems were also not affected at all.

53. However, the fact that the hackers only appear to have gained access to one module does not make the breach less serious.



54. The information stored under "My Health Documents" came from three different sources, as noted in the following table. We also asked for further statistics relating to children and young people, and to ethnicity. All numbers are those supplied by MMH in May 2026:

Source of information	**Type of information**	**Numbers of affected people**
1. Information that patients uploaded about themselves	Any documents, clinical notes, photographs, test results etc – up to and including their whole medical file	8,566
2. Patients at Health NZ hospitals and clinics in Northland	Hospital discharge summaries	90,647
3. Patients who both uploaded their own information and who had Health NZ documents	As above	206
Children and young people	(all types)	13,670 were children under thirteen. 4,570 were young people between 13 and 17.
Ethnicity statistics	(all types)	Number not available
Document statistics		
Count of Health NZ documents affected: 403,730		
Count of patient uploaded documents affected: 22,609		

55. Early in the discussions about the breach, MMH told the Privacy Commissioner's office that another category of documents had been affected: that is, GP referral correspondence to specialists. Between 2017 and 2019, MMH stated that it had proactively extracted these documents from the MedTech patient management system to make them easily available to patients. It stopped this activity in 2019 after realising that the activity duplicated documents that were already elsewhere in the platform. Around 20,000 people were said to have been affected. In its cyber breach update of 13 January 2026, MMH stated that specialist referral documents were not accessed. This explains most of the discrepancy between earlier published numbers (126,000) and the numbers provided more recently.

56. All this health information is inherently sensitive and some of it was highly sensitive (for example any mental health or sexual health notes or other medical information of an intimate nature). While hospital discharge documents do not reveal the patient's whole medical record, details of events and procedures may still reveal intimate information.

57. Because of the nature of the documents stored in the My Health Documents module, some of the stolen information also includes personal identification details, such as names, birth dates, NHI numbers, addresses, email addresses, and phone numbers. Compromise of this information can also cause significant harm to people.

58. This information is sensitive at the individual level and it can also be sensitive for whānau or hapū.

What effect the breach has had on people

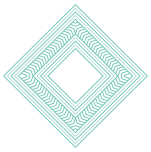
59. The theft and exposure of medical information has caused substantial distress and uncertainty for many affected people. More than 150 of those people have written to us to explain how the breach has affected them. GPs have also

written, expressing concerns on behalf of their patients, and noting that the damage to trust in health portals is having an effect on their own practices.

60. Many of our correspondents are expressing feelings of anxiety, stress and embarrassment. Many are angry.

61. Some of the more specific experiences of people whose medical information was accessed include:

- One person had stored their whole medical file with MMH when they moved to New Zealand, as a safe place to put it so they could share it with a GP. The breach has therefore exposed every aspect of their health.
- Māori correspondents have told us that the loss of their information has affected their broader whānau as well as themselves (a common issue in relation to health information), and that their feelings of cultural safety and trust in the health system have been damaged. Some are more hesitant to make important health-related appointments due to fear of their health information being released in future.
- For several people, anxiety about access to their records is exacerbating their PTSD or other health conditions.
- Some are concerned that disclosure of the information might affect their employment if it was to surface later (for example, information about their mental health condition, or other health status).
- Many are still unclear about exactly what health information of theirs had been taken ("was it my brain scan or was it my phone number?") and this alone is creating anxiety.
- It is a common theme in the correspondence that people did not know that their information had been stored in the MMH portal.



- Another common theme is that they had moved practices and thought that the MMH portal information had been deleted.
- There are also many complaints about the timeliness and clarity of communications about whether their information was affected or not.

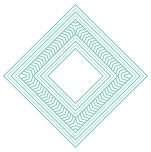
62. In the abstract, disclosure of non-medical information may appear less sensitive. However, for some of our correspondents, it is precisely the loss of this information that is causing them most concern. Examples include:

- people in jobs where exposure of contact details could put them and their families at risk
- people who have left situations of family violence and whose former partners are unaware of their current location
- the potential for the information to be used for identity theft, for phishing or for other criminal activity, particularly if the stolen information is also associated with other accounts under their name.

63. We have also heard from people who were unaffected by the breach itself, but who are now uncertain whether they can trust messages that appear to come from MMH. While many hospital documents are also posted to patients, some patients have become justifiably wary about clicking links coming from the portal, and are therefore potentially missing out on other important health messages.

Assessing the risks of harm

64. The people who are at most obvious risk of harm are the people whose information was included in the sample set that the hackers published. There is no reliable way of knowing who has seen that information. It was visible online for several days before the High Court injunction was obtained and we were



contacted by some people who informed us they had viewed and analysed the information.

65. The people whose information was exposed in this way have all been specifically notified by MMH that their information was included in the sample dataset.

66. It is less clear that the remaining data that was stolen has been made available to others. MMH has commissioned monitoring, which is continuing. So far, that monitoring has not found any signs that the dataset has been put up for sale. The sample information has also been taken down from some websites, using the injunction that MMH had obtained from the High Court. The fact that there is no evidence so far of further sale may help to alleviate people's concerns to some extent.

67. However, we also recognise that monitoring does not necessarily capture all distribution of information, and criminals do not take any notice of injunctions. It is also unclear whether the hackers still hold the information or whether it has been destroyed. As a result, it is understandable that people will remain concerned that there is an ongoing risk that their information will be sold or misused.

68. We therefore recommend that monitoring to detect activity associated with MMH stolen data should continue, to provide a degree of ongoing assurance for people that their information has not been offered for sale.

The inquiry

69. Given the seriousness and the scale of the breach, the Privacy Commissioner announced an inquiry on 21 January 2026, under section 17(1)(i) of the Privacy Act 2020. OPC issued its terms of reference on 27 January 2026.

70. Section 17(1)(i) enables the Commissioner:

> "to inquire generally into any matter including … any practice or procedure, whether governmental or non-governmental, or any technical development, if it appears to the Commissioner that the privacy of the individual is being, or may be, infringed…"

71. The findings of the inquiry will also be used to help to review complaints from affected people and, if the Commissioner considers this necessary, to investigate or seek to resolve those complaints.

72. In addition, many findings will be relevant to other patient health portals and organisations that contract with them. They can be used to improve practice across the board.

Scope of the inquiry

73. As the Terms of Reference state, the inquiry falls into two phases.

74. **This report deals only with Phase 1**. It considers three key issues:

- The respective responsibilities of MMH, Health NZ, and users of the MMH portal (particularly GP practices) for the security of patient information in the portal.
- What "reasonable security safeguards" look like in this context.
- Whether MMH and Health NZ had those reasonable security safeguards in place at the time of the breach, as required by Rule 5 of the Health Information Privacy Code 2020.

75. The report therefore sets out our Office's regulatory expectations of what security safeguards patient health portals should have in place. It also sets out what organisations engaging with portal providers need to do to ensure their patients' information is adequately protected. Regardless of which portal provider is chosen, patients need to be able to feel confident about using these increasingly important health sector tools.

76. Some of these findings are also relevant to other agencies that handle sensitive personal information or use third party platforms. We recommend that all those agencies should review the findings of this inquiry, and make any necessary adjustments to their own security settings.

77. **Phase 2** will consider all other (non security-related) privacy issues raised by the breach. These are set out in more detail in the Terms of Reference but are likely to include at least:

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

Methodology

78. MMH and Health NZ provided initial information and documents to us as part of the mandatory breach notification process under the Privacy Act.

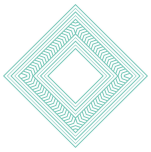
79. In addition, under this inquiry, we made statutory demands under section 87 of the Privacy Act for a wide variety of information that was relevant to the issue of security safeguards, including technical reports, governance reports, project

documentation and so on. OPC holds that information in confidence, except to the extent that it is necessary to refer to it as part of this published report, in order to give effect to the Privacy Act by explaining our findings (see section 206 of the Privacy Act).

80. We engaged DEFEND, a New Zealand cyber security and cyber resilience firm, to provide us with expert independent analysis about what the relevant security standards were in the context of this breach, analysis of all documentation provided by MMH, and an assessment of whether MMH met the required standards here.

81. Information provided by enquirers and complainants has informed our views on the harm caused by the breach.

82. MMH, Health NZ and GP representative organisations have had an opportunity to comment on the findings about their responsibilities and their actions. We have taken those comments into account in this final Phase 1 report.



3 The respondent agencies

Manage My Health: the patient health portal

83. Patient health portals have been a feature of the New Zealand digital health environment for nearly two decades. A health portal allows patients to view defined types of the health information that their GP (or, here, their hospital) holds about them. Commonly, they also allow patients to communicate with health providers.

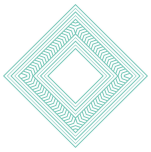
84. All health portals in New Zealand are currently operated by private companies, rather than being owned and managed by the public health system.

85. Manage My Health ("MMH") is one of several health portal companies operating in New Zealand and was one of the earliest (it was originally incorporated in 2008). Like many New Zealand companies, it is very closely held, with only two directors including the Chief Executive. Its holding companies also share the same directors and ownership.

86. MMH contracts with GP practices to provide certain digital services to patients, such as booking appointments, ordering repeat prescriptions and video-calling. Patients with activated accounts can also use either an app or the MMH website to access certain types of health information about themselves that is stored on the platform. What they can access will depend on what the GP practice or other health sector agency has chosen to make available (such as clinical notes or correspondence, shared healthcare records, laboratory test results and so on).

87. MMH also provides other software solutions, such as facilitating the transfer of shared health care records. Those other software solutions are separate from the patient portal service and are out of scope for this inquiry.

88. Unlike most other patient portals in New Zealand, the MMH portal does not simply act as a system to view information that is stored in the GP practice's



own patient management system. Instead, copies of health information are stored within the MMH platform itself, and patients can then access that information by signing in to their account.

89. There are several different sections (or modules) in the MMH health portal. The main screen has a dashboard with key information and also has tabs for:

- Booking an appointment
- New repeat prescription
- My Health Records (which includes shared care records and GP notes and correspondence)
- Lab results
- Messages
- Information about the health centre or centres where the patient is registered
- Articles and advice.

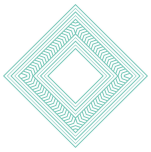
90. The only module affected by the breach was a specific module called “My Health Documents”. If patients store their own health information in MMH, this is the module where that information will be located. It is the module where all the affected Northland hospitals’ discharge documentation was stored.

91. At the time the breach occurred, MMH stated that it had around 1.85 million user accounts in New Zealand. It also operates overseas in Australia and India.

The difference between a registered account and an activated account

92. During this inquiry, it has become apparent that there is an important difference between a **‘registered’** MMH account and an **‘activated’** account.

93. Essentially, a **registered** account is created *in the name of* the patient. One common way this can occur is when a GP practice engages MMH to provide



portal services to patients (such as bookings and prescriptions). The GP practice forwards some basic information to MMH (such as name and an email address). This enables MMH to send an automated message to the patient inviting them to click a link that takes them to a sign-up screen where they can set up a password and get information about the MMH service.

94. If the patient follows those steps, the account is **activated**, and the patient can then use the services and view the information in the portal.

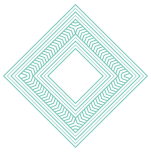
95. If the patient does not follow those steps, the account remains 'registered' only. Any information stored against that registered account remains in the MMH portal, but is not visible to the patient. It stays in the portal until it is deleted in accordance with MMH's policies. Retention and deletion policies and practices will be considered in more detail in Phase 2 of the inquiry.

96. It has become apparent through the inquiry that thousands of patients were unaware that they had an MMH account at all. This created complications with notifying those patients. We intend to consider the issue of account creation in detail as part of Phase 2 of the inquiry, as it is central to the question of whether patients provided authorisation for accounts to be set up.

Health NZ (Northland)

97. As part of the health sector reforms, New Zealand's District Health Boards (DHBs) became part of Health NZ, which inherited all the contracts, responsibilities and liabilities of the DHBs. While all the actions that we discuss in this section were those of the Northland DHB (which, at most relevant times was a separate legal entity) we therefore refer throughout to Health NZ as the responsible agency.

98. In 2019, Health NZ started to investigate the possibility of improving patient services by sending hospital discharge documentation to a digital patient health



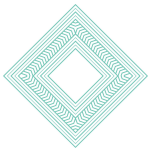
portal for patients to access, rather than patients having to wait for printed paperwork before they could leave hospital.

99. The project had the support of the local Consumer Council (which included Māori representation), and the Consumer Council had a member on the steering group. There was also consultation with some other community organisations, including one large PHO, whose Chief Executive was also on the steering committee. In addition, the project team consulted with some key local groups such as the Alzheimer's Foundation, Parkinson's Society and the Northland Digital Enablement Group.

100. Health NZ's research showed that one of the things that frustrates patients most when leaving hospital is the long wait to get printed discharge documentation (or "transfer of care" records) before they can go home. Relevant information is electronically forwarded to GP practices, but discharge documents contain a record of hospital procedures for the patient. These notes can include a record of surgical or other treatments, medication administered, test results and clinical observations. Discharge documents also include instructions for patients about how to manage their health after leaving hospital (e.g. wound care, diet and so on). Patients need access to that information at the time they leave hospital or shortly afterwards.

101. Health NZ identified an opportunity to address this frustration and provide better patient services. Instead of printing the documents for the patient, the discharge documentation could be completed later in the day and sent through to the patient's health portal account for them to access. It considered that there were several obvious benefits:

- it would enable the patient to leave hospital as soon as they had obtained any prescription
- it would free up beds, which in turn would help new patients to be moved onto the ward more quickly and relieve bottlenecks elsewhere



- digital provision of information would save printing costs
- it would save the patient from having to keep the paperwork safe.

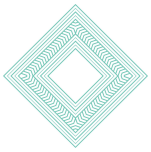
102. After an initial proof of concept, and technical development, a formal pilot was started in Whangārei Hospital in 2021. It was evaluated as a success, and Health NZ then worked towards rolling out digital provision of discharge documentation across some areas of Whangārei Hospital.

103. In 2023, Health NZ established a steering group, including senior leadership, that acted as an internal governance group throughout the rest of the project. The steering group was fully engaged with Health NZ's local IT team, which focused on functionality and user interface issues. A MMH staff member also attended the steering group, as the project's design and implementation partner. However, the group did not include members with security expertise or privacy expertise.

104. The discharge documentation aspect of the project went live in November 2023. Health NZ confirmed to us that the agreement is still in place – that is, the information is still being shared with patients through MMH.

105. Health NZ also identified that health portals could be used for other types of hospital documentation and, in 2024, the project was expanded to two other areas.

106. The first was to send the patient their laboratory test results, in cases where a hospital specialist had ordered the test rather than the patient's GP. Not all lab test results were being sent to GP practices which had resulted in patient complaints about lack of access to information. Also, patients in certain areas of care (such as renal) may be reliant on prompt access to their lab test results in order to help to manage their own health. It was felt that sending the results through to the patient portal would enable quick access, without requiring GP practices to first file the information and then supply it to the patient.



107. The second was to give patients better access to information about where they sat in a referral queue and access to referral letters (which could include the reason for the referral, medical history, symptoms or diagnoses). It was felt that digital delivery would:

- allow patients to get that information as soon as it was available, rather than having to wait for postal delivery
- save confusion if the patient misplaced the referral paperwork
- reduce risks associated with misaddressed deliveries
- reduce postage and printing costs.

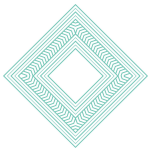
108. Provision of lab test results went live in mid-2024 and referral documentation in 2025.

109. Lab test results were sent to the “My Health Records” section of the patient’s MMH account, and referral messages were sent through the message facility. Neither have therefore been affected by the breach, which only affected “My Health Documents”.

110. However, hospital discharge summaries were stored in the patient’s My Health Documents module of MMH. These are therefore the principal type of records that have been compromised by the breach.

MMH’s involvement

111. The decision to engage MMH was made at the proof-of-concept stage. There is no evidence that MMH’s privacy or security status were considered as part of a procurement or due diligence process. The project documentation simply suggests that MMH was the natural selection at the start of the project. There were several reasons for this:

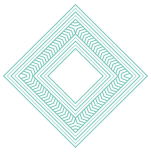


- MMH already had contracts with around 70% of GP practices in Northland, so there was a greater likelihood of being able to engage a critical mass of patients.
- MMH was the only provider that offered an independent repository function that would allow consumers to access information from different sources (GP practices, hospitals etc) in one place.
- Health NZ considered that MMH was already Ministry of Health approved and it was reportedly being used by more than a million people in New Zealand.
- Health NZ considered that the MMH portal met the Health System Design Council's principles for approving new systems.

112. While there were plans to expand to other portal providers in time, Health NZ therefore chose MMH as its sole supplier. It was also an active design partner: a MMH representative was part of the project steering group throughout the project.

113. With Health NZ's agreement, MMH created specific processes to receive Whangārei Hospital documentation and associate it with the correct patient account. In brief:

- Hospital staff forwarded the relevant documentation to MMH using the automated HealthLink messaging platform.
- The documents were stored in a specific repository (called the EDI folder), operated by MMH.
- MMH matched documents in the repository against existing patient accounts.



- If there was a positive match, the relevant documents were then transferred to the "My Health Documents" section of the patient's account so that the patient could access them.
- If there was no match, documents would be deleted and a note made on the audit file.
- All information is hosted in New Zealand.

Signing up patients and practices

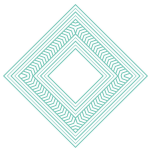
114. When the project started, the project documentation records that only around 19% of patients already had a MMH account. Those numbers needed to be a lot higher to achieve the desired benefits of the project.

115. During both the pilot and the wider roll-out, Health NZ therefore actively engaged with patients in Whangārei Hospital to encourage them to sign up with MMH so that they could get digital, rather than printed documentation. A staff member was made available to help people to register accounts, using tablets or other movable technology on the ward. People could decline, and some did, but many people agreed.

116. Once the patient had set up an account, they received an email or a text message from the hospital confirming that the account now existed and inviting them to opt out if they had changed their mind and did not wish to receive hospital documentation this way.

117. The resourcing required to sign people up in hospital was intensive, though. It took nursing or administrative staff away from other tasks and was unsustainable in such a busy work environment. The project team looked to other solutions.

118. In particular, Health NZ decided to encourage and support Northland GP practices to engage with MMH if they wished to do so. Health NZ agreed with



MMH that it would pay the MMH licensing fees for all the Northland GP practices. This resulted in wider take-up of MMH across the region. All (or nearly all) GP practices ended up licensed to use MMH, and many registered their patients in the service. Health NZ continues to fund this service.

119. While the numbers of Northland patients with MMH accounts rose during this time, it appears that many of those accounts were never **activated by the patient**. A **registered** account (in MMH's terms) existed for the patient with some basic details, but the patients had not proceeded to set up a password, and therefore did not use the portal.

120. There may be a number of ways in which registered accounts were created. We will consider in detail how this occurred as part of Phase 2 of our inquiry, as it is relevant to whether or not patients authorised the creation of their accounts. Having information in non-activated accounts also frustrates the purpose of storing the information in the portal at all: by definition, patients would be unable to view that information.

121. The key issue to note at this stage is that the MMH matching process at the relevant time only required that a patient account was registered. It did not have to be activated for documents to be transferred to the My Health Documents module. This seems to be one of the reasons why so many patients appear to have been unaware that their information was stored in MMH and were therefore taken by surprise by the breach. The difference in terminology also matters to the understanding between the parties. MMH understood one thing by the term "registered" and Health NZ understood something else.

122. MMH states that it has now changed that matching process and a match is only classified as 'positive' if the account has been activated by the patient.

4 Responsibilities for the security of information in the portal

123. One key aim for Phase 1 of the inquiry was to establish which organisations are legally responsible for having and maintaining the 'reasonable security safeguards' that the law requires. This section of the report sets out those legal responsibilities.

The relevant law: the Health Information Privacy Code 2020

124. Under the Privacy Act, the Privacy Commissioner can issue Codes of Practice that modify the Information Privacy Principles (IPPs) so that they apply to specific types of information, specific types of agencies or industries, or specific activities. These modified IPPs are known as "Rules".

125. The Codes are secondary legislation: that is, they become the law in the context to which they apply. A breach of a Rule is the same as a breach of an IPP, and can be the subject of complaints and enforcement in the same way. All other aspects of the Privacy Act also operate as normal: for example, agencies have exactly the same obligations to inform the Privacy Commissioner and affected people about "notifiable privacy breaches", such as the MMH breach.

126. In the context of this inquiry, the rules that govern MMH, Health NZ and primary care providers are set out in the Health Information Privacy Code 2020 ("the Code").

127. Rule 5 of the Code is essentially the same as IPP5 of the Privacy Act, with one additional obligation relating to disposal. It states that:

> (1) A **health agency** that **holds health information** must ensure—
>
> (a) that the information is protected, by such security safeguards as are reasonable in the circumstances to take, against—

(i) loss;

(ii) access, use, modification, or disclosure that is not authorised by the agency; and

(iii) other misuse;

(b) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the health agency, including any storing, processing, or destruction of the information, everything reasonably within the power of the health agency is done to prevent unauthorised use or unauthorised disclosure of the information; and

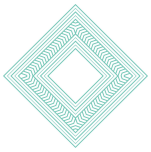
(c) that, where a document containing health information is not to be kept, the document is disposed of in a manner that preserves the privacy of the individual.

128. The terms in bold are each discussed separately below to show how the Code applies here.

Health information

129. The patient information that is sent to and held in MMH is all "**health information**" as defined under clause 4(1) of the Code. It is either:

- information about the person's health or disabilities, including their medical history
- information about the health services or disability support services that they are receiving or have received – such as which GP they are registered with, referral correspondence from specialists, documents showing which hospital they were in, and so on



- information derived from the testing or examination of any body part, or any bodily substance of that individual – such as lab test results, or results of other diagnostic tests
- incidental information that is collected as part of providing any health or disability services – this includes administrative or contact information, such as name, NHI number or other identifiers, email or phone contacts, and demographic information such as ethnicity or location information.

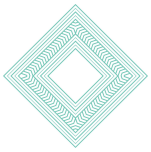
Health agencies

130. While all the information is health information, the Code only applies if the agency collecting, holding and managing the health information is a "**health agency**" as defined by clause 4(2) of the Code. (If the agency is not a health agency, the agency will instead have to comply with IPP5 of the Privacy Act.)

131. Health NZ and primary health care organisations (such as PHOs and general practices) are self-evidently "health agencies". They directly provide health and disability support services to the people whose information is held in the MMH portal, or that was held in that portal at the time of the breach (see clause 4(2)(a) of the Code).

132. MMH is also defined as a health agency under the Code but for different reasons.

133. MMH does not provide diagnoses or direct health advice to people. Instead, its function is to offer a range of digital services that patients and health practitioners can use. It is not a more general IT support provider or supplier. Its whole business is based around receiving, transferring, processing and storing health information. It does so under contract with health providers, particularly with GP practices and – in the context of this inquiry – with Health NZ in Northland. It also offers options for patients to upload their own information.



134. As such, MMH is therefore also defined as a health agency under clause 4(2)(j) of the Code because it "provides services in respect of health information, including … under an agreement with another agency." The same is likely to be true of other health portal providers and operators of patient management systems.

135. All the agencies that are relevant to this inquiry are therefore health agencies and the Code applies rather than the IPPs in the Act.

Which of the health agencies "held" the information that was affected by the breach?

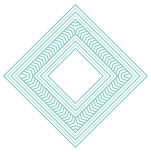
136. As the wording of Rule 5 makes clear, only a health agency that **holds** health information is directly responsible for ensuring reasonable security safeguards under Rule 5(1)(a).

137. In addition, if an agency that holds information then engages a service provider and gives that provider health information in order to carry out services, the agency has an obligation under Rule 5(1)(b) to ensure everything is done to prevent unauthorised use or disclosure of that information. This is a continuing responsibility that applies throughout the provision of the service.

138. There is also an obligation to ensure secure destruction of health information that is no longer required under Rule 5(1)(c).

139. Where there is a direct relationship between the agency and the person whose information is stored, it is clear that Rule 5(1)(a) applies, regardless of whether the information was originally sourced from another agency.

140. However, where the agency engages a third party to store, process, distribute or otherwise handle the information, it can be harder to identify whether – and at what point – that principal agency or the third party (or both) legally 'holds' that information.



141. Section 11 of the Privacy Act is relevant to that question. It applies where one agency is arguably acting on behalf of another. Section 11 states that:

> (1) This section applies if an agency (**A**) holds information for or on behalf of another agency (**B**) (for example, the information is held by A as a representative or agent of B, or for safe custody or processing on behalf of B).
>
> (2) For the purposes of this Act, the personal information is to be treated as being held by B, and not A.
>
> (3) However, the personal information is to be treated as being held by A as well as B if A uses or discloses the information for its own purposes.
>
> (4) For the purposes of this section, it does not matter whether A—
>
> (a) is outside New Zealand; or
>
> (b) holds the information outside New Zealand.
>
> (5) To avoid doubt, if, under subsection (2), B is treated as holding personal information,—
>
> (a) the transfer of the information to A by B is not a use or disclosure of the information by B; and
>
> (b) the transfer of the information, and any information derived from the processing of that information, to B by A is not a use or disclosure of the information by A.

142. The situation here is not straightforward. Some health information is sent to or through the MMH portal by individual patients themselves. Some is supplied by GP practices to help them provide services to patients. Health NZ engaged MMH to deliver the Northland hospitals' information to patients through the portal. Since a subset of the information on the MMH platform (information uploaded by patients, and hospital discharge information from Northland) was

affected by the breach, it is important to identify whether Health NZ or MMH 'held' that information.

143. The key questions are therefore:

- Whether MMH held the health information on behalf of the individual patients – in which case, it has direct responsibilities to those patients for the security of the information under Rule 5(1)(a) and section 11 is not relevant.
- Whether MMH held the health information only for or on behalf of healthcare providers or Health NZ, in which case section 11(2) applies. Only the healthcare providers and Health NZ would legally 'hold' that information. MMH would not hold it and would not have direct responsibilities under Rule 5.
- Whether MMH held the health information on behalf of healthcare providers or Health NZ but also used the health information for MMH's own purposes, in which case, section 11(3) applies. The healthcare providers or Health NZ would still legally hold the information that they supplied to or provided through the MMH portal, but MMH itself would also be deemed to 'hold' that information and would have direct responsibilities under Rule 5.

144. See the table in Appendix A for a summary of our findings about which agency is responsible for which type of information.

Findings relating to MMH

145. We have concluded that all information in the My Health Documents module, regardless of its source, is "held" by MMH. MMH was not simply holding or processing information on behalf of GP practices and Health NZ.

Self-uploaded information: MMH is solely responsible under Rule 5(1)(a)

146. Most obviously, MMH allows individual patients to self-register. It also allows patients to use the portal to store their own health records. In those situations,

the contractual relationship is clearly between MMH and the patient alone. Neither the patient's GP practice nor (if relevant) their hospital has control over what is uploaded or what happens with that information.

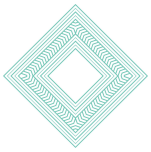
147. MMH has informed us that no self-registered patients have been directly affected by the breach. However, 8,566 patients were affected after uploading their own information, with another 206 patients who had both self-uploaded information and hospital discharge documentation that was stolen. It is clear that under Rule 5(1)(a), MMH is the sole agency responsible for having reasonable security safeguards in place to protect that information.

Information in the portal that was sourced from Health NZ

148. Up to the point where the hospital-related information is transferred to a patient's account in the portal, we consider that MMH does not legally hold the information. It is simply processing information on Health NZ's behalf:

- That information is clearly still in Health NZ's control.
- Health NZ defines what types of information it will supply to patients using this method.
- It sends that information through HealthLink to the MMH temporary store.
- It engages MMH to match the information against registered MMH accounts and then transfer that information to the portal.

149. However, once that information is held in the portal, we have concluded that the situation changes. MMH now holds that information on the **patient's** behalf, for all the reasons explained earlier. It is no longer acting on Health NZ's behalf and is responsible for its security under Rule 5(1)(a). Effectively, the information has been successfully "posted" to the patient (in the form of a record that the patient can access on an ongoing basis). Exactly as with physical posting, Health NZ has no visibility of the information in the portal, no access to patients'

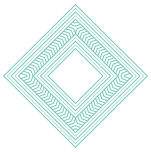


accounts, and no further control over what is done with that information. It was simply the original source of the information.

150. The contracts that MMH entered with Health NZ and with GP practices are not particularly clear about the basis for the relationship. However, those contractual terms clearly show that MMH is asserting that it has a direct relationship **with the patient** in relation to all information that is stored in the portal (regardless of the source of that information):

- Any patient who activates an MMH account has to agree to the terms of use and the privacy policy.
- Both those documents are framed in terms of a direct relationship between MMH and the patient. The patient needs to set up their access credentials (password and, now, multi-factor authentication), is expected to protect those credentials, has sole choice over whether to maintain the account or delete it, can upload their own information and can (to some extent) choose which services to use.
- The patient's information is retained in the MMH system indefinitely until the patient chooses to close their account. GP practices do not have a say in whether the account continues to exist: it is the patient's account not theirs. Even if a patient moves to a practice that does not use MMH, their account will remain open. Patient accounts also remain open if a practice stops using MMH.
- The contracts with GP practices, Health NZ and other health sector users incorporate those same terms of use and privacy policy, as well as MMH's "code of conduct" and business terms and conditions that set out further expectations about issues such as access management.

151. Secondly, the terms of use and the privacy policy state that MMH can use personal health information for a variety of purposes that go beyond supporting the GP practice, including:



- sending the patient links to resources that MMH considers the patient might be interested in receiving based on the patient's personal health information (unless the patient opts out)
- unspecified research purposes
- marketing.

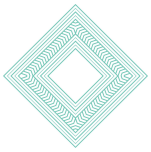
152. MMH has told us that the terms of use and the privacy policy do not mirror its actual practice. In particular, it does not in fact use patient information for marketing or research and all reporting uses aggregated and de-identified information. We acknowledge the point and agree that actual practice is important. However, the terms in the documentation are still a relevant consideration. That documentation is MMH's own, and in some cases its terms form part of a legally enforceable agreement.

153. MMH has told us that it is in the process of updating that documentation to reflect what actually occurs. We agree that this will be helpful, both for users and for MMH itself.

154. We also note that MMH told us that, between 2017 and 2019, it proactively transferred referral documentation from MedTech to the portal. Such an activity also indicates that MMH was acting as a holder (or 'controller') of that information, not merely acting on behalf of another health agency.

155. Regardless of whether MMH in fact uses information for any of the secondary purposes in its documentation, its whole model is one of a direct relationship with the patient. This is the main feature that we consider is relevant.

156. As a result, we have concluded that MMH holds the information and is legally responsible under Rule 5(1)(a) of the Code (not merely under any contract to its customers) for ensuring that its portal has reasonable security safeguards.



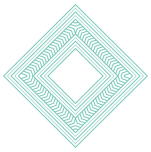
Findings relating to Health NZ

157. As will be obvious from paragraph 148, we consider that Health NZ held the patient's health information up to the point that the information was transferred to the portal. Health NZ collected the health information from patients, created the documents that were subsequently provided through the MMH portal, and supplied those documents to MMH under contract. Health NZ was the initial holder and source of the health information. It engaged MMH to store, match and distribute the information to patients on its behalf.

158. Throughout that process, therefore, Health NZ is the sole holder of the information. It is clearly responsible under Rule 5(1)(b) for doing everything reasonably within its power to ensure that its service provider (MMH) had adequate safeguards in place to prevent unauthorised use or unauthorised disclosure of the information, both during the initial processing and once the information was made available to patients through the portal (it has a continuing obligation to get assurance that the information is secure for the duration of the contract).

159. We also considered whether Health NZ also continues to legally 'hold' the information that it supplied to patients through the MMH portal under section 11 of the Privacy Act and therefore whether it, too, had obligations under Rule 5(1)(a). We have concluded that it does not.

160. As set out in paragraph 149, we consider that MMH was no longer acting on Health NZ's behalf, but was operating under its direct relationship with the patient. It had completed the job that Health NZ engaged it to do: that is, to deliver the information to the patient. Health NZ no longer had any practical or legal control over that information. It also could not see whether the patient accessed the information, and had no control over whether the patient maintained their account or chose to delete it.



Findings relating to GP practices

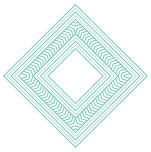
161. The situation is clearer for GP practices. Unlike Health NZ, GP practices are direct users of the MMH portal. They have their own access credentials. They use it to communicate with patients, and provide services to patients. GP practices can also choose which features of the portal to offer as a service to their patients. GP practices therefore legally hold at least some of the information that they supply to, obtain through, and store on the platform.

162. When contracting with MMH – or any other portal provider – Rule 5 therefore requires the GP practice to take reasonable steps to ensure that the information is secure. GP practices 'hold' and are jointly responsible with MMH for the security of all patient information that they have supplied to MMH in order to set up the initial registered patient account.

163. It is potentially arguable that for some of the services offered through the portal, MMH may simply be processing information on behalf of the GP practice (or other health agency), rather than also holding that information. However, none of the information affected by this breach was sourced from GP practices or engaged those services. It would be a subject for specific discussion if it was relevant to an individual situation.

164. As discussed later, the fact that GP practices hold information in the portal does not mean that they are responsible for every aspect of its security. For example, they do not hold and are not responsible for information that patients upload for themselves. They also have no ability to control the security settings that MMH applies. The law only requires them to take reasonable steps to make sure the information is secure. Part 8 of this report provides some further details about what we consider those 'reasonable steps' are in the context of health portals.

165. Also, here, none of the stolen information taken from the "My Health Documents" module was supplied by GP practices. The GP practices therefore did not hold the *specific* information that was affected by the breach. It is



therefore unlikely that a complaint against an individual GP practice for a breach of Rule 5 would succeed in the context of this breach. However, GP practices need to be aware that they do have some security obligations. This is a good opportunity to review their processes and ensure that they have taken the steps they need to.

The need to amend the Act

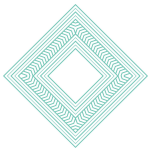
166. This inquiry is a useful illustration of how the current provisions of the Privacy Act (particularly section 11) work. We consider that there is an opportunity to simplify the settings and meet consumer and regulatory expectations.

167. While the inquiry has concluded that MMH is legally responsible under Rule 5(1)(a) of the Code, this has relied on a close examination of how MMH operates. Other patient health portals – as well as other third party health services – operate differently and a security breach would not necessarily lead to the ability for OPC to take compliance action against that third party provider under Rule 5 of the Code.

168. Put simply, it should not be that complicated for the regulator, health consumers or health sector users of these services to identify which service provider or agency is accountable under the Privacy Act or its Codes for fundamental security measures. We also consider that the existing model, which relies on principal agencies making use of contractual remedies where their service providers fail to meet IPP 5 (or Rule 5) obligations, is insufficient.

169. Most obviously, direct liability for security settings would simplify the process for individuals seeking to complain about a security breach. In particular, it would simplify the section 11 analysis for an OPC investigation (and any later Human Rights Review Tribunal examination) and therefore improve efficiency.

170. In addition, OPC should be able to take direct compliance action against a third party provider that fails to have reasonable security safeguards in place. At the moment, OPC's ability to bring compliance action relies on showing that the

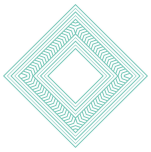


third party is using information on its own behalf or engaging directly with consumers, not merely processing or storing information for a client organisation.

171. Finally, businesses – particularly small businesses such as most GP practices – should not have to rely on contractual provisions alone to get assurance that the third parties that they engage have reasonable security settings in place. It is unduly burdensome for each business to have to take separate legal action under contract to enforce security expectations. For example, the current settings could mean that thousands of individual GP practices would need to take legal action against a health portal provider or practice management system operator if there is a failure of a contractual obligation to maintain security. Contracts are important, but businesses should be able to have confidence that the law itself also requires the third party to have reasonable security settings in place.

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

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



Remedies are only triggered if there is an "interference" with privacy

174. This inquiry considers whether MMH, Health NZ or (in a more generalised way) GP practices may have infringed the privacy of people whose information was stolen in the cyber security incident.

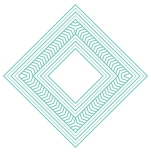
175. A breach of one or more of the Rules of Code is a clear infringement of privacy and is a serious matter. It can trigger compliance actions from the OPC. In particular, it can lead to a compliance notice requiring the agency to bring its practices into compliance with the Code.

176. People also have the right to bring complaints against one or more agencies.

177. Here, for those people who have been affected and who may be considering complaining to OPC, it is worth noting that a breach of a Rule of a Code or an IPP does not, on its own, usually mean that they would be entitled to compensation or some other kind of remedy. (The only exceptions are for breaches of rights to ask for access and correction of information). A second step is needed before a complaint can be successful.

178. This is because, to get a remedy, there needs to be an "interference with privacy" as defined by section 69 of the Privacy Act. The person must show not only that there was a breach of the Code by an agency (which is a question that this inquiry helps to answer) but also show that that breach has caused or may have caused harm to them. Harm can take the form of financial loss, loss of some kind of benefit, or significant emotional distress. Mere annoyance or uncertainty is not enough. Generalised concerns about the potential for identity theft (always a possibility with cyber security incidents) may also not be enough.

179. With such large numbers of affected people, it is inevitable that people will have been affected in different ways. Some may simply be annoyed or frustrated. Many may be angry that there has been a breach but the loss of the particular information may not have caused them significant distress. Others may have



suffered deep distress but for reasons that relate to issues that are not linked to a breach of one or more Rules of the Code. OPC might not be prepared to investigate a complaint in such circumstances.

180. However, others may be able to show both that they have suffered a type and level of harm reflected in the Privacy Act, and also that the harm was caused by a breach of one or more Rules by an agency. That latter group may therefore have suffered an interference with privacy so as to trigger a possible remedy under the Act.

5 Reasonable security safeguards

Security is about more than IT protections

181. Security safeguards most obviously include **technical** IT protections that can help to prevent unauthorised access to information, or use or disclosure of that information. These are the controls built into systems to ensure people can only access what they are allowed to, to detect suspicious behaviours, and to prevent information from being accessed or taken inappropriately. Examples include access controls, multi-factor authentication, monitoring for unusual activity, protecting applications from misuse, and limiting the ability to access or download large quantities of data.

182. However, what is less well understood is that security safeguards also include **organisational** controls such as:

- embedding privacy and cyber security due diligence into procurement processes for engaging third party providers
- appropriate contractual obligations, including clarity about what personal information is involved, permitted information uses or limitations on those uses, an ability to validate compliance with legal responsibilities, and breach management processes and responsibilities
- adequate governance, both during a project, and after a process shifts to 'BAU'
- thorough risk management processes and documentation
- contract management and assurance processes that ensure that those obligations are fulfilled
- periodic review of risks, and review triggered by any material change

- testing, monitoring and re-testing (both of the vendor's system, and local integration) to ensure controls are effective and remain so
- well designed and implemented policies and processes
- staff vetting, privacy training and guidance.

183. Safeguards also include **physical** security measures, such as controlling access to premises, locking away information, clear desk policies and so on. However, since physical security is irrelevant to this breach, we have not considered it further in this inquiry.

184. Technical, physical, and organisational measures need to work together to create a broader framework to protect personal information and mitigate information security and cyber security risks. This is recognised not only by OPC's existing privacy management guidance, "Poupou Matatapu – Doing Privacy Well", but also by standards that can help to inform what Rule 5 of the Code requires (in particular the National Cyber Security Centre ("NCSC") Minimum Cyber Security Standards, relevant International Standards Organisation (ISO) standards and the Health Information Security Framework).

"Reasonable in the circumstances"

185. Rule 5 of the Code does not require an absolute security guarantee. IPP5 of the main Act is the same. It simply requires agencies to do what is reasonable to protect the information.

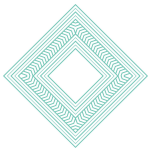
186. However, "reasonableness" is not a low threshold. Agencies must have safeguards that are proportionate to the overall risks for individuals if their information were to be lost or misused. It is OPC's consistent position that the more sensitive the personal information is, the stronger the protections are expected to be.

187. The size, complexity and resources of the agency can also influence what is proportionate and practicable in the circumstances. However, a small agency whose business is to handle high risk information (such as health information) will not be held to a lower standard simply because of its size or because security costs money. It will be expected to have strong and effective protections in place. The nature and number of those protections may simply be different from those that a large and more complex agency will be expected to deploy.

188. For example, as we discuss later, it is not reasonable to expect every individual GP practice to commission separate, independent security testing on a patient portal that it is considering using. It should be able to rely on approved, centralised testing, or testing conducted by a representative agency such as a PHO. However, even for a small practice, it is reasonable to require the practice to make sure that appropriate security testing has been done. It is also reasonable to require the practice to assess how the portal will integrate with their own patient management systems and how to train their staff to use it safely.

189. MMH and other patient health portal providers are small businesses, as are many health sector suppliers. However, their entire business is to receive and process personal health information, and make it available to patients. In MMH's case, it has also designed its portal product as a stand-alone repository of patient information.

190. All this information is inherently sensitive. In addition, patient confidentiality is a foundational principle in medicine. Health practitioners are entitled to rely on third party suppliers that support them to do everything reasonably practicable to protect the confidentiality of the information they hold. MMH and other patient health portal providers are therefore expected to have very high security standards. While MMH is a small business, the expectations on it are still substantial. Security is a fundamental requirement.



Relevant standards that inform the interpretation of Rule 5

191. We consider that what is required under Rule 5 of the Health Information Privacy Code can be usefully informed by current New Zealand government health sector security standards (the Health Information Security Framework or "the Framework").

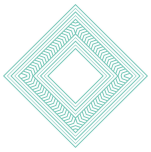
192. It is not for OPC to enforce that Framework, and we have not attempted to do so. However, the Framework is an important aid to interpreting what Rule 5 of the Code means. This is because the Framework not only sets out expectations that are specific to New Zealand health agencies handling health information, but also reflects what the sector has determined is practicable and proportionate for each category of health agency (that is, what it is 'reasonable' to expect of that type of agency).

193. It is therefore our view that health agencies can and should use those aspects of the standards that apply to them to help them understand and meet their legal obligations under Rule 5. This is particularly important where those standards are expressed as clear expectations rather than general guidance.

194. For patient portal providers, the relevant sections of those standards are those that apply to health sector suppliers. There are also separate standards for hospitals and for health sector agencies of different sizes.

195. We have also taken into consideration other recognised security frameworks, standards, and guidance that are relevant to the protection of health information and the operation of digital health services in New Zealand. This included guidance issued by the NCSC, and internationally recognised information security standards and practices, including those aligned to ISO/IEC 27001 and National Institute of Standards and Technology (NIST). The Health Information Security Framework broadly aligns with those other standards, but provides greater health sector specificity in some areas.

196. What is ‘reasonable’ will necessarily change over time, and is highly context-dependent. Importantly, it also does not depend simply on whether an agency can show it has a variety of documents, processes or controls that are set out as requirements under one or more frameworks. Instead, the question often is whether safeguards relevant to the risks involved were operating effectively in practice at the time of the incident.



6 Did MMH have reasonable security safeguards in place at the time of the breach?

Summary of findings

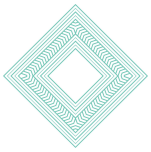
197. This incident involved the use of valid stolen patient user credentials to access the MMH platform. The credentials were probably stolen from the patient's own computer, though this is not completely clear. Regardless of how the credentials were obtained, however, the compromised user account should only have provided access to that patient's own records and no more. Instead, use of these credentials was able to result in the unauthorised access and extraction of a substantial volume of sensitive health information affecting many thousands of people.

198. This incident was not the result of a single control failure. Instead, it was the result of a combination of weaknesses across prevention, detection, and response safeguards, alongside broader issues relating to governance, oversight, and the consistent application of security practices.

199. We consider that some of the risks relevant to the incident were foreseeable before the breach occurred. While the precise sequence of events may not have been specifically anticipated, safeguards were not sufficiently effective to mitigate those risks at the time of the breach. If safeguards had been operating more effectively, both the likelihood of the breach occurring in the first place and the impact when it did would probably have been reduced.

200. Our overall assessment concludes that, at the time of the breach, MMH had not taken sufficient or reasonable steps to ensure that security safeguards were effectively implemented and operating as intended at the time of the incident.

201. **We therefore consider that MMH breached Rule 5 of the Health Information Privacy Code.**



202. Importantly, these findings do not necessarily reflect MMH's current security position. We are aware that MMH has already taken a variety of steps to improve its safeguards since the breach occurred and that it has further mitigations in train or planned. Where we have been told of those improvements, we have noted them.

203. However, we have not yet independently validated that those controls are in place and that they are operating effectively. Now that Phase 1 of the inquiry is complete, and we have determined what safeguards were missing at the time of the breach, we intend to issue a compliance notice to require MMH to complete any required remediations, and to demonstrate to our satisfaction that all the breaches of Rule 5 that were identified by this inquiry have been fixed effectively.

204. Since we have not yet independently verified that the problems at the time of the breach have been effectively remediated, we have been cautious with the details provided below, so that we do not publish information that could in itself create a security risk for the platform.

Key security safeguards where controls were not effective

205. Given that this inquiry is focused on a particular cyber security incident, the analysis below necessarily focuses on those security controls that are most relevant to that incident.

206. We have found seven areas where protections were ineffective:

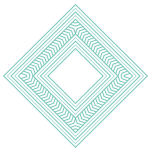
    a. The need for multifactor authentication

    b. Identity and access management

    c. Web security

    d. Patch and vulnerability management

    e. System acquisition, development, and maintenance



f. Logging and monitoring

g. Data leak prevention

207. Three further areas had only partially effective protections in place:

a. Governance, oversight and risk management

b. Information security incident management

c. Change management.

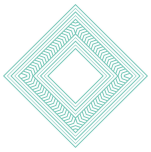
208. A full consideration of MMH's security settings is outside the scope of this inquiry and is therefore outside the scope of any compliance notice that we can issue at this time. However, we encourage MMH to undertake a broader review to ensure that all security safeguards, governance processes, and risk management practices are operating effectively in practice, and are aligned with recognised standards and good practice relevant to the protection of health information (particularly the Health Information Security Framework).

(a) Multifactor authentication

209. Relevant guidance such as the NCSC Minimum Cyber Security Standards identify multifactor authentication (MFA) as an important safeguard to reduce the risk of unauthorised access, particularly in scenarios where credential compromise is a foreseeable risk. The Office of the Privacy Commissioner has also consistently stated that MFA is a core and expected security safeguard under IPP5 for agencies that hold sensitive information.

210. While MFA varies in how useful it is as a control against credential-based attacks, and it is not sufficient on its own to protect security, we therefore consider that enforcing MFA is expected practice for organisations like MMH.

211. At the time of the incident, MFA was not enforced for end-user accounts, despite this being noted as a risk both in MMH's own privacy risk assessments and by the Northland project team. While 2FA or MFA capabilities were



available, their use was optional, and authentication to the platform could be performed using a single factor (username and password). This was despite the fact that, prior to the incident, there had been indicators of potential valid user credential exposure (such as a reported incident in June 2025).

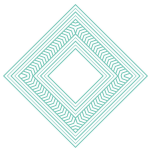
212. According to the documentation we have received, the reason for accepting the risk rather than enforcing the use of MFA was because of MMH's perception that patients did not like it, and it was a barrier to use of the platform. We support steps that ensure digital platforms remain equitable and accessible. However, it is possible to achieve that end and still maintain security. It must not be seen as a trade-off in situations where (like here) the impact of security failures on affected people is too high. The question is not whether to have MFA; it is what types of MFA to offer, so that people can select a method that suits them.

213. Indeed, MMH introduced mandatory two-step verification (2SV) using email-based one-time passwords (OTP) across all user groups in January 2026, preventing authentication without completion of the second factor. Additional MFA options have been introduced more recently, including enabling people to use authenticator applications. MMH has stated that this change has resulted in an increase in calls to their support services, but we consider that the change was necessary.

(b) Identity and access management

214. Effective identity and access management controls are intended to ensure that users are appropriately authenticated and authorised, and that access to information is restricted based on defined permissions and roles.

215. Some authentication processes were in place (except for MFA as noted above). However, authentication alone was not the primary control failure in this incident. An even more significant feature was that controls did not appropriately restrict users to only the data they were authorised to access, and



mechanisms to enforce object-level authorisation were ineffective. This meant that a single compromised account could be used to access and extract data belonging to a large number of people.

(c) Web security

216. Effective web security safeguards are intended to protect applications and users from malicious or unauthorised activity, including through controls capable of detecting and preventing abnormal or malicious activity.

217. Evidence indicated that web security controls were implemented within the environment, including a web application firewall. All user facing traffic to the platform was routed through the firewall, and these technologies provided visibility into network and web activity during the forensic investigation.

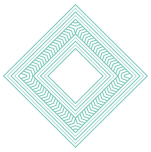
218. Despite the presence of these controls, they were not sufficiently effective to prevent, detect, or limit the malicious activity associated with the incident. It appeared that these controls were also not validated or maintained in a way that provided confidence they would reliably identify or restrict abnormal or unauthorised activity.

219. MMH states that it has now made changes to these controls to improve the ability to detect, restrict, and respond to malicious or abnormal activity.

(d) Patch and vulnerability management

220. Effective patch and vulnerability management practices are intended to support the timely identification, assessment, remediation, and validation of security weaknesses. Recognised security guidance and industry practices also emphasise the importance of effectively managing identified vulnerabilities and validating that remediation activities appropriately mitigate relevant risks.

221. Our inquiry identified recurring vulnerability themes across multiple testing and review activities over time. While MMH undertook testing and remediation activities in response to identified issues, the repeated identification of similar



classes of weakness across evolving systems and environments suggests there were broader issues relating to secure development and application security practices. This made it hard to manage vulnerabilities successfully. As a result, while earlier findings may not have related to the exact technical defect exploited during the incident, they demonstrate that similar categories of weakness continued to arise over time. MMH should have been able to identify these patterns.

(e) System acquisition, development, and maintenance

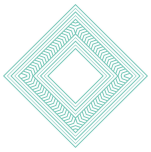
222. Effective system acquisition, development, and maintenance practices are intended to ensure that systems are securely designed, that security risks are appropriately considered during development, and that security testing and review activities are undertaken prior to production release.

223. Multiple sources of evidence indicate that while governance, development, and testing processes existed, secure design principles were not consistently reflected in development outcomes in practice.

224. We also had concerns about the effectiveness of the testing that was conducted. Vulnerabilities were repeatedly identified and subsequently marked as fixed or closed, despite similar issues reappearing in later assessments.

225. Again, the lack of secure design principles increased the likelihood that vulnerabilities could be introduced and persist within the environment. As a result, the weakness enabled a malicious external actor to deliberately use a valid stolen patient user account to access information beyond its intended scope and extract large quantities of patient information.

226. Following the incident, MMH has reportedly made several improvements aimed at strengthening secure development practices and independent security assurance. For example, MMH reports that security design practices and validation are now formally embedded into development processes.



227. MMH has also engaged an independent security provider to conduct biannual vulnerability assessments and penetration testing of infrastructure and applications.

(f) Logging and monitoring

228. Effective logging and monitoring capabilities are important safeguards for identifying malicious activity and supporting the agency to investigate and respond to cyber security incidents. Recognised security practices and guidance show the importance of maintaining appropriate visibility over security-relevant events and system activity.

229. Evidence supplied to the inquiry showed that monitoring and detection capabilities were not operating at a level that would support early identification of suspicious or abnormal behaviour. This reduced MMH's ability to respond to emerging issues before they escalated.

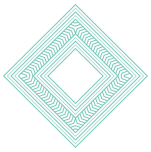
230. Indeed, this particular breach was first identified by an external partner (Health NZ) after information was published online by the hackers. It was not detected through internal monitoring mechanisms, despite large scale malicious activity occurring within the MMH systems for several days.

231. In addition, controls intended to prevent or detect large-scale access to information were not effective, allowing significant volumes of data to be accessed without interruption.

(g) Data leakage protection

232. Effective safeguards for protecting sensitive information help to ensure that access to sensitive data is appropriately restricted and that mechanisms exist to identify, detect, or limit unauthorised access, disclosure, or extraction of information.

233. The investigation identified that a substantial volume of health information was exfiltrated from the MMH environment. Multiple sources provide differing



estimates of the scale of the breach, but all numbers show that the breach was large scale (with nearly 100,000 affected people and more than 420,000 extracted files).

234. Controls intended to prevent or detect large-scale access to sensitive information were not effective or were not configured to detect real-world attack patterns. Large-scale or anomalous data retrieval was able to occur without triggering alerts or response actions. In addition, there were no effective mechanisms in place to identify or interrupt data exfiltration as it was occurring. The activity was only identified after the fact, and through external and retrospective analysis, rather than through proactive controls within the environment.

Key security safeguards where controls were partially effective

(a) Governance, oversight and risk management

235. The importance of sound governance for privacy is stressed in OPC's resource Poupou Matatapu – Doing Privacy Well. There are four core elements of governance: leadership (setting expectations and driving a sound culture); oversight, both of new proposals that may affect privacy and the wider privacy programme; accountability at a senior level for how the organisation handles personal information; and senior sponsorship of the privacy function.

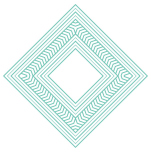
236. Typically for many New Zealand businesses, MMH is a small and very closely held company. This can create a risk of governance concentration – that is, where development and oversight functions may not be sufficiently independent of overall decision-making. It is unrealistic to expect small agencies to have the complex governance structures that larger entities can employ, but agencies whose business involves holding and managing sensitive personal information still need to ensure that their governance structures are adequate to manage the risks associated with that information.

237. We have received evidence to show that MMH had some security and privacy representation both at management level and at Board level. Managers and Board members clearly asked questions about steps that had been taken. A sample of meeting notes shows that security was actively considered at both levels, questions were asked about incidents or testing results, and remediation actions were reported back. These were useful steps. The level of reporting was light in the notes that we viewed, and did not consider privacy specifically, but more fulsome reporting may occur at different times of year.

238. MMH has informed us that it is continuing to strengthen its governance frameworks and we recommend that the approach taken by Poupou Matatapu (which is scalable for small businesses) is a valuable resource for it to use.

239. One key concern in relation to this breach is that we consider that MMH's privacy impact assessments relating to the Health NZ Northland project were weak and did not allow for effective risk management decisions either at the design level, management level or Board level. In particular, the first privacy impact assessment (PIA) we reviewed (from 2022) was largely generic rather than specific to the project. While the later PIAs to support the extension of the project to lab tests and referral notifications were more specific about what was changing, they still did not clearly describe and assess the information flows and processes. This meant that they did not adequately assess privacy and security risks associated with the proposed new process.

240. One particular aspect that was missed was the fact that the matching process for Health NZ information would import information into registered but non-activated accounts. This created privacy risks that should have been addressed. It also both led to confusion in the communications with Health NZ (which does not appear to have appreciated the difference in the terminology) and also was a material cause of substantial quantities of health information being stored in the My Health Documents module without patients having taken



active steps to activate an account. MMH has informed us that the issue has now been fixed.

241. Northland hospitals' information is still being supplied to patients through MMH. We therefore consider that it is essential that MMH should update its own PIA to more accurately reflect the way in which that information flow works, and what privacy safeguards apply to it. MMH's status as a legal 'holder' of that information makes such an update particularly important.

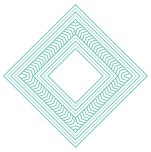
242. While it is beyond the scope of this inquiry, we also suggest that this is an opportunity for MMH to review all its PIAs over other aspects of its system to ensure that they address all relevant issues appropriately. Phase 2 of the inquiry is likely to provide some helpful indications for MMH of what else needs to be fixed.

(b) Information security incident management

243. Effective incident management capabilities are intended to support structured response, coordination, communication, escalation, and continuous improvement activities during cyber security incidents.

244. Once the incident was identified, MMH demonstrated that it was able to mobilise response activities in a timely manner, including initiating investigation, implementing containment measures, and engaging external specialists. This response occurred during a holiday period, which created real challenges for MMH, but it was still able to act promptly.

245. Evidence supplied to the inquiry indicates that incident management, and related documentation existed prior to the incident. However, the available evidence did not demonstrate that these processes had been regularly tested or exercised prior to the incident, or that the associated capabilities had reached a level of maturity proportionate to the sensitivity and scale of the information held by MMH.



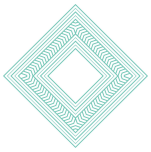
246. Again, MMH states that it is continuing to make improvements as a result of what it has learned from this incident. These include formalising incident response procedures, assigning security ownership and accountability, introducing of Board-level security reporting, and establishing of a structured security programme. These improvements are appropriate but we note that it is important not only to have documentation and processes in place, but also to validate that they work in practice.

247. Under pressure, MMH's incident management process also did not create a timely, complete and consistent view of the incident. Some degree of variability is often inevitable in the immediate aftermath of a major breach. However, the variability has been particularly noticeable in this incident – for example difficulties in assessing what information was compromised, how many people were affected and who those people were so that they could be notified. In this real-world situation, MMH's systems and processes appear to have let it down. While this will be an issue to explore further during Phase 2 of our inquiry, it appears that this may have complicated MMH's ability to support affected people and to provide clear communications to others. It will be important for MMH to ensure that its systems support it better in future.

(c) Change management

248. Effective change management practices commonly include the use of separate environments for development, testing, and production activities, together with validation processes intended to reduce the risk of unintended security impacts during system changes and releases.

249. We received evidence that indicates that MMH maintains separate environments for testing and for use by consumers. Vulnerability assessment and penetration testing activities were conducted against non-production environments, and there is evidence of some (albeit limited) validation of security fixes within production. These are positive features, which suggest that



MMH meets expectations about having environment separation as part of the development and release process.

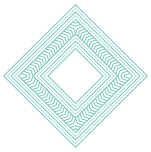
250. However, we identified concerns regarding the effectiveness of decommissioning and change lifecycle processes. Evidence provided to support account decommissioning and retention activities relied on historic examples, rather than demonstrating consistent and current operation of these processes. While this is not inherently an issue, the absence of more recent evidence, particularly in the context of material changes and the incident itself, raises questions about whether these processes were operating reliably prior to, and at the time of the incident.

251. This is further supported by post-incident improvements introducing periodic validation of account removal processes. The improvements are welcome but the need for them suggests that the effectiveness of these controls may not have been consistently verified prior to the incident.

Health sector security safeguards that were not relevant to this breach

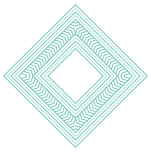
252. All health portal providers and other third party suppliers operating in New Zealand should ensure that their processes and practices reflect the expectations set out in this inquiry. A good starting point is to ensure that all relevant controls set out by the NCSC Minimum Security Standards and the Health Information Security Framework are in place. These standards tend to align closely with OPC's expectations under Rule 5 of the Code. The NIST and ISO also set out other security controls that are relevant to third party suppliers.

253. This inquiry has necessarily focused on matters that were relevant to the breach. However, there are other potential areas of vulnerability that third party suppliers such as health portals would be wise to consider. These other examples include:



- supply chain management
- test environment management
- cloud security
- endpoint security
- information backups
- cryptography
- business continuity
- asset management.

254. Since those safeguards and others like them would not have prevented or lessened the impact of the breach, we have not assessed whether MMH met those standards. However, we recommend that MMH and other health portal providers carry out all necessary checks to ensure these safeguards are effectively implemented, to prevent different kinds of breaches from happening in future.



7 Did Health NZ have organisational security controls in place at the time of the breach?

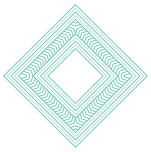
Summary of findings

255. By the time of the breach, the Northland hospital project had concluded and the transfer of patient records to MMH had become a routine process. The result of that project was therefore that hospital records relating to nearly 91,000 people were now stored in MMH accounts under "My Health Documents".

256. As discussed earlier, we consider that, under Rule 5(1)(b) of the Code, Health NZ was responsible for the design and implementation of its project to provide hospital documentation to patients through a health portal. It was required to have sufficient organisational security controls in place to make sure patient information would be kept safe.

257. More specifically, in this context, these organisational security controls involve:

- **Early due diligence** – taking all reasonable steps to ensure that its chosen provider (MMH) would protect patients' health information against unauthorised use or disclosure.
- **Risk assessment and risk management** – conducting a full privacy impact assessment, independently from the vendor, to ensure that the project steering group had a clear understanding of risks to patient privacy and how those would be mitigated.
- **Legal safeguards** in the form of sound contractual provisions that would place appropriate obligations for the safety of the information on the provider and enable Health NZ to obtain periodic assurance about compliance with the contract.
- **Ongoing monitoring** – having mechanisms to ensure the vendor continues to maintain appropriate safeguards over time including periodic auditing and



review of security assurances.

- **Appropriate governance and oversight** over the procurement process, the project design and project implementation (including once the project moved to BAU).
- **Privacy-centred project design** – including ensuring that adequate privacy advice is available throughout the project.

258. Our inquiry has found deficiencies in most of these areas. In the context of a major and novel project to supply significant quantities of personal health information to patients via a third party vendor, we consider that these deficiencies amount to a breach of Rule 5(1)(b) of the Code.

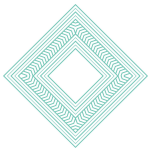
259. As with MMH, this is not a question of a failure of a single security control. Instead, it was a combination of weaknesses that resulted in Health NZ moving ahead with the project without sufficiently addressing security questions.

260. Many of what OPC considers to be reasonable security standards are also reflected in the HISF standards for hospitals. That is therefore a useful document for Health NZ to consider.

Early (pre-contractual) due diligence

261. Due diligence of suppliers in relation to their privacy and security capabilities should be embedded into standard procurement practice. Those capabilities are fundamental to whether the supplier should be selected to handle personal health information.

262. Health NZ identified MMH as its preferred supplier from the start of the project. It was an active design partner throughout the project, including being a member of the project steering group. As discussed earlier, there were a number of factors that influenced the decision to use MMH.



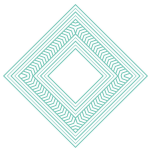
263. Health NZ specifically anticipated the need to extend the arrangements to include other portal providers in due course. However, no tender was done, and Health NZ does not appear to have systematically evaluated other providers to see whether they had a stronger security and privacy profile. Instead, it simply appears to have accepted that MMH was its most obvious partner to get the project started.

264. Health NZ was certainly conscious of the importance of security. The steering group asked for and received various representations from MMH about its security settings, including compliance with ISO standards. It also received MMH's security testing reports.

265. However, there is little evidence that Health NZ performed independent checks at the start of the project, for example by engaging an internal information security team to ask for and review MMH's security documentation, to ensure that the hospital information would be adequately protected during the transfer and matching process and once it was in the patient portal. More detailed security information was only required shortly before the discharge summary project went live in November 2023, and then only in the context of bringing Top Health (a GP practice based at Kaitaia Hospital) on board. Health NZ does not appear to have conducted its own testing until late in 2024.

266. Before that, the project team appears to have relied largely on information from the vendor when committing to the engagement and that information was not detailed enough for the context of the project. We consider that this was insufficient from a pre-contractual due diligence perspective and also from an ongoing project management perspective.

267. As noted earlier, we have evidence that Health NZ considered MMH to be a "Ministry of Health approved" supplier. It would not be surprising if this influenced whether Health NZ considered it necessary to do early independent checks. The implication is that the Ministry of Health had checked that MMH's security was adequate, and Health NZ could therefore rely on that assessment.



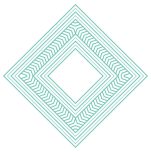
268. If there had indeed been a central checking programme, this may have been a reasonable approach (depending on the scope of that programme). However, this assumption appears to be wrong.

269. The Ministry of Health has long recognised the value of patient health portals as part of its digital health strategy. As reflected in the 2017/2018 report by the Office of the Auditor General, the Ministry has actively encouraged the take-up of portals in the health sector, supported by GP representative organisations. The Ministry of Health also conducted an assessment of the security settings in all existing patient portals in 2018. At that time – and possibly even as late as the proof of concept or pilot projects in 2020/21 – it might therefore have been possible to assert that MMH was 'Ministry-approved'.

270. However, security is not a set and forget. The digital environment is dynamic and rechecking is needed to ensure that any assessment is up to date. The Ministry in fact did not have an ongoing programme of work: the 2018 assessment seems to have been a one-off. Nor did any other organisation take on the responsibility for conducting central security testing of portals on behalf of the health sector.

271. By the time Health NZ moved into full project mode, to roll out the discharge documentation, the 2018 assessment was therefore well out of date. Rather than assuming that the Ministry had approved MMH as a supplier, Health NZ should have verified whether that was in fact the case. This would have alerted it to the fact that there was no ongoing security checking programme and that the responsibility for conducting any security checking of the patient portals had reverted to Health NZ itself.

272. As we comment later, it is our firm view that a central programme should be reinstated to validate the security of patient portals.



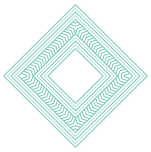
Risk assessment

273. Health NZ asked for and obtained MMH's assurance reports such as Service Organisation Control ("SOC") 2 reports and ISO certifications. This gave it a view of MMH's operations and compliance status against various international standards and best practices, which was a good start. However, there is no evidence that Health NZ conducted other potentially relevant risk assessments promptly.

274. For example, it did not appear to have conducted a cloud risk assessment against the questionnaire that was then in use for New Zealand government agencies before engaging with MMH. The only cloud risk assessment was done later in the project as part of onboarding Top Health, a primary healthcare provider located within Kaitaia Hospital. While a cloud risk assessment does not in itself provide security validation, it prompts the agency to ask appropriate questions.

275. Nor is there evidence of a proper internal security risk assessment before the discharge document project went live. Health NZ was essentially reliant on information provided by MMH to assess whether MMH had adequate security processes in place. Given the nature of this project and the sensitivity of the information, that was not sufficient.

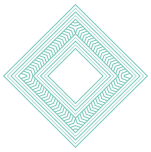
276. There does not appear to be any privacy impact assessment documentation relating to the proof of concept or the pilot project. The lack of a full PIA at this stage was a significant oversight – the project involved the routine collection, use and disclosure of large quantities of patient information. It was also a lost opportunity. A full risk assessment to support a pilot allows the agency to test the effectiveness of privacy safeguards in a controlled, real-world setting and identify any corrections that might need to be made. It is a vital source of information for both design teams and senior decision makers.



277. A member of the project team did complete a PIA in February 2023 as part of the wider rollout. That PIA was signed out by the local privacy officer who may or may not have been in a position to provide advice. (Relevant personnel have left the organisation and are no longer available to contact, which has affected the evidence that Health NZ was able to give us). However, it is clear that the burden of producing the PIA largely fell on the member of the team who had access to a template but who did not have existing privacy knowledge. It is therefore not surprising that the resulting PIA was extremely weak. We intend no criticism of the author: the problem lay with Health NZ's support for PIAs at the time.

278. For example:

- The PIA was generic in nature, rather than being specific to the information flows and processes that were involved in the project. A PIA should analyse risks arising from the specific data flow, from end-to-end.
- It did not provide sufficient detail of risks and mitigation controls to inform decision-making.
- It applied some of the IPPs incorrectly.
- It often reflected content from MMH's own inadequate PIA (including statements about security), rather than taking a more independent view.
- It was also completed only a month before the contract was signed (though it is unclear when the writing process started). Since this is the only iteration of the document that we have, we consider that this was too late to be useful. It gives the impression that Health NZ simply considered a PIA as a tick on the checklist for signoff, rather than being a tool that would be used throughout the project to help Health NZ to design the processes and safeguards appropriately.



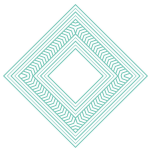
279. The quality of the 2023 PIA and the lack of other independent assessment means that we do not consider that the project steering group and senior leaders had access to the level of risk advice that was necessary to ensure that patient information would be properly protected against unauthorised use or disclosure.

280. We also consider that the lack of a proper risk assessment was a material cause of much of the compromised information being in the MMH portal. In particular, the documentation refers to hospital information being matched against “registered” MMH accounts. A more diligent enquiry should have unearthed the fact that a “registered” MMH account is different from an “activated” account. Importing patient information into registered but un-activated accounts raises very different privacy risks from those involved when information is imported into accounts that patients are actively using.

281. Health NZ now operates a centralised privacy function with a specialist team that can advise project teams, support them to produce PIAs, or review the quality of PIAs that are being written. This should make it less likely that such quality issues will arise in future, although the workload across such a large organisation still makes these findings relevant.

Legal safeguards

282. We do not have any record of agreements made between Health NZ and MMH to support either the proof of concept or pilot projects. We note that it is important to have proper agreements in place to support pilot projects, particularly given the sensitivity of health information. Such agreements will specify the safeguards that need to apply to the pilot information: for instance, whether information is live or test data, whether it is going into a live environment or is located in a sandbox and whether the information must be destroyed at the end of the pilot.

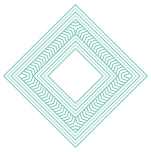


283. Health NZ and MMH signed a License and Services Agreement to support the eventual rollout of the discharge documentation. It was dated 8 December 2022, but was not signed by MMH until February 2023, and was not signed by Health NZ until 7 March 2023.

284. There is no record that it was reviewed by a legal team within Health NZ. Health NZ has told us that Northland DHB did not have an in-house legal team at that time. Nor did it have access to the level of centralised procurement and privacy advice that is now available in the organisation. This lack of support is likely to have contributed to Health NZ's failure to identify the deficiencies in the contract.

285. In our view, the contract fell short of what we would expect in order to provide sufficient legal safeguards to ensure security under Rule 5(1)(b). In particular:

- The contract is high level in nature. It seems to have been a standard contract drafted by MMH and was geared more to licensing of MMH software than to the information sharing and processing arrangement that the parties intended. In other words, it was the wrong kind of contract for the purpose.
- The contract is over-reliant on MMH's terms of use, code of conduct and privacy policy. These policies and other documents may be updated unilaterally by MMH, creating uncertainty and potentially shifting obligations. There is also no reference to Health NZ's equivalent policies.
- It did not contain clear descriptions of the information that would be collected and processed, nor how that processing was to take place.
- It did not specify in sufficient detail what safeguards were to be applied to the personal health information (such as data handling, storage, and access restrictions). Indeed, it shifted much of the responsibility for managing privacy to Health NZ and the end users. MMH's own obligations are expressed in relatively vague terms.



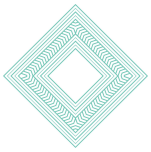
- Reference to compliance with privacy legislation was high-level and non-prescriptive.
- It did not limit MMH use of the personal health information that was to be supplied.
- Health NZ's ability to undertake assurance activities was limited.
- It did not contain incident response and breach notification obligations.
- We also note that the contract – which is still in place – was not updated to reflect later aspects of the project. It only refers to the process for receiving information from Whangārei Hospital. However, the project was extended in 2024 and 2025 to include hospital lab test results and clinic letters from different Health NZ hospitals and facilities in Northland.

286. The parties also signed an Enterprise Procurement Agreement (signed on 1 March 2023) and which is still in place. The purpose of this additional agreement was to record Health NZ's agreement to cover the cost of licences for Northland GP practices to use MMH. As such, it is a simple purchasing agreement and does not contain any further detail about respective obligations for security.

287. While the Licence and Services Agreement does provide a basis for asserting some enforceable obligations, we do not consider that it is strong enough to enable Health NZ to meet its obligations under Rule 5(1)(b) to do all that is reasonably in its power to ensure the third party service provider would protect the patient information against unauthorised use or disclosure.

Ongoing monitoring

288. The project steering group continued work after the discharge documentation phase was finalised. The project timelines and scope were extended to include



the lab test results and referral notification. These eventually went live in 2024 and 2025.

289. During that time, it is clear that the steering group were closely monitoring progress with signing up GP practices to MMH, patient take-up of the services, and implementation issues (such as lack of staff time and/or technology to support patients to create their MMH accounts in hospital).

290. It is clear that security and privacy oversight improved during these latter stages of the project. For example:

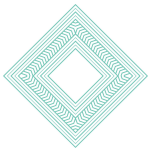
- Further documentation was required from MMH (including updated ISO certificates, and security testing reports
- A security review was conducted between Health Alliance and MMH
- A cloud risk assessment was conducted for Top Health.

291. MMH also experienced a security incident during this time that was (properly) reported to the steering group. The steering group tracked the resolution of that incident. This again shows some degree of post contractual monitoring.

292. However, most of the security assessments still substantially relied on risk assessments and security certifications issued by MMH, and the quality of the privacy assessments was still fairly low and insufficiently specific. There is also no evidence that Health NZ independently verified that remediations identified by security testing were completed and were effective.

Appropriate governance and oversight

293. The project team appears to have functioned successfully. However, while there was governance at the project steering group level, it is unclear whether information and risks were being reported up to other governance groups in Health NZ.



294. The project steering group also does not appear to have included members with expertise in security and privacy. While some privacy concepts such as obtaining patient consent were considered, we have not received evidence that privacy was a central focus for the steering group (and due to changes in personnel, it has not been possible for Health NZ to confirm this). In our view, given the scale and nature of the project, the project should have ensured it had access to this expertise, preferably as an active member of the steering group.

295. During the latter stages of the project, the lack of multifactor authentication was specifically raised as a risk to the project steering group. Advice was provided to the business owner at Health NZ who formally accepted the risk.

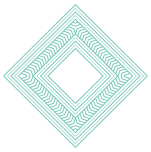
296. Unfortunately, in our opinion, the MFA advice was incomplete, and it shows the project team's lack of access to privacy experience. It focused heavily on perceived user resistance to MFA (based on MMH's stated experience rather than its own research), and noted various situations in which MFA would not help to manage risks. However, the advice did not include any consideration of situations where a patient's valid credentials were stolen and used (that is, the exact scenario that occurred with this breach) and whether MFA would provide better protection. Nor did it reflect the increasing expectations from security standards organisations and from regulators that MFA should be in place as one means of protection for highly sensitive information.

Conclusion

297. We have found that these failings were material contributors to the breach.

298. These failings relate to a project from several years ago. Health NZ now operates under a different structure, and works in materially different ways, including:

- having access to centralised legal, privacy and security advice



- new standard digital contract templates
- improvements in PIA and security assessment processes and review
- steps to ensure that Health NZ complies with the new all-of-government information sharing standard for engaging with third parties.

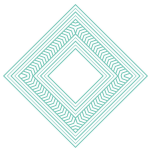
299. However, patient information is still being sent from Northland hospital facilities to patients through the MMH portal, and Health NZ is still paying the GP practice licence fees to use MMH. It is essential that Health NZ confirm that it has now done all that it can reasonably do to ensure that that information is safe.

300. We specifically expect Health NZ to prioritise the following areas (if not already done):

- Fully review all ongoing transfers of Northland hospitals' information to patients through the MMH portal, to provide assurance that the information is now secure. This includes developing a clear, accurate privacy impact assessment that is independent of MMH. That PIA should cover all aspects of the Northland hospitals' information transfers.
- Ensure that the match process has been corrected and that hospital information is only transferred to a patient's MMH account when the patient has activated that account.
- If Health NZ decides to continue with the contractual arrangement with MMH, develop a new contract that better reflects the nature of the information transfers and the obligations of the parties.

General procedures

- Require formal privacy and security risk assessments and assurance before piloting new projects or proceeding with procurement



- Establish minimum contractual standards aligned to the new government information sharing standard
- Strengthen PIA quality and timing to support decision-making, with a particular focus on ensuring that PIAs reflect the specific information flows and processes involved in a process, and that appropriate advice is received to ensure the quality of those PIAs.
- Implement ongoing vendor assurance and audit mechanisms.
- Formalise governance earlier in the project lifecycle.
- Improve documentation of risk decisions and mitigation strategies.

301. We therefore intend to issue a compliance notice to Health NZ to ensure that the relevant steps have been taken to comply with Rule 5(1)(b), and to validate that the controls in place are operating effectively

8 Reasonable security standards for primary health providers

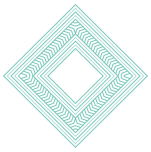
302. It is important for GP practices that use patient health portals (or other third party services) to understand that the GP practice remains responsible for the collection, security and handling of any health information that it stores, processes, makes available or transfers through that patient health portal.

303. Our recent engagements with GPs on this breach have shown that many have a gap in understanding about these obligations. It is essential that GP practices fully understand their responsibilities, given the sensitivity of the information that they handle, and the increasing prevalence of engaging third party providers to assist with aspects of managing that information.

304. As it happens in this case, GP practices did not store information in the My Health Documents module of MMH, and MMH was not handling any of that information on their behalf. Like Health NZ, they also had no direct control over MMH's technical security settings. It would therefore be unlikely that a complainant could show that any failure of their GP practice to meet 'reasonable security standards' was a material cause of the breach.

305. As a result, it has not been necessary for this inquiry to review what each individual GP practice has or has not done. There are thousands of general practices in New Zealand, and there will be significant variability in whether they engaged MMH at all, what they contracted MMH to do, what information was stored in the portal, and what patients were told.

306. Instead, we have set out our general expectations for the reasonable security safeguards that GP practices should have in place when engaging a patient health portal. We expect all GP practices to take this opportunity to review their existing settings and make sure that they are meeting these expectations for engaging with third party providers such as patient health portals.



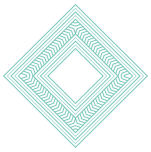
The need for more centralised verification of third party provider security

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

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

309. However, GP practices and many other health portal users (for instance, specialists) are mostly small businesses. Primary health funding does not cover the engagement of expert security and contract advisers. GPs and their staff also cannot do the work themselves: they are not security or contract specialists. While they have substantial obligations to ensure that patient information is secure, there is a real practical limit to their ability to reliably validate security documentation or assertions made by providers. Also, realistically, they are provided with 'take it or leave it' contracts. Even PHOs may have little effective market power, and individual GP practices may have none.

310. We consider that this status quo is unrealistic and unnecessarily burdensome. It leads to duplication, uncertainty and unnecessary expense for GP practices or other healthcare professionals. Checking by multiple organisations as part of due diligence or ongoing assurance also increases compliance costs and engagement costs for suppliers.



311. Australia has approached this issue by introducing, amongst other things, a registration system for health organisations who wish to access and use electronic health records including organisations offering repository or portal services (the "My Health Records" Act).

312. Whether or not the New Zealand government considers that an Australian-style approach is appropriate, we consider that central government needs to do more to improve security confidence in health sector suppliers who are an increasingly important part of the system.

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

314. We have also commented earlier that we do not consider that it is realistic to rely solely on principal agencies' ability to enforce contractual security obligations. Such an approach is unreasonably burdensome and unrealistic. GP practices are an excellent illustration of this: thousands of individual practices that use the same product should not have to take individual legal action for breach of contract to address a security failing or be recompensed for any compensation that they have had to pay to patients.

315. Instead, vendors should have direct obligations to comply with IPP5 of the Privacy Act or the equivalent Code rules, even if they are processing or storing information on behalf of the principal agency. We have recommended that the Ministry of Justice should consider amending the Act to mirror the obligations in Article 32 of the European General Data Protection Regulation.

Obligations for GP practices and other health providers

316. While certain core security issues can and should be managed at a central level, GP practices (and other health providers) still have significant obligations under Rule 5 of the Code to manage security of patient information.

317. We consider that these key obligations include:

- **Due diligence** (currently) – sighting relevant security certificates from the provider, and asking the provider to supply evidence that it has a regular and independent testing programme.
- **Due diligence** (once there is a central security validation system) – checking that the provider's security validation is current.
- **Risk assessment** – doing a privacy impact assessment, independently from the vendor, to ensure that the practice has fully thought through all aspects of integrating the portal into their patient management system, and that patients are properly informed and involved.

  While we recognise that this is burdensome for an individual practice, support may be available from a PHO, or a group of practices or PHOs that use the same technology may be able to collaborate to produce a core PIA that can then be adjusted as necessary to fit the individual practice conditions.
- **Legal safeguards** – having a basis to consider that the contract that is offered by the provider contains proper privacy safeguards and adequately explains what the provider is responsible for and what the practice is responsible for.

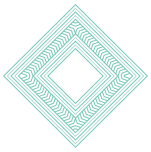
  Again, full contract consideration is likely to be difficult at an individual practice level, particularly in an environment of take it or leave it contracts. However, both the Health Information Security Framework and the new all-of-government information sharing standard set out expectations for

contracts with third parties. Any central verification system may be able to consider such issues and this would be more likely to drive change across contracts in the health sector. For example, this could mirror the model contracts approach in the GDPR.

In the absence of a central government approach, GP practices and their PHOs can collaborate to try to influence the contracts that vendors are offering.

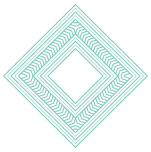
- **Periodic review** – this is a dynamic environment and settings need to be periodically checked. "Set and forget" is not a valid option.
- **Appropriate governance and oversight** over the procurement process, integration and implementation.
- **Staff training and contractual obligations** to ensure that security risks are not introduced inadvertently and that action can be taken if a staff member misuses any access to patient information or to the portal.
- **Access and credential management** to ensure that only staff who need access have it, and that the practice's access credentials are not compromised.
- **Sharing the minimum information necessary to enable the portal to invite the patient to set up an account** – do not send more information to the portal than is required for the task.

318. GP practice obligations also go beyond having reasonable security safeguards. As will be discussed in Phase 2 of this inquiry, it is GP practices who are responsible for many core privacy controls such as gaining patient consent before signing up to a portal, providing clear communications, and informing patients about the retention of their information.



319. GP practices also had a major role in supporting patients with this particular breach and we will talk to them during Phase 2 to get the benefit of their experience.

320. We also intend to visit Northland during Phase 2. We want to listen to affected GP practices and people, so that we can better understand the issues that they faced and the impact that the breach has had on the community.



9 What can others learn from the experience of this inquiry?

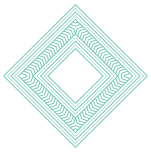
321. As this report shows, our inquiry has focused on this particular serious breach, the direct causes of that breach, and whether any failings by relevant agencies amounted to a breach of Rule 5 of the Health Information Privacy Code. However, we strongly recommend that all patient health portal providers, and all health agencies that engage with them should consider the findings carefully and review their own practices to make sure that they are meeting the expectations that we have set out.

322. It is particularly important for those organisations to understand that 'security' under the Privacy Act and its Codes requires more than carefully managed IT settings. We expect agencies to take a systemic approach – ensuring they have skilled people, secure technical systems, appropriate policies and processes, an ability to detect if things go wrong, and sound governance.

323. Other agencies that handle sensitive information, or who engage third party providers to do so for them, should also take note of the findings of this inquiry. IPP5 and Rule 5 of the Code are largely identical and many findings will be equally applicable whichever aspect of privacy law technically applies.

324. Headline lessons from Phase 1 of this inquiry include:

- The NCSC and Health Information Security Framework standards that apply to your type of organisation are useful indications of what is likely to be required under Rule 5. Make sure you meet them – they are there to help you be confident that you have the right settings in place.
- Privacy needs to be built in from the start and be part of system design – not an afterthought or a check-box exercise.
- Over-reliance on a vendor's information about its security and privacy risk profile is problematic – a degree of independent assessment is essential.



- Privacy is not a ‘set and forget’ exercise, particularly in innovative and dynamic environments such as health services – review settings from time to time and ensure that controls are still in place and operating effectively
- Make sure your contracts are fit for purpose and contain appropriate clauses to ensure personal information is protected.
- Conduct regular independent testing of security systems – but look beyond individual vulnerabilities to underlying causes, so that you stop problems from resurfacing.

Appendix A – Table showing which agencies had responsibility for security of the relevant information

	Manage My Health	Health NZ	GP practices
Hospital information supplied by Health NZ (note: only hospital discharge information affected by breach)	Once in the portal, responsible under Rule 5(1)(a) due to: • direct relationship with patients • control over the platform, accounts, and access.	Responsible under Rule 5(1)(b) for supplier engagement and for the security of the information up to the point it is delivered to patients through the portal.	Not responsible (not held by GP practices)
Patients' self-uploaded information	Responsible under Rule 5(1)(a)	Not responsible (not held by Health NZ)	Not responsible (not held by GP practices)
Patient information supplied by GPs	Not affected by this breach	Not affected by this breach (not held by Health NZ)	Not affected by breach but responsible under Rule 5 while using MMH portal for other services