Compliance Notice

Issued by the Privacy Commissioner under section 123 of the Privacy Act 2020

Issued to:	Health New Zealand – Te Whatu Ora
Notice number	CN 02/2026a
OPC File reference	CE/0603
Means of service	Email

1 Compliance notice issued

1.1. The Privacy Commissioner has determined that Health New Zealand – Te Whatu Ora (**Health NZ**) failed to comply with the requirements of Rule 5(1)(b) of the Health Information Privacy Code 2020 (**the Code**) in relation to the provision of hospital documentation in Northland to patients through the Manage My Health (**MMH**) portal. As such, the Commissioner has decided to issue this compliance notice under section 123 of the Privacy Act 2020 (**the Act**). The basis for the Commissioner's decision is set out in section 4 of this notice.

1.2. To remedy its non-compliance with the Code, Health NZ is required to take the steps set out in the Schedule to this notice, within the specified timeframes.

1.3. The Commissioner has provided Health NZ with the opportunity to comment on a draft of this notice, as required by section 124(3) of the Act, and the Commissioner has taken those comments into account before issuing this compliance notice.

2 Background

2.1. Health NZ was established under the Pae Ora (Healthy Futures) Act 2022 and replaced 20 District Health Boards (**DHBs**) including the Northland DHB. Health NZ assumed the contracts, responsibilities and liabilities of the DHBs.

2.2. Following the Northland DHB's pilot project to use the MMH digital portal to send Whangārei hospital discharge documentation to patients, Health NZ established a

project in 2023 to expand this use of the MMH portal for sending patient discharge information from other Northland hospitals to patients.

2.3. On 31 December 2025 a cyber security breach affected the MMH patient portal in which a large amount of patient information was extracted by criminal threat actors. The cyber security breach affected around 99,416 individuals in total.

2.4. Approximately 91% of affected individuals were Health NZ patients in Northland. This was due to the unique arrangement between MMH and Health NZ to make hospital discharge documentation available to patients through the MMH patient portal. The compromised information amounted to 403,730 Health NZ documents stored in the specific module called “My Health Documents”.

2.5. On 6 January 2026, Health NZ reported a notifiable privacy breach to the Commissioner, as required under section 114 of the Act, due to its supply of patient information to the MMH patient portal.

2.6. The Commissioner announced an inquiry on 21 January 2026 under section 17(1)(i) of the Privacy Act. The inquiry is being conducted in two phases.

2.7. The Commissioner’s findings about Health NZ’s responsibility for the security of the information affected by the cyber security breach under the Code are set out in the phase one inquiry report dated 25 May 2026 (**Inquiry Report**). As almost 40% of people in Northland are Māori, the Privacy Commissioner found that the cyber security breach was therefore likely to have had a disproportionate effect on Māori.

3 Breach of the Health Information Privacy Code – rule 5(1)(b)

3.1. The Commissioner found that Health NZ did not meet its obligations to ensure patient information would be protected to the required standards for due diligence, contract drafting, governance, risk management and ongoing assurance. These failures amounted to a breach of rule 5(1)(b) of the Code, as set out in the Inquiry Report.

3.2. As a “health agency”, Health NZ has the obligation under rule 5(1)(b) of the Code to ensure that, if it is necessary for the information to be given to a person in connection with the provision of a service to Health NZ, including any storing, processing, or destruction of the information, everything reasonably within the power of Health NZ is done to prevent unauthorised use or unauthorised disclosure of the information.

3.3. The information that Health NZ provides to MMH in connection with a service is "health information" as defined under clause 4(1) of the Code. It is information about health services provided to identifiable individuals. While hospital discharge documents do not reveal the patient's full medical record, details of events and procedures can reveal intimate information about individual patients. The health information is sensitive at the individual level and can also be sensitive for a person's whānau or hapū. It may include information about hospital admissions and personal or health information such as name, address, National Health Index number and medical history.

4 Relevant decision factors

4.1. As set out in the Inquiry Report, the Commissioner determined that Health NZ was responsible for having the necessary organisational security controls in place to make sure patient information would be kept safe when providing hospital documentation through MMH's patient portal, but there were deficiencies in these organisational controls that meant Health NZ had not complied with the expected security standards. Those deficiencies were found to be contributing factors to the cyber security breach. In particular:

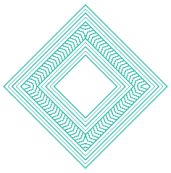
a. Health NZ did not conduct sufficient due diligence before it decided to engage MMH.

b. There were serious problems with the quality of the privacy risk assessments, though things improved somewhat in the later stages of the project.

4.2. The way in which the MMH system would manage the information provided by Health NZ was insufficiently understood by Health NZ and key technical issues were not identified.

4.3. Health NZ's project team appear to have relied too much on assessments about the security and privacy of information provided by MMH, rather than taking a more independent view.

c. In 2023 there was an active project steering group and senior leadership for the project to expand the use of MMH portal to Northland hospitals, but that group did not include direct privacy or security representation as would be expected for a project of this novelty, complexity and scale.



d. There was 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).

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

4.4. Following completion of the Inquiry Report, Health NZ informed the Commissioner that it had stopped providing patient health information to MMH.

4.5. However, the breach is not a matter that is solely of historic interest. Health NZ has informed the Commissioner that it is likely to consider other digital solutions for sharing hospital information with patients in the future. The Commissioner has therefore identified the steps that Health NZ must take to ensure it does not repeat the breach of rule 5(1)(b) that was identified by the inquiry, and that it is meeting its security obligations if supplying this patient information to a third-party service provider in the future.

4.6. In deciding to issue this compliance notice, the Commissioner has taken into account the public interest in holding Health NZ accountable for its security obligations under the Code and requiring Health NZ to ensure its compliance with those obligations. Health NZ is a central provider of health services within the New Zealand public health system. The management and mitigation of privacy and security risk in relation to sensitive health information supports the recovery of public trust and confidence in the use of digital services in the public health sector following a major cyber security breach.

4.7. In deciding to issue this compliance notice, the Commissioner has concluded that a compliance notice is necessary to remedy Health NZ's breach of rule 5(1)(b) of the Code, taking into account the following matters under section 124(1) of the Act.

4.8. There is no other appropriate available means under the Act to deal with the breach of the Code by Health NZ, other than by investigating individual complaints by affected individuals. The Commissioner considers that the failure to comply with rule 5(1)(b) of the Code requires independent verification that appropriate measures are put in place to support the recovery of public trust and confidence in the use of digital services in the public health sector following the major cyber security breach which Health NZ's

breach of the Code contributed to. This is not a measure available as part of the investigation of an individual's complaint or other less formal regulatory interventions available to the Commissioner.

4.9. The breach of the Code was particularly serious, given the sensitivity of the affected health information and the resulting cyber security breach having impacted public trust and confidence in the health sector's use of patient portals.

4.10. The steps that Health NZ has reported it has taken following the cyber security breach should reduce the likelihood of Health NZ's breach of the Code being repeated. Health NZ is likely to consider other digital solutions for sharing hospital information with patients in the future. It is therefore necessary for Health NZ to take the steps required by this notice to further reduce the likelihood that this breach of the Code could be repeated in future.

4.11. A significant number of people (approximately 99,416) have been affected by the breach of the Code resulting in the cyber security breach, particularly patients in Northland and with a likely disproportionate effect on Māori patients.

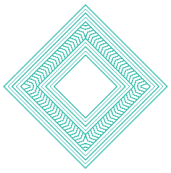
4.12. Health NZ has been co-operative in its dealings with the Commissioner and accepts that its obligations under rule 5(1)(b) of the Code were not complied with. The Commissioner recognises that Health NZ raised the cyber security breach affecting the MMH portal with the provider and Health NZ's efforts to respond to the security breach.

4.13. It has not been possible to estimate the costs of complying with the notice, however Health NZ is already working towards meeting these requirements to address the Commissioner's findings in the Inquiry Report as fundamental security and privacy requirements.

5 Requirements of this notice to remedy the breach

5.1. Health NZ is required by this notice to take the particular actions set out in the Schedule attached to this notice.

5.2. These actions are required to ensure that Health NZ does everything reasonably within its power to prevent the unauthorised use or disclosure of the health information



Health NZ supplies in connection with digital services for the distribution of hospital discharge information to patients by or through any third-party service provider.

5.3. Health NZ is required to report to the Commissioner on the actions taken to remedy the breach by the dates set out in the Schedule.

6 Enforcement, appeal, and publication

6.1. Under section 131 of the Act, Health NZ has the right to appeal this compliance notice, in whole or in part, to the Human Rights Review Tribunal (**Tribunal**). The Tribunal may allow an appeal for one of the reasons listed at section 131(3) of the Act. An appeal must be lodged in the Tribunal within 15 working days of this notice being issued.

6.2. The Commissioner may bring enforcement proceedings in the Tribunal if there is reason to believe that Health NZ has not remedied the breach as required by this notice or fails to report to the Commissioner on the steps taken to remedy the breach as required by this notice (sections 130 and 133 of the Act).

6.3. The Commissioner may publish details of this compliance notice in accordance with section 129 of the Act.

Compliance Notice issued at Wellington, New Zealand:

Michael Lindo Charles Webster
Privacy Commissioner

Dated: 22 September 2026

Schedule – Required Actions

Actions required:

In order to ensure that everything reasonably within the power of Health NZ is done to prevent unauthorised use or unauthorised disclosure of patient health information when procuring digital services for the distribution of hospital discharge information to patients (**services**) by or through third-party service providers (**providers**) (**the MMH Replacement Project**), Health NZ must implement a project plan that appropriately identifies and manages privacy and security risk from governance, procurement, and implementation perspectives.

At a minimum, the project plan must include the following requirements and measures to be taken when procuring the services by or through a provider(s) for the MMH Replacement Project.

Issue A: Project governance

1. Health NZ must ensure that there is a project steering group, with links to broader governance groups and led by a senior staff member.
2. The project governance group and project steering group will include privacy and technical security expertise.
3. Privacy and security will be standing items on project governance group and project steering group agendas.

Issue B: Privacy risk management

1. As part of the services procurement process Health NZ must carry out initial privacy assessments of the provider(s) and their portal solutions. These must be carried out independently of any provider and Health NZ's privacy team must have appropriate input into them.
2. At the system and process design stage, Health NZ must carry out a privacy impact assessment. This must include a detailed assessment of the information flows between Health NZ and the provider(s). This must be carried out independently of any provider and must be reviewed by Health NZ's privacy and legal specialists.
3. The privacy impact assessment must be reviewed and updated:
    a. immediately prior to the implementation of the MMH Replacement Project;

b. Prior to any extension of the data points included in the MMH Replacement Project; and
c. Prior to any expansion of the geographic scope of the MMH Replacement Project beyond the Northland region.

4. The privacy impact assessment must be reviewed annually once the MMH Replacement Project is implemented, with a system in place to ensure that those reviews are carried out.
5. Health NZ must consult with the Office of the Privacy Commissioner before the MMH Replacement Project is implemented.

Issue C: Information security requirements and processes

1. Project documentation must record:
    a. clearly defined cyber security and privacy requirements for the services provided to Health NZ;
    b. evidence that each potential provider selected by Health NZ at the outset of the MMH Replacement Project has been independently assessed against the Health Information Safety Framework (or any replacement framework) and has met a suitable standard for use as part of the project, prior to entry into any contract for the services; and
    c. a requirement that all providers must provide Health NZ with a live demonstration of their product's compliance with HISP prior to entry into any contract for the services.
2. Health NZ must use security testing attestation processes that meet the National Cyber Security Centre Minimum Cyber Security Standards (or any replacement standards or frameworks).
3. If any independent reviews of digital forensic and incident reports for providers are completed, the findings and recommendations must be recorded in a way that can inform Health NZ's ongoing security practices.

Issue D: Contracting processes

1. Contracts with providers must include:
    a. Robust privacy and security obligations on the provider and its sub-contractors (if permitted) including obligations on the provider and its sub-contractors to remediate issues of concern and risks to health information through enforceable contract terms.
    b. An obligation on the provider to provide Health NZ with the effectiveness of the provider's security controls and incident mitigation following any cyber security incidents.
    c. Security incident and privacy breach notification obligations on the provider, which make it clear when the provider is required to make such notifications to Health NZ.
    d. Regular assurance reporting obligations on the provider covering compliance with the provider's contractual obligations, the protection of health information supplied by Health NZ and confirmation that the provider's security and privacy safeguards are operating as intended.
    e. Audit powers to ensure Health NZ can:
        i. Regularly assess security risks during the term of the contract.
        ii. Check that health information supplied by Health NZ is used and retained by the provider as intended under the contract.
        iii. Check that the services are being delivered in accordance with agreed processes and systems.
    f. A process to enable issues of concern identified by the provider or by Health NZ to be escalated and resolved.
2. Legal advice must be required before Health NZ enters into contracts with providers for the services.

Timeframe for completion:

These actions must be taken by **29 January 2027**.

Evidence of action completed:

On or before **12 February 2027**, Health NZ is required to supply the Commissioner with copies of the project plan developed and implemented to satisfy these actions.

Condition of notice – further information

Health NZ must also provide any further information in relation to these actions that is reasonably required by the Commissioner to ensure and verify that the actions have been completed.