Compliance Notice

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

Agency	Manage My Health Ltd NZBN: 9429032552072
Notice number	CN 01/2026
File reference	CE/0603
Means of service	Email

1 Compliance notice issued

1.1. The Privacy Commissioner has determined that Manage My Health Ltd (**MMH**) failed to comply with the requirements of rule 5(1)(a) of the Health Information Privacy Code 2020 (**the Code**). 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, MMH is required to take the steps set out in the Schedule to this notice, within the specified timeframes.

1.3. The Commissioner has provided MMH 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. MMH is one of several health portal companies operating in New Zealand. It contracts with GP practices and other health agencies to provide certain digital services to patients, such as booking appointments, ordering repeat prescriptions and video-calling. Patients with activated accounts can 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 and laboratory test results). Patients with activated accounts can also upload their own documents if they wish.

2.2. On 31 December 2025 a cyber security breach affected the Manage My Health 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.

2.3. Approximately 91% of affected individuals were Health New Zealand – Te Whatu Ora (**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.

2.4. The compromised information amounted to 403,730 Health NZ documents and 22,609 documents that had been uploaded by patients.

2.5. The only module in the MMH patient portal affected by the cyber security 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.

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 MMH'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 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)(a)

3.1. The Commissioner found that MMH did not meet its obligations under rule 5(1)(a) of the Code to ensure patient information it held in the My Health Documents module of the portal was protected, by such security safeguards as are reasonable in the circumstances to take, against loss, access, use, modification, or disclosure that is not authorised by MMH, and other misuse.

3.2. The Code applies to “health agencies” that are dealing with “health information”.

3.3. MMH falls under the definition of 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.”

3.4. 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 an individual has received or is receiving, information derived from the testing or examination of any body part, or any bodily substance of that individual, or incidental information that was collected as part of providing any health or disability services.

3.5. At the time of the breach, MMH’s key security safeguards were ineffective and did not meet the requirements of rule 5(1)(a) of the Code. These are set out in more detail below.

3.6. What is required of a health agency under rule 5 of the Code can be usefully informed by current New Zealand government health sector security standards, including the Health Information Security Framework.

4 Relevant decision factors

4.1. As set out in the Phase 1 Inquiry Report, the Commissioner determined that MMH was responsible for having the necessary security standards in place to make sure patient information was kept safe within the portal, but that there were deficiencies in these controls that meant that MMH had not met the expected security standards. In particular, the Report set out seven areas where security protections were ineffective:

a. The need for multifactor authentication (MFA)

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.

4.2. The Commissioner has identified the steps that MMH must now take to ensure it meets its security obligations under rule 5(1)(a) of the Code. In taking the step of issuing this compliance notice, the Commissioner considers that there is a substantial public interest in holding MMH accountable for its security obligations under the Code and requiring MMH to ensure its compliance with those obligations.

4.3. 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 cyber security breach. MMH is one of the major providers of patient health portals in New Zealand. At the time of the breach, MMH reported that it had 1.8 million registered users. Ensuring that MMH has remedied the issues that led to the breach is important in restoring trust in both MMH and patient portals more generally.

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

4.5. There is no other appropriate available means under the Act to deal with the breach of the Code by MMH, other than by investigating individual complaints from affected individuals. The Commissioner considers that the failure to comply with rule 5(1)(a) of the Code requires independent verification that reasonable security safeguards have been put in place to prevent this breach from continuing or recurring. This is not a measure available as part of the investigation of an individual's complaint.

4.6. The breach of the Code was particularly serious, given the sensitivity of the affected health information held in the patient portal and the resulting cyber security breach. The breach was also serious because the health information was accessed by malicious actors (the hackers) who published at least some of the information on the dark web. The circumstances of the breach mean the information can never be recovered.

4.7. Based on the information provided by MMH in phase one of the Commissioner's inquiry, the Commissioner considers there is a real likelihood of a repeat of the breach of the Code. While MMH states it has taken steps following the cyber security breach that will address the breach of the Code, these have not been verified by the Commissioner. The Commissioner considers it is necessary for MMH to take the combination of steps required by this notice to reduce the likelihood of a repeat of the breach of the Code (which may include some steps already taken by MMH) and for the Commissioner to independently verify that these appropriate steps have been taken.

4.8. A large 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.

4.9. MMH has been co-operative in its dealings with the Commissioner, which are continuing under phase two of the Commissioner's inquiry. MMH has also taken proactive steps to address its non-compliance with the Code since the incident, including the implementation of MFA, IAM, and web security controls.

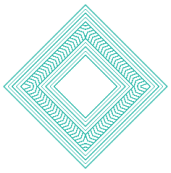
4.10. It has not been possible to estimate the likely cost of complying with the notice. Based on the information provided in phase one of the Commissioner's inquiry, some cost will have been incurred already. The Commissioner considers it is appropriate for MMH to expend the resource required in order to remedy the breach of rule 5(1)(a) of the Code, as the remediations relate to fundamental security and privacy requirements for sensitive health information.

5 Requirements of this notice to remedy the breach

5.1. MMH is required by this notice to take specific actions to ensure that MMH does everything reasonably within its power to prevent the unauthorised use or disclosure of health information stored within the MMH portal.

5.2. The specific actions that MMH is required to take are set out in the Schedule – Required Actions.

5.3. MMH 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, MMH has the right to appeal this compliance notice, in whole or in part, in 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 MMH 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 sections 129 of the Act.

Compliance Notice issued at Wellington, New Zealand:

Michael Lindo Charles Webster
Privacy Commissioner

Dated: 28 August 2026

Schedule – Required Actions

Issue A: Patch and vulnerability management

Action required:

To ensure that vulnerabilities are effectively identified, managed, and remediated in a structured and consistent manner proportionate to the sensitivity and criticality of the information and systems involved, MMH is required to implement and maintain effective vulnerability management controls by taking the following action:

1. Develop and implement appropriate standards, policies and/or procedures that:
    a. specify timeframes for the remediation of vulnerabilities that are appropriate to their level of risk.
    b. ensure that remediation activities address underlying causes of vulnerabilities, particularly where similar issues have been identified over time.
    c. ensure that remediation activities are validated to confirm that identified vulnerabilities have been effectively addressed in practice.
    d. ensure that recurring vulnerability themes are identified and treated as indicators of broader issues requiring systemic remediation.
    e. ensure that vulnerability management activities are subject to appropriate governance, including oversight of remediation progress and formal risk acceptance where applicable.

Timeframe for completion:

This action must be taken by **26 February 2027** [six months from date of issue of notice].

Evidence of action completed:

On or before **26 March 2027**, MMH is required to supply the Commissioner with satisfactory evidence that the above action has been completed. The evidence is to include, but is not limited to:

- The documented standards, policies, and/or procedures developed and implemented.
- Records demonstrating the implementation of those standards, policies and/or procedures including:
    - examples across a range of severity levels.

- evidence of frequency and outcomes of testing or security assessment.
- evidence demonstrating that remediation activities occur within the defined or risk-appropriate timeframes.
- evidence demonstrating that remediation actions have been validated (e.g. retesting outcomes, verification activities, or equivalent assurance).
- outputs from recent penetration testing or security assessment, together with evidence of how identified vulnerabilities have been managed and resolved.
- evidence demonstrating how recurring vulnerability themes are identified and addressed, such as aggregated analysis, root cause reviews, or improvement initiatives.

- Governance and oversight artefacts demonstrating monitoring of vulnerability management activities, including escalation and risk acceptance where applicable.

By **31 August 2027**, MMH is required to supply the Commissioner with satisfactory evidence of a second report demonstrating outputs from penetration testing or security assessment, together with evidence of how identified vulnerabilities have been managed and resolved. This report must demonstrate outputs that occurred at least six months after the report above.

Issue B: System acquisition, development, and maintenance

Action required:

To ensure that systems are securely designed, developed, tested, and maintained, MMH is required to implement and maintain effective secure development and system assurance controls, by taking the following action:

1. Develop and implement appropriate standards, policies and/or procedures in order to effect a structured secure development lifecycle that incorporates security considerations throughout system acquisition, development, and maintenance. These standards, policies and/or procedures should ensure that:
    a. secure-by-design principles are applied in development activities, including appropriate controls for access management, API security, and protection of health information.
    b. vulnerabilities identified through development and testing activities are incorporated into a consistent process for remediation and closure.
    c. recurring vulnerability themes identified through testing or operation are used to inform improvements in development practices.

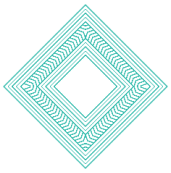
Timeframe for completion:

This action must be taken by **26 February 2027** [six months from date of issue of notice].

Evidence of action completed:

On or before **26 March 2027**, MMH is required to supply the Commissioner with satisfactory evidence that the above action has been completed. The evidence is to include, but is not limited to:

- The documented standards, policies, and/or procedures developed and implemented.
- Records demonstrating the implementation of those standards, policies and/or procedures including:
    - evidence of security design or review activities conducted as part of system development or change processes.
    - evidence demonstrating how recurring vulnerability themes are identified and addressed through improvements to development practices.



- evidence demonstrating that vulnerabilities identified through testing are tracked, remediated, and validated.
- evidence demonstrating independent validation or assurance of security controls prior to or following production release.

Issue C: Logging and monitoring

Actions required:

To ensure that security relevant activity is appropriately monitored, detected, and responded to, MMH is required to implement and maintain effective logging and monitoring controls, by taking the following actions:

1. Develop and implement defined operational processes for reviewing, triaging and responding to security alerts including appropriate measures to ensure that:
    a. Logs are retained and accessible to support investigation and response activities.
    b. Log data is monitored and analysed to identify suspicious, abnormal, or unauthorised activity.
    c. Security alerts are configured to identify relevant threat scenarios and are actively monitored.
    d. Logging and monitoring controls are capable of supporting timely detection and response to incidents in practice.

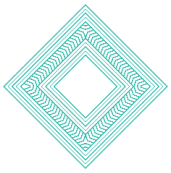
Timeframe for completion:

These actions must be taken by **30 November 2026** [three months from date of issue of notice].

Evidence of actions completed:

On or before **22 January 2027**, MMH is required to supply the Commissioner with satisfactory evidence that the above actions have been completed. The evidence is to include, but is not limited to:

- Records demonstrating the implementation of the processes including:
    - evidence demonstrating monitoring and detection capability.



- evidence of configured alerting for relevant security events or abnormal behaviour.
- evidence demonstrating detection and response to security events.
- evidence demonstrating retention and accessibility of logs sufficient to support investigation activities.

Issue D: Data leak protection

To ensure that sensitive health information is protected from unauthorised disclosure or exfiltration, in a manner proportionate to its sensitivity and volume, MMH is required to implement and maintain effective data loss prevention controls, by taking the following actions:

1. Ensure data loss prevention controls are in place to:
    a. detect and prevent unauthorised access to, or extraction of, health information.
    b. ensure MMH can accurately identify, analyse, and quantify data access and potential exfiltration during an incident.
    c. ensure suspected data exfiltration events generate alerts and are responded to in a timely manner.
2. Implement logging, monitoring and alerting to identify bulk data access, export activity, and anomalous data access patterns.

Timeframe for completion:

These actions must be taken by **30 November 2026** [three months from date of issue of notice].

Evidence of actions completed:

On or before **22 January 2027**, MMH is required to supply the Commissioner with satisfactory evidence that the above actions have been completed. The evidence is to include, but is not limited to:

- Documentation describing data loss prevention controls and how they apply to health information.

- Evidence demonstrating controls implemented to detect and restrict bulk data access or extraction.
- Evidence of logging, monitoring, and alerting for abnormal or high-volume data access patterns including relevant configuration and sample outputs.
- Evidence demonstrating detection and response to data access or exfiltration events.
- Evidence demonstrating the ability to identify and quantify data access during an incident or investigation.
- Outputs from testing or validation activities demonstrating the effectiveness of web security controls.

Condition of notice – further information

MMH is required to provide the evidence set out above to the Commissioner by the dates specified. MMH must also provide any further information in relation to these actions that is reasonably required by the Commissioner to ensure and verify that an action has been completed.