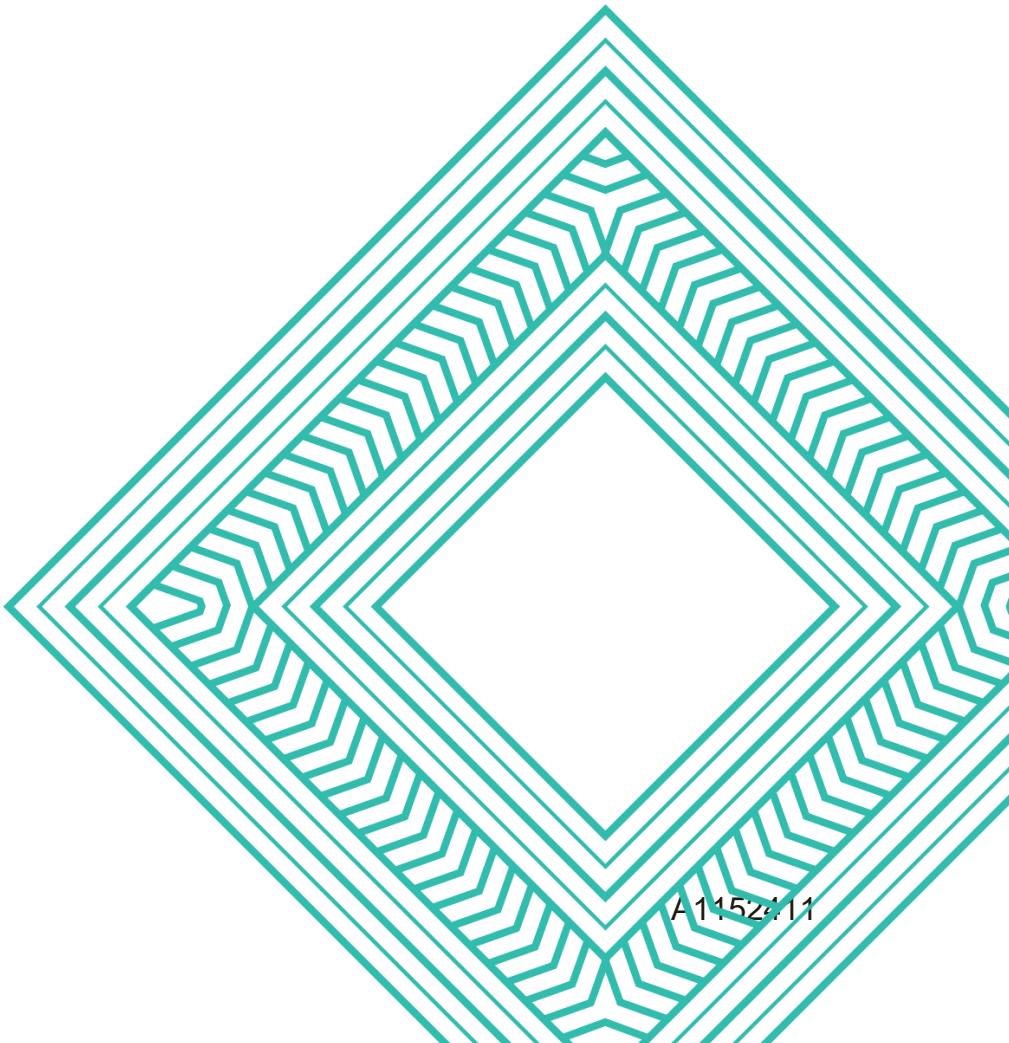
Privacy Commissioner
Te Mana Mātāpono Matatapu

Terms of Reference

Privacy Commissioner's Inquiry into the Cyber Security Breach affecting the Manage My Health Limited patient portal

January 2026



A11524111

Privacy Commissioner
Te Mana Mātāpono Matatapu

Terms of reference

Privacy Act 2020 – Inquiry under section 17(1)(i) into the cyber security breach affecting the Manage My Health Limited patient portal.

Background and context

Manage My Health Limited (**MMH**) is a private business operating a patient portal used by some general practices around New Zealand and other parts of New Zealand's health sector. The portal holds medical information and enables patients to communicate with health professionals and store their personal health documents for convenient access. On 1 January 2026 MMH notified the Office of the Privacy Commissioner (**OPC**) of a security breach affecting its patient portal. MMH reported unauthorised access to a document module of its patient portal by a ransomware attack. The attackers published a sample of the personal information obtained online. This incident is referred to as the "cyber security breach" or "breach".

On 6 January 2025 Health NZ–Te Whatu Ora (**HNZ**) notified OPC that discharge summaries from Northland Hospital stored in the MMH portal had been affected by the cyber security breach.

The breach has been extensively reported in the media and individuals have raised their concerns and initial complaints about the breach with OPC.

The affected patient information includes sensitive personal information and health information, such as clinical notes, lab results, vaccination records, and medical photographs. It also includes personal identification details, such as names, birth dates, addresses, email addresses, and phone numbers. OPC understands that over 100,000 New Zealanders may have been affected by the breach.

Purpose and objectives of the Inquiry

The purpose of this Inquiry is to establish the circumstances of the cyber security breach. It will also address the impacts on affected individuals, compliance with relevant standards and compliance with the Privacy Act.

As New Zealand's privacy regulator, the Privacy Commissioner has a public assurance function and may make public comment on privacy issues that are of serious concern to the public.

The Inquiry supports the Privacy Commissioner's regulatory response under the Privacy Act including the investigation and conciliation of complaints from affected individuals under Part 5 of the Act, the investigation of potential compliance issues under Part 6(2), and the Commissioner's advisory and guidance functions.

Information, analysis and the conclusions drawn from phases of the Inquiry will support these further aspects of the Commissioner's response under the Privacy Act that can progress alongside the Inquiry.

Matters in scope of this Inquiry

The Inquiry is to investigate, make findings and report on:

- the context for and causes of the cyber security breach
- the scale of the incident and patient information affected
- people's experience of the breach, including whether any communities have been disproportionately affected by the cyber security breach
- the adequacy of the security safeguards in place at the time of the cyber security breach
- the relevant policy, contractual, and governance arrangements in place at the time of the breach between MMH, HNZ, primary care providers, Primary Health Organisations, and other health sector agencies
- whether relevant policies and processes were complied with

- whether the Privacy Act framework has been complied with, including the Health Information Privacy Code 2020.

The Inquiry may also comment and make any relevant recommendations or findings as appropriate on any associated matters, including:

- the adequacy of the breach response, including the process of notification to affected individuals and to the Privacy Commissioner
- patient access to their information on the MMH portal during the response to the cyber security breach
- the security and governance framework for the protection of sensitive patient information within patient portals
- transparency and awareness of patients about the handling and retention of their information on the MMH portal
- policies and processes concerning the collection and retention of patient information on the MMH portal
- other matters arising relating to the storage and security of health information and personal information within the health sector.

Matters out of scope of this Inquiry

The Inquiry will not consider:

- the responses of government agencies not within scope of the Inquiry, the National Cyber Security Centre or the Police to the cyber breach, including the handling of the ransom demand and criminal matters by the New Zealand Police.

Privacy Commissioner's functions and powers

The Inquiry is a Commissioner initiated inquiry under section 17(1)(i) of the Privacy Act. The Privacy Commissioner may inquire generally into any matter including any

practice or procedure, whether governmental or non-governmental, or any technical development, if it appears that the privacy of the individual is being or may be infringed.

In exercising functions and powers under the Act, the Commissioner acts independently and with regard to cultural perspectives on privacy as well as other matters.

As part of the Inquiry, the Privacy Commissioner may use statutory powers to summon witnesses and obtain relevant information and documentation under section 203 of the Act from any organisation or individual that is considered to have information pertinent to the Inquiry. Section 89 of the Act applies, and information and documentation collected as part of this Inquiry is privileged under section 90 and will be held subject to section 206, OPC's obligation of secrecy.

Methodology

Inquiry phases

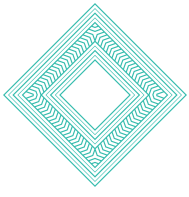
The Inquiry will be carried out in phases to ensure an efficient and effective response to the cyber security breach, and to support the exercise of any relevant functions under the Privacy Act:

Phase one

The initial phase of the Inquiry will consider and reach findings on preliminary issues relating to security safeguards under information privacy principle 5 and the respective responsibilities of MMH, HNZ and users of the MMH portal for the security of patient information held within the portal.

The Commissioner's findings through the initial phase of the Inquiry will inform:

- any specific advisory or compliance response by OPC to particular issues raised by the cyber security breach as provided by the Privacy Act



- the investigation and conciliation of complaints from individuals (or their representatives) about an interference with their privacy.

As these preliminary issues are established, OPC will progress any complaints by individuals under Part 5 of the Act as appropriate. The progression of complaints are dependent on this information from phase one.

Phase two

Phase two will address remaining matters in scope of the Inquiry. The second phase of the Inquiry will:

- make any findings and recommendations on matters not covered in phase one
- consider whether additional inquiry phases are needed.

As above, the Commissioner's findings through phase two of the Inquiry will inform the relevant complaints, investigation and advisory functions that are part of OPC's response to concerns relating to the breach.

Technical expertise and public submissions

The Commissioner will consult independent technical cyber security experts and may establish a technical advisory group for the purposes of the Inquiry.

The Commissioner will also consider information and evidence from relevant parties. The Commissioner may meet with interested groups or experts and may call for information and comment on any matter or issue relating to this Inquiry

Timeframes and reporting

Commencement

The Inquiry commences on 28 January 2026.

Phase one is estimated to be completed by 30 April 2026. This timeframe is dependent on OPC receiving independent cyber security advice and timely responses from relevant parties in response to information requests.

The scope of phase 2 will be confirmed following completion of phase one. Timing will be dependent on the scope of the remaining issues and cooperation from relevant parties.

Other aspects of the Commissioner's response to the cyber security incident, including the management of complaints by individuals under Part 5 of the Privacy Act, are not subject to the Inquiry's expected timeframes.

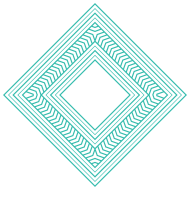
Recommendations

During any phase of the Inquiry, in addition to recommendations on any of the matters in scope in relation to MMH, the Privacy Commissioner may make any relevant recommendations to reduce the risk of cyber security incidents affecting patient portals, including wider system improvements, as necessary, to ensure patient trust and confidence in the protection of sensitive personal and health information.

Publication

The Privacy Commissioner intends to publicly report at the end of each phase of the Inquiry. These reports will include any relevant recommendations.

The Commissioner may also make interim statements during the course of the inquiry about relevant developments, including OPC's advice and recommendations to relevant parties.



Relationship to other Reviews into the Manage My Health cyber incident

The Privacy Commissioner regulates the use, collection and management of health information under the Privacy Act 2020 and the Health Information Privacy Code 2020. This Inquiry is independent from any other review or investigation into the MMH cyber breach and is being undertaken using the Privacy Commissioner's section 17(1)(i) inquiry powers. These powers allow the Commissioner to require the provision of information from any reviews or investigations, including from individuals, that are pertinent to his lines of inquiry. The Commissioner's findings will inform advisory or compliance action, investigation and conciliation of complaints from individuals or their representatives and recommendations for improvement at the agency, sector and system level.