MINISTRY OF HEALTH
MANATŪ HAUORA

133 Molesworth Street
PO Box 5013
Wellington 6140
New Zealand
T+64 4 496 2000

10 June 2025

s 9(2)(a)

Ref: H2025066843

Tēnā koe s 9(2)(a)

Response to your request for official information

Thank you for your request under the Official Information Act 1982 (the Act) to the Ministry of Health – Manatū Hauora (the Ministry) on 13 May 2025 for information regarding the Ministry's usage of artificial intelligence (AI). You requested:

> *"I'd like to know how much government agencies are using artificial intelligence.*
>
> *Does your organisation have an AI policy or guidance for staff? I would like to see a copy of that guidance if it exists.*
>
> *If it doesn't exist yet, what advice have you given staff so far on using AI? And do you have a timeline for creating your own AI policy?"*

Presently, the Ministry is utilising AI tools and systems in a limited capacity. Some Ministry staff are trialling the usage of Generative AI tools in their work, in the form of Microsoft 365 Copilot.

To guide this, the Ministry has a general Artificial Intelligence Policy, which covers all forms of AI usage. This policy has been released to you in full and a copy has been enclosed.

I trust this information fulfils your request. If you wish to discuss any aspect of your request with us, including this decision, please feel free to contact the OIA Services Team on: oiagr@health.govt.nz.

Under section 28(3) of the Act, you have the right to ask the Ombudsman to review any decisions made under this request. The Ombudsman may be contacted by email at: info@ombudsman.parliament.nz or by calling 0800 802 602.

Please note that this response, with your personal details removed, may be published on the Ministry website at: www.health.govt.nz/about-ministry/information-releases/responses-official-information-act-requests.

Nāku noa, nā

Celia Wellington
Deputy Director-General
Corporate Services | Te Pou Tiaki

Artificial Intelligence policy

Published 20/03/2025

Purpose

This policy provides guidance to ensure that the use of Artificial Intelligence (AI) tools and systems within the Ministry of Health (the Ministry) is safe, ethical, compliant with our obligations as both a government-sector and health-sector organisation, and consistent with the Ministry's mission, vision and values.

Policy scope

This policy applies to:

- Ministry staff (including permanent, fixed term and contractors)
- External parties (vendors and suppliers) who are working with Ministry information
- All forms of AI – including, but not limited to:
    - Generative AI (GenAI) systems (including both text and image generators)
    - Machine Learning (ML) systems
    - Large Language Models (LLM)
    - Natural Language Processing (NLP) tools.

Definitions

Definitions related to terms used in this policy can be found in the organisational glossary.

We are committed to:

1. Fostering innovative use of technology for improved productivity and efficiency within the Ministry.
2. Enabling appropriate use of AI/ML tools within the Ministry, in an ethical manner and consistent with our Information Management, Security and Privacy best practices.
3. Protecting the confidentiality, integrity and availability of all organisational and personal data, including but not limited to:
    a. Government Information, including sensitive or classified information
    b. Staff information, such as employment information
    c. Personally Identifiable or Patient Health Information (PII/PHI) in accordance with the Ministry's good practice guidelines
4. Continued compliance with the New Zealand Government's Protective Security Requirements (PSR), the New Zealand Information Security Manual (NZISM) and the Health Information Security Framework (HISF aka HISO 10029:2022).
5. Incorporating advice from other sources, including the New Zealand Government system leads for Data, Digital and Cyber Security, when establishing policy.

We will achieve this by:

Applying the following principles:

1. Only AI tools, software and systems that have been formally approved for use by the Ministry, will be used.
    a. approval will be granted under the Ministry's existing Certification and Accreditation framework,
    b. an appropriate Risk Assessment must be completed,
    c. either a Privacy Impact Assessment (PIA) or Privacy Threat Assessment (PTA) must be completed,
    d. formal Approval will be granted after:

i. endorsement by the Information Technology Security Manager
ii. approval from the Chief Information Security Officer and the Chief Information Officer

2. AI tools will be used where necessary or appropriate, and with caution.
    a. Noting that AI tools may provide answers that contain factual errors, bias, or inappropriate content, Ministry staff are responsible for checking the accuracy and validity of the information drawn from AI tools.
    b. While AI tools may be used in gathering information, data analysis and developing recommendations, Ministry staff remain responsible for both the content of any document, paper or email containing AI-derived information, and any decisions made using AI-supported business processes.
3. In order to remain transparent and accountable, it is important to accurately record how and why decisions are made by the Ministry. A record regarding the use of AI and its effect on information and other records must be maintained.
4. Information submitted for processing by AI, including reference material and 'prompts' or commands issued to an AI, must be:
    a. UNCLASSIFIED, where the system operates outside of an Accredited Ministry IT system (such as Microsoft Copilot for Web)
    b. IN-CONFIDENCE (or below), where the AI system operates within a Certified and Accredited Ministry IT system
    c. RESTRICTED (or below), where the system is *specifically* Certified and Accredited to enable this functionality (such as Microsoft Copilot for M365), with particular attention to managing the risks.
5. Information or data classified SENSITIVE or RESTRICTED must not be input into AI Tools, except as allowed for in clause 4(c).
6. Information containing Personally Identifiable Information (PII) or Patient Health Information (PHI) must not be input into AI tools, except within systems allowed for in clause 4(b) or 4(c) and where appropriate Standard Operating Procedures have been put in place.
7. When discussing personal scenarios or examples, generic, fictitious or properly anonymised names and situations must be used.
    a. this may include the use of appropriately anonymised health information
    b. Where AI is used as part of a decision making process relating to individuals, the reasoning for the decision needs to be able to be shown.
8. The principles of the Privacy Act 2020 must be applied at all times.
9. Care will be used when using AI for processing data that would otherwise meet the criteria established in the Official Information Act for being withheld

10. Acknowledging varying views, some strongly held, around government use of AI tools, due consideration of our obligations under Te Tiriti must be considered, particularly if Māori data is involved or where Māori interests or outcomes could be affected through the use of AI.
11. Any Ministry use-case for the use of Artificial Intelligence will take account relevant Ministry, Health System and Government policies and standards, such as those listed later in this document.

Monitoring of the Artificial Intelligence policy

Ministry People Leaders are responsible for:

- Ensuring their people are aware of, and comply with, this Policy and its associated Business Rules, Guidelines and any Standard Operating Procedures applicable.

The Chief Information Officer (as Policy Owner) has the overall responsibility for:

- Providing appropriate training and support/reference materials, to support people leaders to comply with their obligations
- monitoring activities to ensure effective controls are in place
- carrying out periodic reviews to ensure compliance with the policy, guidance and business rules and the overall principles are being achieved.

Measures of the policy's effectiveness are:

- Where the Ministry's use of AI is compliant with this policy, and
- Where there are no breaches in trust or confidence in the Ministry associated with the use of AI, and
- Where value is being returned through the use of AI in support of the Ministry's activities.

Roles and responsibilities

Person/Party	Responsibilities
Director-General of Health	Accountable for all Ministry activities, including the quality and accuracy of products and the security of the Ministry's official information.
Executive Sponsor (DDG Corporate Services)	Executive Sponsor for all ICT Services

Person/Party	Responsibilities
Chief Security Officer	Responsible for the Ministry's overall protective security policy and practices, by delegation from the Chief Executive / Director-General of Health
Chief Information Officer / Group Manager, Digital and Information Services	Policy Owner Responsible for Information Management and Technology used for Digital and Information Services across the Ministry.
Privacy Officer	Responsible for the Ministry's overall privacy policy, and oversight of privacy practices
People Leaders	Ensuring their people are aware of, and comply with, this Policy.
Our people	Comply with the requirements of this policy and related guidance and business rules.

Guidance and rules to help good decision making

Additional guidance and business rules are in place and should be read in conjunction with this policy for decisions related to:

- Business Rules and guidelines for the use of Artificial Intelligence (to be developed).

Policy details

Policy Owner

Chief Information Officer (CIO)

Last reviewed date

20/03/2025

Next review date