



**Te Tari Taiwhenua  
Internal Affairs**

23 February 2024

45 Pipitea Street, Thorndon, Wellington 6011

PO Box 805, Wellington 6140

Phone +64 4 495 7200

Email [OIA@dia.govt.nz](mailto:OIA@dia.govt.nz)

Website [www.dia.govt.nz](http://www.dia.govt.nz)

Anon via FYI

[fyi-request-25521-6e3067d3@requests.fyi.org.nz](mailto:fyi-request-25521-6e3067d3@requests.fyi.org.nz)

Tēnā koe

**Your Official Information Act 1982 request, reference OIA23/24-0530**

I am responding to your email of 25 January 2024, requesting information under the Official Information Act 1982 (the Act). I have attached your request in full at **Appendix A**.

The timeframe to respond to your request has been extended by 15 working days to **15 March 2024** under section 15A(1)(b) of the Act. The extension is required because the necessary consultations to make a decision on the request cannot reasonably be made within the original time limit.

You have the right, under section 28 of the Act, to seek an investigation and review of my decision by the Office of the Ombudsman. The postal address of the Office of the Ombudsman is PO Box 10152, Wellington. Alternatively, you can phone 0800 802 602 or email [info@ombudsman.parliament.nz](mailto:info@ombudsman.parliament.nz).

Nāku noa, nā

Jeremy Cauchi

**Director Ministerial, Monitoring, and Capability**

## **Appendix A**

*Dear Government Chief Privacy Officer Katrine Evans,*

*According to the Digital.govt.nz website (link):*

*The GCPO is responsible for:*

- providing leadership by setting the vision for privacy across government*
- building capability by supporting agencies to lift their capability to meet their privacy responsibilities*
- providing assurance on public sector privacy performance*
- engaging with the Office of the Privacy Commissioner and New Zealanders about privacy.*

*I am a NZ citizen. I am seeking very clear and specific information as to the methods, programmes or applications that have been approved by the DoIA (e.g., Government Chief Privacy Officer & Government Information Security Officer) for the sending/receiving private information (e.g., health information, court documents) electronically, which meet the NZ standards, regulations, and legislative requirements.*

*We all know that email is not safe from interception or unauthorised access. Yet, it has been my experience that many agencies use this method for sending private, sensitive information electronically, while not taking any type of security measure.*

*For your convenience, I've listed some of the relevant legislation and standards below.*

*Section 22 (IPP 5) of the Privacy Act 2020 states:*

*Storage and security of personal information An agency that holds personal information must ensure—*

*(a) that the information is protected, by such security safeguards as are reasonable in the circumstances to take, against—*

*(i) loss; and*

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

*(iii) other misuse; and*

*(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 agency, everything reasonably within the power of the agency is done to prevent unauthorised use or unauthorised disclosure of the information.*

*(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.*

*The Health Information Privacy Code 2020 includes two more clauses to rule 5.*

*(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.*

*(2) This rule applies to health information obtained before or after the commencement of this code.*

*Health information and other information security standards include, but are not limited to:*

- *Ministry of Health: HISO 10029 and HISO 10064; • Center for Internet security (CIS) • CERT NZ Top Ten:*
- *Cloud Security Alliance (CSA) Cloud Controls Matrix:*
- *Health Insurance Portability and Accountability Act (HIPAA) (US):*
- *ISO 27001 Information Security Management Standard:*
- *ISO 27002 Information Technology – Security Techniques – Code of practice for information security controls • ISO 27799 Health informatics – Information Security Management in health using ISO/IEC 27002:*
- *New Zealand Information Security Manual (NZISM):*
- *Protective Security Requirements (PSR)( [link](#)) • National Cyber Security Centre • Information security management protocol ([link](#)) • New Zealand Government Security Classification System*

*This is also a request for all risk assessments undertaken by the DIA (any of the Government Chiefs) for the use of email to transfer private information (e.g., health information or court documents) by NZ Agencies (e.g., MoH, Health NZ, ACC, MoJ, ...). If your office has not conducted any risk assessments for any government agencies, then I request your assistance and ask you transfer this part of my request to the proper agency/organisation.*