

19 February 2024

Anon

By email only to: fyi-request-25520-9d5a536c@requests.fyi.org.nz

Tēnā koe

Official Information Act Request (Our Ref: OIA/0333)

I refer to your Official Information Act request of 25 January 2024.

Your request:

Part 1

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 (like health information) electronically, which meet the standards, regulations, and legislative requirements.

I also refer to standards set out by the:

- 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) ([external link](#))
- National Cyber Security Centre
- Information security management protocol ([external link](#))
- New Zealand Government Security Classification System

Part 2

This is also a request for all risk assessments undertaken by the OPC for the use of email to transfer patient records by NZ Agencies (e.g., Health NZ, ACC, MoJ, ...). If the OPC 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.

My response

Your Part 1 request is declined under section 18(e) of the Official Information Act on the basis that having searched our systems, we have not located the information requested as to whether the Department of Internal Affairs (including the Government Chief Privacy Officer and Government Information Security Officer) have approved electronic methods for sending and receiving health information in light of any relevant standards regulations or legislation.

I have consulted with the Department of Internal Affairs about your request. As you have made a similar request directly to DIA, it is, therefore, not necessary for me to transfer your request.

Your Part 2 request

Your Part 2 request is declined under section 18(e) of the Official Information Act on the basis that having searched our records, we have not located the information requested about risk assessments carried out by OPC on the use of email to transfer patient records.

Please note that the Privacy Commissioner's role is an advisory one when consulted by government agencies on technical options that have privacy considerations. It is not OPC's role to carry out risk assessments.

However, OPC proactively releases advice on security issues including email.

For a selection of our publicly available advice, please see the following:

- Secure email for health information, OPC blog 19 April 2016¹
- Outlook's email trap for the unwary, OPC blog 22 August 2014²
- Nurses data breach: what happened and how to get help, OPC blog 2 November 2016³
- Reporting and avoiding breaches in the health sector, OPC blog 15 April 2022⁴
- Preventing privacy breaches, OPC webpage⁵

Request for assistance

I have considered your request for assistance to transfer your request, as OPC does not hold records about conducting risk assessments.

It is possible that DIA, the Ministry of Health or Te Whatu Ora may hold information about risk assessments for using email to transfer patient records. However, you will need to contact these agencies directly if you wish to request information about risk assessments being carried out by agencies other than OPC.

¹ <https://www.privacy.org.nz/blog/secure/>

² <https://www.privacy.org.nz/blog/outlook-email-trap/>

³ <https://www.privacy.org.nz/blog/nurses-data-breach-what-happened-and-how-to-get-help/>

⁴ <https://www.privacy.org.nz/blog/reporting-and-avoiding-privacy-breaches-in-the-health-sector/>

⁵ <https://www.privacy.org.nz/responsibilities/privacy-breaches/preventing-privacy-breaches/>

Conclusion

If you are not satisfied with this response, under section 28 of the Official Information Act, you have the right to ask the Ombudsman to investigate and review my decision on your request.

Nāku iti noa, nā

A handwritten signature in blue ink that reads "Liz MacPherson". The signature is written in a cursive style and is contained within a thin black rectangular border.

Liz MacPherson
Deputy Privacy Commissioner