Te Kawa Mataaho
Public Service Commission

22 January 2026

«Title» «First_Name» «Last_Name» «Post_Nominals»
«Sector_Designation_»
«Agency»

By email: «Email»

Dear «First_Name»

Safeguarding the integrity of public information and data

Happy New Year – I hope you had, or are having, a good break.

I am writing to you following the recent data breach involving the Manage My Health platform, where private patient health information was compromised.

While the immediate response is underway, it highlights significant challenges for how we, as leaders of the Public Service, ensure that the systems and partnerships we rely on uphold the highest standards for protecting New Zealanders' most sensitive information.

This breach is not simply a technical lapse; it reflects a breakdown in the trust we place in those who manage and hold personal information and data. Although the breach occurred outside government systems, it highlights the reality that public outcomes increasingly depend on complex networks of providers, platforms, and intermediaries - many of which sit beyond direct government control or accountability. Trust is the foundation of our future digital strategy and operating model, and it is essential that we are doing everything we can to deserve the trust of New Zealanders.

While there might not be strict or technical accountability, this incident highlights the implied expectation on the public sector to prevent such breaches. Recent events, and associated public commentary, expose vulnerabilities in how accountability and assurance are applied across these arrangements and underscores the need for stronger oversight of third-party entities that collect, process, or share personal information within our sectors.

It is important that we lift the level of assurance we receive about the integrity of how people's information and data are held. In my view, we should apply the same rigour to this as we apply to health and safety. Just as it is unacceptable for someone to be injured at work, it is unacceptable for personal information – collected in relation to services and contracts we fund – to be compromised.

In light of recent events, I would like you to confirm your agency's arrangements for managing, protecting, and overseeing personal information and data handled by third party providers and across your supply chain. This includes:

- all entities within your sector that you are responsible for, acting on behalf of or funded by government (including, for example, contracted service providers, Non-Governmental Organisations, Crown entities, and shared services); and

- all entities operating within your sector without a direct contractual or regulatory relationship with government but that collect, process, or share personal information and data in ways that materially affect public outcomes.

I would like your assessment of the information and data held through the supply chain of third parties your agency manages, the level of assurance and controls currently in place across these arrangements, and whether additional controls or assurance are required to strengthen the protection of personal information and data. If there are any vulnerabilities or risks, I would like your views on how these can be addressed. I understand that what I am asking is similar to what your agency would have responded to in relation to the 2022 Mercury IT breach.

I would like you to report back to me by 27 February 2026 with your initial assessment. In considering your response, I would encourage you to refer to the Government Communications and Security Bureau's Supply Chain Cyber Security guidance and the Standard for providing non-government third parties with access to, or collection of, Government held personal information.

Separately, I have asked Paul James to lead work on reviewing and strengthening the current policy and operational settings for how third parties handle personal information and data. This work will include:

- a review of the current policy and operational settings for how third parties manage and protect personal information and data, with a focus on consistency of standards, clarity of roles and responsibilities, and the adequacy of current assurance and oversight arrangements across sectors.

- identification of gaps or weaknesses in the existing framework and clear recommendations for how these should be addressed. This may include consideration of regulatory options, as other international jurisdictions have done, to strengthen accountability, obligations and incentives.

As we have previously discussed, data collected and held by government agencies (and their accredited partners in their respective funding and supply chains) is a key asset for us as a system and a foundation of our digital future. The public, businesses, and communities must have confidence that their personal information and data is held safely and with integrity. Recent events have given rise to questions in that regard – we cannot be passive and allow our systems and actions to be undermined. This is the second time in the space of twelve months we have been exposed to significant information and data protection failures.

If your team would like to discuss these matters, please refer them to Robert Anderson, Manager, Public Sector Performance at the Commission.

Many thanks for your help and support on this.

Yours sincerely

Sir Brian Roche KNZM
Te Tumu Whakarae mō Te Kawa Mataaho
Public Service Commissioner | Head of Service