Think Your Data Is Safe? Think Again.

Posted on: January 19, 2026

When a fried chicken chain has tighter cybersecurity than our digital health providers, it’s time to admit something’s wrong.

With the Manage My Health privacy breach dominating headlines through the start of 2026, the lack of a penalty regime under the Privacy Act 2020 has been a hot topic of conversation for many.

In New Zealand there is no express penalty regime for a privacy breach. Instead, the Privacy Commissioner can issue fines of up to $10,000.00, but only in specific situations such as when an organisation:

- ignores a compliance notice;
- misleads another agency to obtain someone else's personal information;
- deliberately destroys personal information to avoid providing it; and
- fails to notify the Privacy Commissioner of a privacy breach.

While more serious cases can be escalated to the Human Rights Review Tribunal (which has the power to award penalties of up to $350,000.00), the process for receiving compensation this way can be a lengthy and difficult process.

In June 2024 the Deputy Privacy Commissioner commented that "a civil penalty regime is a critical tool missing from [the Office of the Privacy Commissioner's] regulatory toolkit," before going on to note that many take a classic New Zealand '*she'll be right*' attitude to privacy and their obligations under the Privacy Act.

The Manage My Health breach has seen an estimated 120,000 patients affected with their sensitive medical information held to ransom. Manage My Health CEO Vino Ramayah publicly revealed that the hacker gained access via a valid user password. While the portal does offer two-factor authentication, it is not mandatory.

A web standards consultant with experience in government website security had raised concerns about Manage My Health's weak security six months earlier, further noting that KFC has a mandatory two-factor authentication system which is above the login security of that of Manage My Health.

With personal data now one of the world's most valuable assets, complacency in the digital age carries an ever-growing risk. Without real incentives for organisations to prioritise privacy, or meaningful penalties for failing to do so, that complacency is likely to persist.

In Australia, significant privacy reforms were introduced in late 2022 following the Optus and Medibank data breaches. Medibank, Australia's largest private health insurer, failed to protect the sensitive medical information of roughly 9.7 million

Australians, with court documents indicating that the absence of multi-factor authentication was an entry point for the hackers.

While the Office of the Australian Information Commission was able to bring civil penalty proceedings against Medibank for up to AUD $2.2 million per contravention, the reforms that followed brought dramatic penalty increases for serious or repeated breaches. The maximum penalty, for each contravention, was increased to the greater of:

- AUD $50 million;
- three times the value of the benefit derived (either directly or indirectly); or
- 30% of the organisation's annual turnover.

The reforms were widely regarded as a move to drive stronger accountability among organisations responsible for protecting personal information.

With the Manage My Health breach being cited as one of the biggest privacy breaches in New Zealand history, the need for comparable reform is clear. If New Zealand wants organisations to treat privacy as a serious obligation rather than an optional extra, the Government will need to introduce a regulatory framework that genuinely incentivises robust data protection and creates meaningful consequences when those organisations fall short.

The Manage My Health breach provides a timely reminder of how important strong privacy policies and protocols are for organisations and businesses of all sizes, especially when dealing with sensitive personal information. Here are some key take aways for you to consider for your business:

1. What personal information are you collecting, using, and/or handling, and why? Consider reviewing and updating your privacy impact assessment to ensure you are meeting the requirements under the Privacy Act.
2. Weak passwords, shared logins, and optional multi-factor authentication remain leading causes of data breaches. Reviewing access controls is one of the most cost-effective steps to reduce risk.
3. Regular security testing and quick remediation are essential.

4. Regulatory reform may increase penalties in the future, but reputational harm is already costly.
5. Australia’s tougher penalty regime signals where New Zealand may be heading. Strengthening privacy practices now will help keep businesses ahead.
6. Because personal data is easily targeted and monetised, businesses should ensure governance, training, and incident-response planning reflect its value.
7. Don’t let your complacency cost people their privacy.

If you need assistance with reviewing or implementing a privacy policy for your business, or have other queries or concerns regarding your obligations under the Privacy Act, please reach out to our Corporate and Commercial Team.