MINISTRY OF HEALTH
MANATŪ HAUORA

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

26 NOV 2019

Vincent

By email: fyi-request-11391-611aa252@requests.fyi.org.nz
Ref: H201908793

Dear Vincent

Response to your request for official information

Thank you for your request for information under the Official Information Act 1982 (the Act) on 5 October 2019 regarding the Tū Ora Compass Health (Tū Ora) cyber security incident.

On 1 November 2019 the Ministry of Health (the Ministry) extended the due date for the response in accordance with section 14 of the Act, as further consultation was required.

On 5 October 2019 Tū Ora publicly disclosed that there had been several unauthorised intrusions into its public-facing systems. As a non-governmental organisation Tū Ora is responsible for the security of its systems and the protection of private information contained therein.

The Ministry provided support to Tū Ora to respond to the incident, including establishing an 0800 number for affected individuals. Further information about the response is available on the Ministry's website: https://www.health.govt.nz/our-work/emergency-management/cyber-security-incident.

The Ministry has released several documents related to your request, subject to redactions under the Act where appropriate. These documents are publicly available on the Ministry website: https://www.health.govt.nz/our-work/emergency-management/cyber-security-incident.

I have responded to each part of your request below. Please note that parts of your request have been grouped together to simplify this response.

- *The names and vendors of any systems involved in this breach.*

The cyber security breaches affected public-facing websites operated by Tū Ora Compass Health, THINK Hauora, Cosine Primary Care Network, Te Awakairangi Health Limited and Ora Toa.

The Ministry understands that Tū Ora contracts with a private IT provider which maintain the websites involved in the incident. The name of this provider is withheld under section 9(2)(b)(ii) of the Act as releasing this information would unreasonably prejudice the commercial position of the person who supplied or is the subject of the information. You may wish to contact Tū Ora directly for this information: https://compasshealth.org.nz/Contact-Us.

- A copy of all risks or risk register documents that identify direct or indirect impacts on patients as a result of this breach, or any other data breach.

The Ministry has not prepared any specific risk or risk register documents regarding impacts of the breach. However, information about specific risks is contained in the documents published on the Ministry website (notably the 20 September 2019 Memorandum and the two communications plans): https://www.health.govt.nz/our-work/emergency-management/cyber-security-incident. This part of your request is therefore refused under section 18(d) of the Act as the information is publicly available.

The Ministry considers that the biggest risk arising from the incident is the possibility of people being targeted by scams and phishing attempts, for example malicious actors purporting to hold sensitive information about a person. We recommend that people remain vigilant, maintain good online security practices and report any suspicious contact or activity to the appropriate authorities.

- A copy of any communications plan, internal or external, relating to this breach.

- Any and all communications to the Minister of Health that includes or mentions this breach.

All briefings to the Minister of Health and communications plans prepared by the Ministry and Tū Ora are published on the Ministry website: https://www.health.govt.nz/our-work/emergency-management/cyber-security-incident. These parts of your request are therefore refused under section 18(d) as the information is publicly available.

In addition to these briefings, the Ministry kept the Minister of Health and the office informed about developments via his regular scheduled meetings throughout the response period.

- All penetration or security tests, performed by a reputable third party organisation, against health systems held, managed or utilised by PHOs.

- All communications with any external organisation that are providing any sort or review, advisor, or investigative role in relation to this breach.

600 websites operated by district health boards (DHBs) and Primary Health Organisations (PHOs) were scanned by the Government Communications Security Bureau's National Cyber Security Centre (NCSC) to assess whether they had the same vulnerabilities as the Tū Ora websites.

The NCSC scanning identified five websites operated by three DHBs that had potential vulnerabilities. One was a 'false positive' where subsequent analysis showed the vulnerability had been previously patched and was secure.

In the other four instances, vulnerabilities were confirmed, and immediate actions were taken by the affected DHBs to mitigate any risk. The Ministry has been advised that none of these websites contained, or provided immediate access to, confidential health information relating to patients.

As there is no patient information on the sites, because the risks have been mitigated, and to minimise the risk of inadvertently abetting further illegal activity, the Ministry is not currently naming the DHBs or the websites.

The Ministry has released information about the security testing undertaken by the NCSC, including further information about the range of assurance activity underway to strengthen ICT security in the health system: https://www.health.govt.nz/news-media/media-releases/results-cyber-testing-600-health-websites.

Copies of reports and communications in relation to this testing are withheld in full under the following sections of the Act:

- section 9(2)(c) to protect the health and safety of members of the public
- section 9(2)(e) to prevent or mitigate material loss to members of the public.

- All communications in the past 6 months and documentation relating to decisions around the audit of access to information held by any PHO.

The Ministry has not made any decisions to audit access to information held by a PHO. This part of your request is therefore refused under section 18(e) of the Act as the information requested does not exist.

I trust this information fulfils your request. You have the right under section 28 of the Act, to ask the Ombudsman to review any decisions made under this request.

Please note this response, with your personal details removed, may be published on the Ministry website.

Yours sincerely

p.p.

Shayne Hunter
Deputy Director-General
Data and Digital