Memorandum

Cyber security breach at Tū Ora Compass Health

Date due to MO:	13 September 2019	**Action required by:**	<N/A>
Security level:	[redacted]	**Health Report number:**	20191772
To:	Hon Dr. David Clark, Minister of Health		

Contact for telephone discussion

Name	Position	Telephone
Shayne Hunter	Deputy Director-General, Data and Digital	s 9(2)(a) [redacted]
Darren Douglass	Group Manager, Digital Strategy & Investment, Data and Digital	s 9(2)(a) [redacted]
David Metcalfe	IT Security Manager, National Digital Services, Data and Digital (technical SME)	s 9(2)(a) [redacted]

Action for Private Secretaries

N/A **Date dispatched to MO:**

Cyber security breach at Tū Ora Compass Health

Purpose of report

1. This report summarises a cyber security breach at Tū Ora Compass Health (Tū Ora) Primary Health Organisation (PHO).

2. This is not a breach that has occurred within the New Zealand government. PHOs are private organisations, which deliver primary health care services in accordance with a PHO Services Agreement with a District Health Board.

3. Tū Ora reached out for assistance from the Ministry of Health and the National Cyber Security Centre (NCSC, part of the Government Security Communications Bureau).

Background

4. The Tū Ora website was defaced on 5 August 2019. In subsequent analysis, four exploits of their public website server by external malicious actors between July 2016 and August 2019 were discovered.

5. s 9(2)(g)(i) [redacted]

6. Officials are still working with Tū Ora to gain a clear understanding of the information that could be accessed and the extent and scale of the breach.

7. s 9(2)(g)(i) [redacted]

8. Tū Ora took immediate steps to contain the incident after learning of the website defacement. They have also implemented new security controls and are continuing to analyse the affected datasets to inform the incident response plan. The NCSC investigation of the incident is expected to continue for a further two or three weeks.

9. The Ministry of Health is supporting Tū Ora and has developed an incident response plan. This is being done with input from other agencies including the State Services Commission, Department of Prime Minister and Cabinet, Department of Internal Affairs, and the Government Communications Security Bureau.

10. Additional agencies and organisations such as the Office of the Privacy Commissioner, New Zealand Police, and CERT NZ will be engaged as and when needed. Implementation of immediate tasks in the response plan is underway.

11. The incident response plan focuses on three workstreams:

    a. The Ministry of Health is supporting Tū Ora in developing a proactive communication and support plan for the individuals that are impacted by the potential data breach.

    b. Assurance that the Tū Ora incident is resolved.

    c. The Ministry of Health undertaking immediate and longer-term actions to provide greater security assurance across the health system.

12. Officials are working to determine the decision-making rights and processes for any disclosure of this breach. This is not straightforward given the contractual and legal responsibilities associated with data being held by Tū Ora as a private organisation.

13. s 9(2)(f)(iv), s 6(a) [redacted]

14. The Ministry will provide updates to the Minister as response plan actions are completed.

Context

15. Tū Ora is one of the largest Primary Health Organisations (PHOs), in the country. It currently provides primary care services in the Wellington, Porirua, Kapiti and Wairarapa regions. Historically it also provided primary care services in the Manawatu region and still provides technology and data analysis services to THINK Hauora PHO.

16. PHOs are charitable trusts contracted by District Health Boards (DHBs) using a nationally agreed PHO Services Agreement. Tū Ora has contracts with Capital and Coast and Wairarapa DHBs. PHOs provide health services either directly or through contractual relationships with general practices and other health providers. Tū Ora contracts with 60 general practice teams and other health providers.

17. A PHO collects health information from its contracted health providers for reporting for contractual, claims, clinical quality improvement and project monitoring purposes. The PHO Services Agreement requires that PHOs comply with all statutory, regulatory and other legal requirements applicable to the performance of their obligations under this Agreement, including the Privacy Act 1993 and the Health Information Privacy Code 1994 (clause B48(1)(a)). The Agreement also contains specific requirements on PHO about information management, to preserve and protect the safety and security of health information they hold.

18. The Ministry of Health does not generally contract directly with PHOs but does provide standards and guidance to assist PHOs and other health sector organisations with how they meet their contractual obligations for information management. These include HISO Standard, including the Health Information Security Framework, and the Health Information Governance Guidelines, which supplement guidance from the Office of the Privacy Commissioner and others.

19. Tū Ora contracts Primary IT, a private company, to provide IT services. In addition to Tū Ora Primary IT provides services to over 50 medical centres and THINK Hauora PHO.

Incident overview

20. A high-level timeline of the incident is as follows:

    a. 10 July 2019 - Tū Ora was directly contacted by the NCSC notifying them that their web server was exposed to a publicly known s 9(2)(c), s 9(2)(e) vulnerability from 2017. This was not actioned by Tū Ora or their IT service provider.

    b. 5 August 2019 - Tū Ora web server was exploited by this method and the attacker 'defaced' their website, ultimately alerting Tū Ora that they had been attacked.

    c. 6 August 2019 - Ministry of Health was notified by Tū Ora of the successful attack on their website. Tū Ora Compass Health took immediate steps to contain the incident, called in experts to start an investigation, and notified CERT NZ and the NCSC.

    d. 8 August 2019 - The NCSC initiated a forensic investigation; this is continuing and is expected to take a further two to three weeks.

    e. 15 August 2019 – Tū Ora issued a press release stating that is website had come under attack but did not disclose the likelihood that unencrypted personally identifiable information was also stored on that same server.

    f. 15 August 2019 – NCSC provided an update that three further server exploits were found on the server. Based on the information available to date, the server was compromised twice in 2016, and twice in 2019.

21. s 9(2)(c), s 9(2)(e) [redacted]

22. It appears that the breach has been contained and most of the Tū Ora services have been restored. Since the breach, Tū Ora has also implemented several new technical security controls to bolster their security defence and detective capabilities.

23. s 9(2)(c) [redacted] Additionally, access to Tū Ora's environment would provide access to data held on over one million people that have lived within the geographic area of Capital and Coast, Wairarapa and Mid Central DHBs and registered with a GP over the last 17 years.

24. The data held by Tū Ora on an individual will vary considerably depending on their age, diagnoses, test results, and any interventions. At a minimum it would include NHI, name, date of birth, address, ethnicity, gender, and the GP practice where the person is enrolled. s 9(2)(e), s 9(2)(i) [redacted]

25. Officials are still working with Tū Ora to gain a clear understanding of the information that could be accessed and the extent and scale of the breach.

26. Note that the data stored by Tū Ora does not contain the detailed clinical notes captured by general practices and is not used for treatment or diagnosis of people.

27. s 9(2)(b)(ii) [redacted]

Response Plan next steps

1. Communication and support to affected individuals

28. The Ministry is working closely with Tū Ora in preparing communications, media releases and ensuring appropriate support for affected individuals is in place. It is critical that support and advice for affected individuals is ready for any proactive or unplanned disclosure of this breach.

29. Support from Healthline to provide a call centre function is proposed and support from other agencies such as CERT NZ and NetSafe is being explored.

30. Tū Ora have been asked to prepare more information to support the call centre to answer questions from concerned individuals about what information, if any, may have been disclosed and what they can do about it. s 9(2)(g)(i) [redacted] and will require central government and DHB support.

2. Request for health sector assurance

31. The Ministry will require Tū Ora to engage an independent third party to conduct security assurance activities on the new website environment, and other externally facing systems, to validate that they are secure and patched.

32. s 9(2)(h), s 9(2)(g)(i) [redacted]

33. s 9(2)(h), s 9(2)(g)(i) [redacted]

3. Immediate and longer-term health system actions

Request for health sector assurance

34. The Ministry will issue a request by 20 September 2019 for DHBs, PHOs and health shared service agencies to provide assurance regarding the security of their public facing servers and security management practices in direct response to the vulnerabilities identified in the Tū Ora incident.

35. The request will be positioned as a follow up to the recent request for assurances regarding public facing websites in response to recent government data breaches.

36. It should be noted that the Ministry of Health's authority to require PHOs, NGOs, and even DHBs, to complete independent assessments of their environments is limited, due to the contracting arrangements.

Independent security assessments

37. The Ministry is leading the review of information security maturity across critical health organisations such as PHOs, DHBs and large health NGOs, with input from the Government Chief Digital Officer (GCDO) and Government Chief Information Security Officer (GCISO), to identify potential high-risk cyber security vulnerabilities.

38. Planning for the security reviews is underway. The focus is initially on Tū Ora s 9(2)(b)(ii) [redacted] followed by other prioritised critical health organisations.

39. Mitigation plans for any critical vulnerabilities will be agreed with and monitored by the Ministry.

40. Subsequently, we will seek assurance that the data held is appropriate to the business function of the organisation and is secured and managed in accordance with the Health Information Privacy Code and Privacy Act.

41. Agencies and organisations like DHBs, PHOs, and other health providers are responsible for their own security. Steps to review their security posture and aiding them with improvements does not shift the accountability for security across the health sector to the Ministry.

Contracts

42. The Ministry will work with the GCISO and GCDO to release additional guidance around mandatory and recommended contractual clauses for health organisations regarding cyber security and privacy obligations.

Longer term actions

43. The Ministry will continue its stewardship role of promoting better security maturity throughout the health sector. This includes work already underway around:

    a. s 9(2)(f)(iv), s 6(a) [redacted]

    b. Forwarding relevant security vulnerability notifications to the wider health sector;

    c. Reviewing large business cases from DHB's for security related assurance and considerations;

    d. Providing input and advice sought by the sector participants, from small GP practices to the large DHB's, NGO's, and PHO's; and

    e. Providing advice and guidance on improving security, such as recent guidance to improve security of email systems in the health sector.

44. s 9(2)(f)(iv), s 6(a) [redacted]

45. s 9(2)(f)(iv), s 6(a) [redacted]

Recommendations

The Ministry recommends that you:

a) **Forward** a copy of this report to the following Ministers:

- Hon Chris Hipkins, Minister for State Services Commission
- Hon Megan Woods, Minister for Department of Prime Minister and Cabinet
- Hon Andrew Little, Minister for Government Communications Security Bureau
- Hon Tracey Martin, Minister of Internal Affairs

Shayne Hunter	Hon Dr David Clark
Deputy Director General	**Minister of Health**
Data and Digital	Date:

ENDS.

Appendix A – Initial set of Reactive talking points

46. Health agencies are investigating the extent of a cyber incident that could have exposed personally identifiable information in Tu Ora Compass Primary Healthcare Organisation

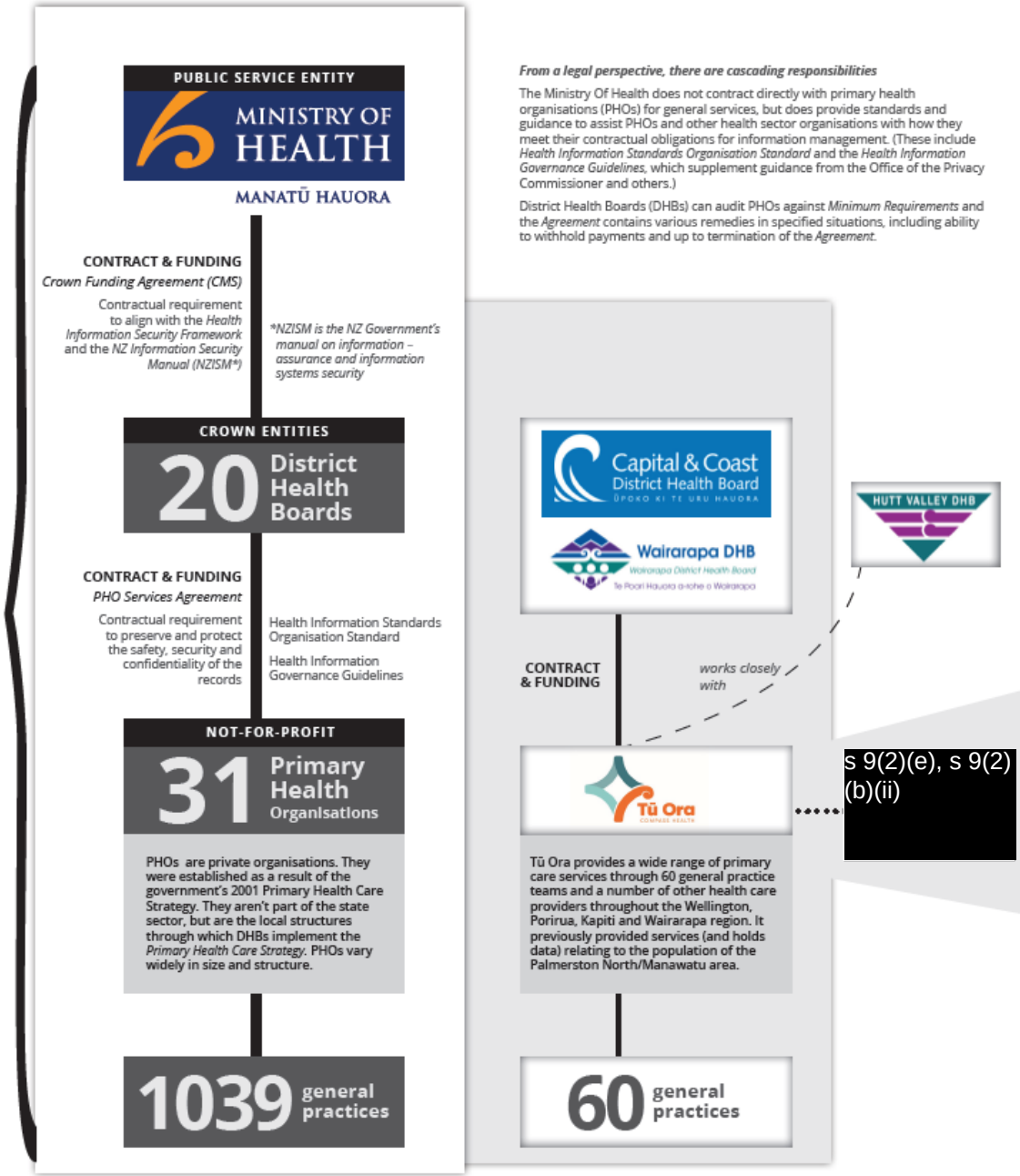
47. Officials are still working with Tū Ora to gain a clear understanding of the information that could be accessed and the extent and scale of the breach An additional update from Tu Ora Compass is expected in coming weeks once the investigation is complete

48. Tu Ora Compass Health has already provided some information about a related incident that resulted in a website defacement and the measures already taken to address it https://www.compasshealth.org.nz/News/Media-Releases

49. The Ministry of Health are leading the development of a response plan that includes actions specific to Tu Ora Compass Primary Healthcare Organisation and actions across the health system.

50. This is not a breach that has occurred within the New Zealand government. PHOs are private organisations, which deliver primary health care services in accordance with a PHO Services Agreement with a District Health Board.

[redacted]



Privacy Act 1993.

Health Information Privacy Code

Privacy Commissioner
Te Mana Mātāpono Matatapu

Health agencies have obligations over the health information they hold. These include taking reasonable security safeguards' to protect health information. This means keeping the information safe from loss, as well as from unauthorised access, use, modification or disclosure.

s 9(2)(e), s 9(2)(b)(ii)

[redacted]

s 9(2)(c), s 9(2)(e)

[redacted]