MINISTRY OF HEALTH
MANATŪ HAUORA

Memorandum

Update on Operation SONIC at 3 October

Date due to MO:	N/A	**Action required by:**	N/A
Security level:	[redacted]	**Health Report number:**	20191913
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]
Sue Gordon	Acting Director-General of Health	s 9(2)(a) [redacted]

Action for Private Secretaries

N/A

Date dispatched to MO:

Update on Operation SONIC at 3 October

Purpose

1. To provide an update on how Tū Ora Compass Health is responding to identified cyber security breaches.

Background and context

About the issue

2. Tū Ora is working closely with the Ministry of Health to manage issues arising from cyber security breaches discovered after the 5 August 2019 breach incident [HR20191826 refers]. We now understand that five associated PHOs, primarily serving patients in the lower North Island, are affected by the breaches.[1]

3. Tū Ora acted quickly to notify the Ministry, the National Cyber Security Centre (NCSC) and the Office of the Privacy Commissioner about the cyber security breaches. This is consistent with its obligations under the Privacy Act 1993 and the Health Information Privacy Code 1994.

4. Subsequent investigation by Tū Ora, an information security provider and the NCSC has not conclusively proved that patient information was accessed, removed or modified during the breach period. However, the nature of the breach is such that this could have occurred at any time.

5. The Ministry established an incident management team on Monday 30 September 2019 to ensure that Tū Ora is supported to respond and manage the issue. A Situation Report was issued to the Watch Group and central agencies the same day (**Appendix 1**).

International context

6. A number of high-profile cyber security breaches have occurred in health systems internationally, including:

   a. the current 'ransomware' attacks on Australian and US hospitals and health care providers

   b. the SingHealth attacks that compromised patient information for 1.5 million Singaporeans

   c. widespread compromising of Picture Archiving and Communications systems in the US and internationally which hold patient radiography results.

7. All systems connected to the internet are under constant threat of cyber-attack and there are thousands of attempts of varying sophistication on an hourly and daily basis. There is no evidence to suggest that the New Zealand health and disability system is disproportionately affected compared to other sectors.

---

[1] Tū Ora Compass Health, Te Awakairangi Health, THINK Hauora, Cosine Primary Care Network, Ora Toa.

8. The Ministry is continuing to monitor the international situation to identify opportunities to support the New Zealand health and disability system to manage data and information security effectively.

Tū Ora has responded to the issue

9. As a non-governmental organisation Tū Ora is solely responsible for the security of its IT systems and any patient information it holds. Tū Ora leadership is clear that it owns the issues and the Ministry is ensuring that its response is appropriate.

10. Tū Ora's Chief Executive, Martin Hefford, has returned to New Zealand to lead Tū Ora's response. Mr Hefford's role as Tū Ora response manager has a dotted line into the Ministry's incident management team structure so that we can effectively coordinate with Tū Ora.

11. Tū Ora has developed detailed communications and stakeholder engagement plans that map out the plan from day one of the issue becoming known (whether by proactive disclosure or in the event of an unplanned disclosure).

The Ministry has been supporting Tū Ora

12. As steward of the New Zealand health and disability system the Ministry is responsible for helping sector players navigate complex situations and respond in the appropriate manner. We will take the lead on the overall health system response and media engagement in relation to health system issues. We will also work closely with government stakeholders in relation to wider government considerations.

13. Tū Ora will take the lead on issue ownership and the immediate response, with the Ministry following in behind to ensure it is well-supported and the system is equipped to respond effectively. The responsibility for engaging with government (including ODESC, GCSB and Ministers) sits with the Ministry.

14. The Ministry's clear expectation is that DHBs, PHOs and NGOs take appropriate measures to protect the privacy and security of patient information. This is made clear through the Health Information Privacy Code 1994, which applies to all health system entities dealing with personal information.

15. Where this has not occurred, we have a responsibility as steward to help the system step up to the required standard. The Ministry will continue to work closely with Tū Ora to help it manage patient data safely and effectively.

Security assurance activity is underway

16. The NCSC is undertaking a targeted scan of DHB and PHO systems to identify a specific set of potential weaknesses, with a focus on high risk and / or potentially vulnerable areas. We expect the results of this scan to be available from 11 October 2019.

17. Ministry ICT is engaging with sector entities (including DHBs and PHOs) to identify areas or systems that require further assurance. The aim is to build an understanding about where other vulnerabilities are and scope the work required to improve security.

18. This work is underway and the NCSC expects to complete this work by early next week. It should be stressed that a systematic approach to identifying and rectifying sector

vulnerabilities is a long-term process. Detailed information may not be known for some months.

19. The Ministry is working with GCDO to leverage off its wider government ICT assurance work. We expect to continue to have high levels of engagement with GCDO, CIOs and the NCSC throughout this work.

We have developed a clearer view of the legal and privacy situation

20. s 9(2)(h) [redacted]

21. [redacted]

22. The Ministry (supported by the Government Chief Privacy Officer) has engaged with the Privacy Commissioner to work through the privacy impacts of the cyber security breach. Initial discussions indicate that our approach to 'responsible disclosure' is appropriate.

23. The primary privacy relationship is between affected individuals and Tū Ora. The Ministry is not party to the breach itself or follow up complaints s 9(2)(h) [redacted] s 9(2)(h) [redacted]

The issue has been approached with care

24. Tū Ora carefully considered whether it should disclose the cyber security breaches immediately after they were identified. The Ministry supported the decision to delay disclosure until further information was available as this approach struck the best balance between meeting the public interest and the responsibility to ensure a comprehensive understanding of the issues.

25. Security of information sits at the heart of trust and confidence in the health system. We considered that taking time to understand the nature and scope of the breaches was important because:

    a. the system relies on the effective flow of information to support positive health outcomes. Disclosing without being able to reassure the public could affect people's willingness to seek health care because of privacy concerns or distress

    b. robust systems and processes need to be in place to support people affected by the breaches (e.g. mental health support)

    c. detailed investigation was required to ensure that Tū Ora can communicate as much information as possible to help the public understand the situation

d. public and media attention could prompt an increase in cyber security attacks as health is seen as a vulnerable target. There is also a possibility of scams, blackmail attempts and phishing attacks. It is important that an appropriate response is in place to manage any subsequent malicious activity.

26. Tū Ora's approach has therefore been to work with the Ministry and other agencies to understand the issue more fully ahead of making a responsible disclosure following the results of the NCSC's initial security scan (para 16 refers).

An immediate response is now required

27. Tū Ora and the Ministry had prepared plans to stand up an urgent response in the event of an unplanned disclosure. As some information about the cyber security breach has reached the public arena, we are moving to deploy this plan.

Communications roles and responsibilities

28. On a practical level Tū Ora and the Ministry will be joined-up in terms of communication, but will be assigned specific roles and responsibilities as follows:

	Roles and responsibilities	**Spokesperson**
Tū Ora Compass Health	- issue ownership - technical response (what Tū Ora has done to secure its systems etc) - primary care interface (supported by the Ministry)	Martin Hefford, Chief Executive
Ministry of Health	- primary media liaison - health system response and assurance - first point of contact for affected individuals (via contact centre)	Dr Ashley Bloomfield, Director-General of Health

29. A media conference will be held at the earliest opportunity. We are keeping your office informed about timing and preparations.

30. As part of the communications approach the Ministry may seek to proactively release key documentation to meet the public interest in this matter. We will provide you with advice about this separately.

Channels for affected individuals

31. Our priority is to provide channels for affected individuals to access information about the issue. Primarily this will be through the Ministry website and a dedicated 0800 number (plus a separate local number for international callers). Calls will be answered by the Ministry's Whanganui call centre. We estimate that our customer service

representatives can field approximately 4500 calls per day. Overflow arrangements are in place.

32. Tū Ora and the Ministry are working closely with Homecare Medical Ltd. We anticipate that some callers will be experiencing personal and mental distress. These callers will be routed to the appropriate support service (e.g. 1737).

Supporting primary care

33. Primary care (both affected PHOs and the wider primary care network) needs to be well supported to answer questions about the cyber security breach. There will be:

    a. a high level of demand for information about what Tū Ora (and potentially other primary care providers) holds about affected individuals

    b. a requirement to supply primary care with information about how to respond to concerned individuals and where to direct them to.

34. Tū Ora will take the lead on communicating with PHOs at the appropriate time. Advice about timing of any sector briefings will be provided within the communications plan.

Next steps

35. The Ministry will keep you informed about communications and response planning. The incident management team may also publish further Situation Reports. We will ensure that your office receives a copy of any updates.

36. There are several wider system issues related to this event that will require further investigation by the Ministry (potentially within the context of the Health and Disability System Review) including:

    a. costs have already been incurred and are likely to rise as the response ramps up. Additional investment to strengthen health system infrastructure may also be required if further vulnerabilities are detected

    b. responding to the cyber security breaches will place strain on Tū Ora and the wider primary care sector. Sustainability of services will be an important consideration

    c. consideration needs to be given to whether key policy settings could be strengthened:

        i. how health system privacy settings and guidelines can support best practice

        ii. the role of service commissioning and contracting

        iii. ICT infrastructure and investment

        iv. audit and enforcement.

37. The Ministry will report back to you with initial thinking on these issues once the immediate response process is underway.

Sue Gordon

Acting Director-General of Health

s 9(2)(g)(i)

s 9(2)(g)(i)

s 9(2)(g)(i)