Communications plan

Ministry of Health Emergency Response – Cyber Incident

---

1. Issue: Health information relating to 1 million people held by Tu Ora Compass PHO and four other PHOs linked with it, may have been accessed as a result of illegal activity over a three year period. Other illegal cyber activity may remain a current threat. This plan guides the Ministry's actions in providing information to the public and media.

2. Background to the issue: On 5 August 2019 Tu Ora Compass PHO experienced an unauthorized cyber intrusion to its computer system. Subsequent investigation showed this was one of four unauthorised intrusions since 2016.

While medical notes from consultations with doctors were not accessible, other sensitive information was. This included notes regarding treatment from nurses, diagnostic results, laboratory results, and referrals to health services including for mental health and sexual assault.

We know that the characteristics of a significant health event are:

- high demand for information
- variable quality of information
- high public sensitivity

This reinforces the need for a well-managed response underpinned by good planning – with appropriate resources and support.

This plan takes a principle-based approach as in any significant event information can change rapidly. The current plan is pitched at a high level with some limits on detail due to information is still being provided. More detailed information around specific issues and key messaging will be worked on separately.

We have aimed for both comprehensive planning and flexibility. The plan outlines our current approach – but can be promptly brought forward if needed to manage an uncontrolled release of information. Similarly, key messages can be easily fashioned into a release at short notice.

3. We want to achieve the following communication objectives:

The Ministry must aim to act to build and maintain trust in publicly funded health services. We'll do this by providing timely information and advice to the public, media and the sector; linking in with other Government and health agencies; and supporting those affected. The Ministry has been working closely with Tu Ora Compass PHO and government agencies to ensure clarity on roles and responsibilities and using agreed and shared messaging. These are outlined below.

	Roles and responsibilities	**Spokesperson**
Ministry of Health	- health system response and assurance - primary media liaison - first point of contact for affected individuals (via contact centre)	Dr Ashley Bloomfield, Director-General of Health
Tû Ora Compass Health	- issue ownership and technical response - primary care interface	Martin Hefford, Chief Executive
GCSB	- wider government sector security - results of initial scan	Andrew Hampton, Director-General of the GCSB

4. Communications on this issue will be targeted at specific audiences:

There are five primary audiences for information provided by the Ministry (summarised in the table below):

- the public – including particular groups that may be more obviously affected and ensuring they're aware of support offered
- the health sector – particularly primary care – and providing sufficient timely information to allow them to be able to perform their jobs appropriately in relation to the issue
- Ministers and Government – primarily the Minister and Associate Ministers of Health, other related Ministers, and DPMC.
- other government agencies, particularly those also affected by this issue.
- Ministry staff – so they are informed about the Ministry's role, the action being taken and its impact, so they can either assist with the response, or work to manage its effect on the sector

Summary of Communications Activity

	Patients	Wider Health sector	Public	Stakeholders
Tu Ora	Walk in GP clinics	Walk in GP or call	Web based information	
DHB	Web based information (affected DHBs)	Web based information (all DHBs)	Web based information	Information and messaging
Ministry	0800 Web based information	0800 Web based information	0800 Web based information Media	Information, messaging, Reference point
GCSB/CERT	0800	0800	0800 Media?	
Police	Receive complaints		Update on activity (through media?)	

5. We will reach those audiences by taking these initiatives:

Generally our plan is primarily focused on the public release of information through the media, our website and social media. Our primary approach is to communicate in ways that build and maintain trust. To do this we will be guided by the following:

- **Announcing early** – providing information promptly and regularly.
- **Using credible spokespeople** - **we** will use key spokespeople within the Ministry and health sector and share messaging
- **Being accountable and transparent**. We will be candid about what we can and can't say, describe the process we are following to provide answers to questions we can't currently answer; and use appropriate channels to achieve our aims.
- **Listening and responding–** ensuring a good feedback loop with our 0800 call centre; social media; and sector feedback to assist in responding appropriately.
- **Refining plans**. As issues and concerns arise, we will be refining our response and communicating the appropriate actions taken.

Our communications will emphasise our efforts to put people and their health first – and the importance of keeping secure their health-related information.

6. Key messaging:

What happened

Unauthorised cyber access to digital information has now been identified as affecting five lower North Island based PHOs (primary health organisations).

A careful investigation has not been able to determine with any certainty whether the unauthorised access resulted in information being taken. We may never know whether information was taken.

Despite this uncertainty the PHOs are informing the public of the event and of the steps they can take to reduce the risk of scams or other illegal activity.

The unauthorised access is a crime and has been referred by Tu Ora Compass Health PHO to the Police. The first unauthorised incident occurred in 2016 and the most recent incident happened on 5 August this year.

Tû Ora Compass links with four other PHOs in the Wellington, Wairarapa and Manawatu areas -THINK Hauora, Cosine, Te Awakairangi and Ora Toa PHOs.

This means data may have been accessed for up to an estimated 1 million people and could cover data held by the PHOs going back to 2002.

None of the PHOs hold information kept by GPs as part of the notes they take when you consult your doctor.

Individual health records, which are a doctor's personal record of health information related to individuals, are NOT affected and are NOT accessible. However associated information relating to individuals and their health may have been accessible.

This could potentially include an individual's National Health Index number, name, date of birth, address, ethnicity, gender and GP practice. For a smaller number of people, it could potentially include laboratory results, alcohol or drug use, or referrals to counselling or specific services.

The primary unauthorised access was to the Tû Ora Compass PHO website. The PHO's website was defaced in early August 2019.

The PHO took immediate steps to contain the incident and investigate its extent. On 15 August, it publicised what it had found and the steps it had taken.

PHOs ensure the provision of essential primary health care services, mostly through general practices, to people who are enrolled with the PHO.

The Ministry of Health has been working closely with Tu Ora Compass Health PHO following confirmation of illegal cyber access to its computer system.

The affected PHOs and the Ministry have sought advice on balancing the level of information provided publicly about the incidents without increasing further security risk.

The media are asked to take care with their messaging as we know prominent reportage of these types of incidents increases the frequency of online scams or phishing attacks targeting those affected.

What's being done for those affected

Advice to anyone concerned about these incidents is to contact xxx (placeholder Moh call centre: 0800 855 066)

Additional supports, such as counselling, health advice or other services are being arranged for those people concerned by the unauthorised access.

Health authorities can provide generic data about information that may have been accessed but not at an individual level though this is currently being looked at.

Advice to those affected

Any approach by anyone seeking information or money based on information thought to be obtained from unauthorised access, should be referred immediately to the police.

Advice on keeping yourself safe from scams and to reduce the risk of misuse of your identity or information is provided by Netsafe https://www.netsafe.org.nz/scam-tips/ or CERTNZ https://www.cert.govt.nz/individuals/guides/stepping-up-your-cyber-security/cyber-security-social-media/

That advice includes:

- watch out for scams or phishing by phone, text or email
- be cautious about clicking on links and attachments in test or email
- don't give out personal information without checking on the company asking and then contact them via another method to verify the authenticity of the request

Actions being taken

The Tû Ora Compass PHO has implemented new security controls and is continuing to analyse information related to the incident to help inform the response.

The incident is prompting warnings, advice, additional testing and planning for further protective measures.

Additional monitoring and cyber stress testing of leading health sector agencies' computer security is being undertaken. The Ministry is working with sector agencies to strengthen defences following the testing.

The Ministry of Health and the Government Communications and Security Bureau believes the testing now underway will identify areas where further remedial action can be taken regarding these PHOs and at any other health agencies which may require strengthened security measures.

The outcome of this work is expected to result in a report summarising what was found, and the measures put in place to increase resilience. This report is expected to be completed by early in the New Year.

7. Key health spokespeople

Ministry of Health: Director General of Health Dr Ashley Bloomfield

Tu Ora Compass Health: Chief Executive Martin Hefford**.**

8. Release approach

MoH received a media query on 3 October 2019 from the Dominion Post asking for confirmation that malware was discovered on a computer system at Compass and that MoH has been notified.

MoH is currently working with the reporter on a possibility information is shared with that reporter under embargo for a Saturday 5 October publication. A media conference would be held on Saturday 5 October for wider public notification.

9. Planned sequencing (advanced by a media inquiry of 3 October)

Thursday 3 / Friday 4 October 2019

Planning continues for briefing of stakeholders Thursday / Friday (Tu Ora briefing affected GP practices; MoH briefs other primary care stakeholders)

Friday 4 October

1030 Tu Ora and MoH interviews with Stuff journalist Tom Hunt for caveated story embargoed online til 5am Saturday, and in print editions.

Saturday 5 October

0800 hrs Ministry of Health and Tu Ora media conference – venue either 133 Molesworth St.

0900 hrs media conference wraps up

To follow: media / social media monitoring / 0800 call rate and respondent feedback. Messaging fine-tuned considering feedback

Monday 7 October

0700 hrs media interview requests for breakfast TV / radio considered

0900 hrs key lines circulated to stakeholders

1000 hrs media advisory published

1200 hrs website updated in response to feedback

1400 hrs media conference – 133 Molesworth St;

1600 hrs information related to the incident (background papers and advice) proactively published on website.

1700 hrs feedback from media/social media/GP practices/PHOs / 0800 collated to inform messaging for Saturday.

1800 hrs decision on media approach for Tuesday

Tuesday 8 October if needed

0700 hrs media interview requests for breakfast TV / radio considered

0900 hrs key lines circulated to stakeholders

1000 hrs media advisory published

1200 hrs website updated in response to feedback

1400 hrs media conference – 133 Molesworth St; spokespeople from Ministry/PHO/ + CERT (keep yourself safe online TBC) present

1600 hrs information related to the incident (background papers and advice) proactively published on website.

1700 hrs feedback from media/social media/GP practices/PHOs / 0800 collated to inform messaging for Saturday.

Appendices

1. **Tu Ora Compass Health communications plan**
2. **Questions and answers (Ministry specific)**
3. **MOH Draft PR 3 October**

Questions and Answers

How do I know if my information has been accessed?

If you live in the lower North Island (Palmerston North or lower) then you are likely affected. However, we don't know if any information was taken. The five PHOs do not hold consultation notes written by doctors after consulting with you. Other information including referrals, diagnostic tests, and laboratory results were held and may have been accessed. The data held by the PHOs goes back to 2002.

How can I find out what's held about me?

We can't at this stage provide information about individuals that was on the IT system due to the way the information was collated and reported. But we can say what types of information was held. The Ministry and PHO continue to investigate whether this information, at an individual level, can be realistically provided.

Secure information exchange between health agencies is critical for the provision of modern, quality and evidence-based healthcare.

Is my information still at risk?

Tu Ora Compass PHO has now strengthened its security following the incident. The Ministry of Health is working with other PHOs and DHBs to check their systems have also been strengthened.

Why did this happen?

The PHO's investigation shows that its systems were vulnerable due to it having outdated software which was no longer being updated to ensure it remained protected. The PHO was in the process of updating its software when it became aware of the breach.

Who is to blame?

The key focus to date has been on ensuring the cyber security risks are managed. There remains ongoing work to look at who was at fault and how we can improve systems to limit the chances of this occurring again.

Can this happen again?

The Ministry of The Ministry of Health is working with other PHOs and DHBs to check their systems have also been strengthened. This work is expected to take around 3-4 months. The Ministry will be publicly reporting on the outcome of this work in the New Year.

Why are there so many instances of information breaches of information?

A: CERT NZ The Government's Computer Emergency Response Team received close to 1200 reports in the three months to 30 June this year – the bulk of them being scams or fraud. The health sector has started on a programme of strengthening its cyber security. This will continue.

Why did it take so long for the problem to be found?

The investigation revealing the breaches in the past was triggered by the defacing of the website. The same week the PHO was planning to start the upgrade of its cyber security. The Ministry of Health is now working with PHOs on strengthening their cyber security.

How long have you known and why did you take so long to tell everyone?

Health authorities have known since 5 August 2019 and since then have been working to provide more information about the incident – Tu Ora published a media release on 15 August 2019 about its website being defaced.

Before making the information, public health authorities wished to ensure there were appropriate supports in place for people who may be concerned at the potential disclosure – as well as taking steps to ensure publicity wouldn't increase the risk of further online harm.

Testing and monitoring of other PHOs and DHBs has been carried out and security measures improved for those organisations.

MOH Draft PR 3 October

Ministry of Health supporting PHO over cyber intrusion

The Ministry of Health has been working closely with Tu Ora Compass Health PHO following confirmation of illegal cyber access to its computer system.

Tu Ora notified the Ministry as soon as it became aware of unauthorised access in early August. Further investigation confirmed previous illegal unauthorised access dating back to 2016.

This means data may have been accessed for up to an estimated 1 million people and could cover data going back to 2002.

The unauthorised access has now been identified as affecting five lower North Island based PHOs (Public Health Organisations) which have a relationship with Tu Ora. The illegal access is a crime and has been referred by Tu Ora to the Police.

"Before making the cyber intrusion public, public health authorities wanted to ensure there were appropriate supports in place for people who may be concerned at potential disclosure – as well as taking steps to ensure publicity wouldn't increase the risk of further online harm," says Dr Ashley Bloomfield, Director-General of Health.

"We can't at this stage provide information about individuals that was on the IT system due to the way the information was collated and reported. But we can say what types of information was held.

"The Ministry and the PHO continue to investigate whether this information, at an individual level, can be realistically provided.

"Secure information exchange between health agencies is critical for the provision of modern, quality and evidence-based healthcare."

The Ministry of Health supports the affected PHOs in publicising these incidents of unauthorised access. Tu Ora Compass PHO has now strengthened its security following the incident.

Dr Bloomfield says anyone concerned about the incidents can contact the Ministry of Health's call centre on 0800 499 500.

"Additional supports, such as counselling, health advice or other services are being arranged for those people concerned by the unauthorised access."

The Ministry of Health is working with other PHOs and DHBs to check their systems have also been strengthened. Additional monitoring and cyber stress testing of leading health sector agencies' computer security is being undertaken. The Ministry is working with sector agencies to strengthen defences following the testing.

The Ministry of Health and the Government Communications and Security Bureau believes the testing now underway will identify areas where further remedial action can be taken regarding these PHOs and at any other health agencies which may require strengthened security measures.

The Ministry will be publicly reporting on the outcome of this work in the New Year.

END

BACKGROUND

Primary health organisations (PHOs) ensure the provision of essential primary health care services, mostly through general practices, to people who are enrolled with the PHO. PHOs are funded by district health boards (DHBs), who focus on the health of their population.