Final (Incomplete) Draft Communications and Response Project Plan

Includes: copies of current media releases/Q&As in appendices

Document History

Version	Date	Distribution list
0.5	19/09/2019	JT, SFS, AD
0.6	20/09/2019	JT, SFS, AD
0.7	20/09/2019	JT, AD
0.8	20/09/2019	JT, AD
0.9	20/09/2019	JT, AD, SFS, CH, LD, MF,DD,PA
1.0	22/09/19	JT, AD, SFS
1.1	22/09/19	JT, AD, SFS
1.2	24/09/2019	JT, AD, SFS, SC
1.3	25/09/2019	JT, AD, SFS
1.4	29/09/2019	JT, AD, SFS,PA, DM, AC, DD, RH, CD, RP, LD, MF, CH
1.5	30/09/2019	JT, AD, SFS, MH
1.6	01/10/2019	AD, SFS
1.7	4/10/2019	JT, AD, SFS, MH
1.8	Overrun by unplanned release	JT, AD, SFS, MH

Approval	Name	Signature	Date
Tū Ora CEO	M Hefford		

1. Table of Contents

1. Contacts

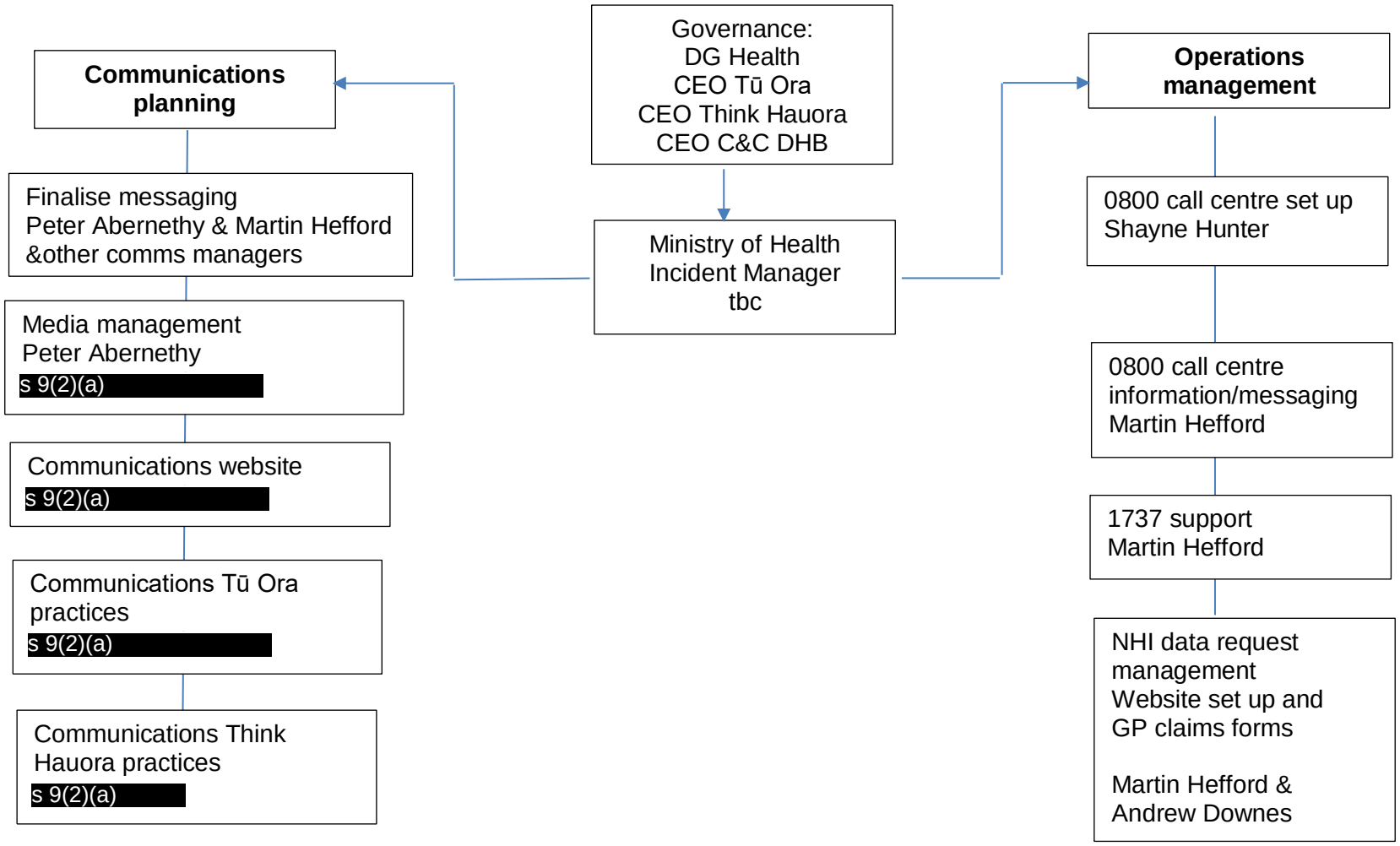
Organisation	Name	Role	Email	Tel no
Ministry of Health	Kate Crawford	National coordination Centre Incident Manager – starts 9:00am 01/10/2019	??	??
Ministry of Health	Darren Douglass	National coordination Centre Incident Manager – until noon 30/09/2019	Darren.Douglass@health.govt.nz	s 9(2)(a)
Ministry of Health	Peter Abernethy	Media relations manager	peter.abernethy@health.govt.nz or media@moh.govt.nz	s 9(2)(a) s 9(2)(a)
Tū Ora Compass Health	Justine Thorpe	Acting CEO	s 9(2)(a)	s 9(2)(a)
Tū Ora Compass Health	Martin Hefford	CEO and Tū Ora incident manager from (2/10/2019)	s 9(2)(a)	s 9(2)(a)
Tū Ora Compass Health	s 9(2)(a)	Communications Advisor	s 9(2)(a)	s 9(2)(a)
Tū Ora Compass Health	Andrew Downes	Tū Ora incident manager until 2/10/2019	s 9(2)(a)	s 9(2)(a)
Acesso	s 9(2)(a)	s 9(2)(a)	s 9(2)(a)	s 9(2)(a)
Acesso	s 9(2)(a)	s 9(2)(a)	s 9(2)(a)	s 9(2)(a)
Acesso	s 9(2)(a)	s 9(2)(a)	s 9(2)(a)	s 9(2)(a)
Think Hauora	Chiquita Hansen	CEO	s 9(2)(a)	s 9(2)(a)
Think Hauora	Lyn Daly	Practice development mgr	s 9(2)(a)	s 9(2)(a)

THINK Hauora	s 9(2)(a)	Communications Manager	s 9(2)(a)	s 9(2)(a)
Capital/Coast DHB	Rachel Haggerty	Acting CEO	s 9(2)(a)	s 9(2)(a)
Capital/Coast DHB	s 9(2)(a)	Communications manager	s 9(2)(a)	s 9(2)(a)
MidCentral DHB	Jonathon Howe	Corporate Communications Manager	s 9(2)(a)	s 9(2)(a)
Dept Prime Minister and Cabinet	Catherine Delore	Director Communications & Engagement	s 9(2)(a)	s 9(2)(a)
Government Security and Communications Bureau	s 9(2)(a)			
Government Security and Communications Bureau	s 9(2)(a)			

2. Incident participants and roles

Organisation	Role	Participant
Ministry of Health	Incident approvals	Ashleigh Bloomfield (DG Health) Keriana Brooking (acting DG Health)
	Spokesperson	Ashleigh Bloomfield/Keriana Brooking & Shayne Hunter (DDG Health and Digital) Peter Abernethy
	Comms lead	Kate Crawford/Greg Phillips
	Incident lead	Darren Douglass
	Technical lead	
Tū Ora Compass	Incident approvals	Justine Thorpe (Acting CE)
	Spokesperson	Larry Jordon (Chair) & Justine Thorpe & Martin Hefford
	Comms lead	s 9(2)(a)
	Incident lead	Martin Hefford & Andrew Downes
	Technical lead	s 9(2)(a)
THINK Hauora	Incident approvals	Chiquita Hansen (CE)
	Spokesperson	Bruce Stewart (Chair)
	Incident lead	s 9(2)(a)
	Technical lead	
	Comms lead	s 9(2)(a)
Capital/Coast DHB	Spokesperson	s 9(2)(a) & Rachel Haggerty (acting CE)
	Technical lead	s 9(2)(a)
MidCentral DHB	Spokesperson/comms lead	Jonathon Howe
	Technical lead	s 9(2)(a)

3. Proposed CIMs Structure



4. Decision History

Decisions waiting confirmation

No.	Item	Date raised	Raised by	Allocated to
1.wc	That a low key communications approach is no longer seen as appropriate and that the approach will be higher profile from the start e.g. media conference. If so: a) all comms messaging needs review and updating b) in scope and out of scope messaging will need review	27/09/2019	A Downes	NHCC incident manager
2.wc	Who is the ultimate decision maker for any and all decisions associated with this disclosure/response plan	27/09/2019	R Haggerty	NHCC incident manager
3.wc				
4.wc				
5.wc				
6.wc				
7.wc				
8.wc				
9.wc				
10.wc				

Decisions Confirmed

No.	Item	Date decision made	Decision maker
1.DC	The Ministry of Health will establish and resource an 0800 number for the public to call for information about this incident	27/09/2019	Ministry
2.DC	The Ministry of Health will establish a national health coordination centre (NHCC) to manage the communications and response plan and Greg Phillips will be seconded from CCDHB to be the incident manager (starting 30/09/2019)	27/09/2019	Ministry
3.DC	Tū Ora will establish a clinical support process via 1737 for people who are distressed and may need support	27/09/2019	Ministry/ Tū Ora
4.DC	Tū Ora will be able to submit a resource/budget for the clinical support response and other associated items to the Ministry	27/09/2019	Keriana Brooking Justine Thorpe
5.DC	The communications response will be able to refer to working with NCSC	27/09/2019	s 9(2)(a) Justine Thorpe
6.DC			
7.DC			
8.DC			
9.DC			
10.DC			

5. Action Logs

Item	Date raised	Assigned to	Completed Y/N
Arrange fully resourced 0800 call centre function	27/09/2019	Shayne Hunter	
Establish national health coordination centre	27/09/2019	Darren Douglass	Y
Update all communications messaging when communications approach confirmed (refer decision waiting confirmation 1-wc)	27/09/2019	Peter Abernethy Martin Hefford s 9(2)(a) [redacted]	
Confirm unplanned release process	27/09/2019	Peter Abernethy s 9(2)(a) [redacted]	
Present resource/budget estimates for clinical support for those seeking support to Ministry	27/09/2019	Justine Thorpe A Downes	
Arrange estimated support required via 1737 for those that may require support	27/09/2019	Justine Thorpe A Downes	
Arrange swipe card access to Ministry of Health for Martin Hefford, Justine Thorpe, s 9(2) [redacted], s 9(2)(a) [redacted], Andrew Downes	29/09/2019	Darren Douglass	
Continue to refine data analysis of data held to segment more and highlight sensetive data	30/09/2019	A Downes	
Add page numbers to comms plan	30/09/2019	A Downes	Y
s 9(2)(ba)(i) [redacted]	30/09/2019	s 9(2)(a) [redacted]	
s 9(2)(a) [redacted] will be contacted by David Metcalf/Darren Douglass	30/09/2019	Justine Thorpe	Y
Add evening forums for GP practices the evening prior to 'go live' to the plan to brief on situation and what they might expect to need to deal with	30/09/2019	Justine Thorpe	Y

6. Detailed Plan

Item	Days prior to go live	Timings	Sign off
Provide Think Hauora with draft communications plan for comment	-25	5:00pm	n/a
draft communications plan completed	-23	10:00pm	Tū Ora CEO
draft communications plan provided to the central agency incident group for approval (Tū Ora and Think Hauora CEO)	-21	5:00pm	Chair central agency incident group
Briefing to Tu Ora Board by DDG Digital and data	-20	6:00pm	
Approval of communications and response plan and advice to Ministers	-18	5:00pm	Central agency CEs
Ministry of Health confirm that 0800 number and associated call centre will be established	-18	5:00pm	Ministry of Health incident manager
Briefing to Think Hauora Board by DDG Digital and data	-18	5:00pm	
Advice received from Ministers	-15	5:00pm	
Discussion with Health and Disability Commissioner	-14	**3:30pm**	
Organise media training for spokepeople from all agencies	-14	5:00pm	Ministry of Health incident manager
Finalise all messaging and communications plan	-11	5:00pm	Ministry of Health incident manager
Circulation of final communications plan to key groups: Tū Ora Board Think Hauora Board Office Privacy Commissioner Health and Disability Commissioner C&C DHB WDHB MDHB	-11	5:00pm	n/a

Item	Days prior to go live	Timings	Sign off
Provide Think Hauora with draft communications plan for comment	-25	5:00pm	n/a
Media training for media spokespeople from all agencies	-11	5:00pm	
organise 0800 number (reachable from overseas)	-8	5:00pm	Ministry of Health incident manager
secure staff for 0800 number assume 13 FTE	-8	5:00pm	Ministry of Health incident manager
organise incident room at Ministry (joint room for Tu Ora and Ministry)	-8	5:00pm	Ministry of Health incident manager
Email channel for queries to be sent to Tu Ora set up and linked to Tū Ora Communications manager (? Should go to incident room?) e.g from 0800, practices etc	-8	5:00pm	
Confirm s 9(2)(b)(ii) claim form (screening term) to be distributed to practices	-5	5;00pm	A Downes
Confirm s 9(2)(b)(ii) service template to be distributed to practices	-5	5:00pm	A Downes
Staff meeting Tū Ora health practice relationship managers	-5	9:00am	
Staff meeting Think Haurora practice relationship managers (or equivalent)	-5	9:00am	
Orientation to 0800 number staff about the incident, their role and information they can provide	-5	5:00pm	Ministry of Health incident manager
Orientation for Ministry, PHO front desk reception/operators about what to do if enquiries come through	-5	5:00pm	Ministry of Health communications manager PHO communications managers
Confirmation of spokesperson for Tū Ora and Think Hauora for media interviews	-5	5:00pm	

7. Go Live Plan

Communications GO LIVE			
Item	**date**	**Timings**	**By whom**
Creation and upload of cyber incident page on Tū Ora website with releases and FAQs. (Page to be hidden until needed)	Starts 10/10/2019 and ends 10:00am 15/10/2019	From –5 days	s 9(2)(a)
Arrange media release	14/10/2019	5:00pm	Peter Abernethy
Tu Ora Practice forums	14/10/2019	6:00pm	CEO, Chair, acting CE + Board members as required
Think Hauora practice forums	14/10/2019	6:00pm	CEO, Chair, Board members as required
Communication to Cosine, Ora Toa and Te AHN	14/10/2019	??	??
Implement s 9(2)(b)(ii) claim form across all Tu Ora, Cosine, Ora Toa and Think Hauora practices	15/10/2019	9:00am	??
Implement s claim form across all s practices	15/10/2019	9:00am	s 9(2)(a)
All staff meeting Tū Ora	15/10/2019	9:00am	
All staff meeting Think Hauora	15/10/2019	9:00am	
Tū Ora cyber incident page go live	15/10/2019	10:00am	s 9(2)(a)
Press conferences: Central agencies Cert NZ Others	15/10/2019 - 20/10/2019	Start 10:00am	Coordinated by Ministry communications manager with support from Tū Ora communications manager and

			Think Hauora communications manager
Media release to: Stuff Manawatu Standard Scoop Pulse IT NZ Doctor Wairarapa Times		10:00am	Tū Ora communications manager
Emailed communications to: GP College, GPNZ , N4		1:00pm	Tū Ora communications manager
Other providers e.g. Optometrists		2:00pm	Tū Ora communications manager

8. Background

During the afternoon of the 5th August 2019 Tū Ora was subject to a malicious cyber intrusion that resulted in a defacement to its public facing website. By 4:30pm the incident was contained and since that time Tū Ora has increased the capacity and capability of its cyber threat detection and management systems as well as working to restore services that needed to be taken off-line as a result of the incident. A cyber security expert was contracted by Tu Ora to do a more indepth review on the 6th of August and the review found evidence of prior intrusions. Cert NZ were notified, and a copy of the cyber expert reprot provided to the NCSC. (refer Appendix 1 for more detail).

During the course of this event all relevant agencies were advised, e.g. Ministry of Health and the Office of the Privacy Commissioner and a media statement was also released on the 15th August. Tū Ora managed to restore all services that were taken off line by 18th September.

Investigation of this event identified that:

1) s 9(2)(c), s 9(2)(e) [redacted]
2) s 9(2)(c), s 9(2)(e) [redacted]
3) s 9(2)(c), s 9(2)(e) [redacted]
4) s 9(2)(c), s 9(2)(e) [redacted]
5) Whilst there is no evidence that access to patient data has occurred, Tū Ora cannot rule out the possibility that patient data may have been accessed from the period of July 2016 to February 2019.
6) The database that supplies Tu Ora Compass Health, also stores data used by Think Hauora – a PHO based in Palmerston North, and some information on patients enrolled in other PHOs in the Wellington area, accessing services provided by Tu Ora.

Subsequently a number of central agencies have come together to develop a tiered response to this event(s).

Tū Ora has an obligation to responsibly disclose that patient data may have been compromised during this extended period from 2016 to 2019 and central agencies will have a role to respond to wider health sector and New Zealand interests.

The purpose of this communications plan is to describe and manage the approach, messages, and actions regarding:

1) Tū Ora ‘s obligations to responsibly disclose that patient data may have been compromised during this extended period from 2016 to 2019
2) The response from central agencies around wider health sector and New Zealand interests.

9. Assumptions

1) This is a live document and is updated as more information is available. Due to the size of the document and potential unplanned release, key messages, the Press release are updated as priority. Information may change.
2) The ‘go live’ for this communication will be 15th October at 10:00am
3) Central agencies will provide approval of this communications plan by 1st October 2019
4) Central agencies will establish a wider communications strategy to manage the wider aspects of pro-active communications and responses in relation to the health sector and wider New Zealand interests

10. Objectives

The main objective of this plan is to:

1) Re-build trust and credibility in the way that organisations, who deliver core services to the New Zealand public, and their associated central government agencies:
    a) pro-actively protect sensitive data and
    b) respond to malicious intrusions as and when they occur

We will achieve this by:

1) Responsibly disclosing information about the potential exposure of patient data held by Tū Ora over a prolonged period of time , (from July 2016 to February 2019), in a series of proactive communications with simple everyday language, which are balanced and will not cause undue alarm to the public
2) Creating a communications funnel where people and organisations can choose to read top line messages with graduation to more detail if required
3) Demonstrating the government level response to this situation for the health and other sectors
4) Planning for interim messages to be available should an unplanned release occur.

11. Stakeholders and Key Interests

The following table briefly describes the main stakeholders and their expected key interests that need to be considered for this communications plan.

Stakeholder	• Key interest
The public	• Unauthorised Disclosure of my personal health information • Why my data is held by the PHO • Safety of my data held by agencies who are meant to look after it • How might my stolen data be used against me e.g. identity theft • That things are being done to address this problem
General practices	• Unauthorised Disclosure of personal health information of staff employed at the practice • Unauthorised Disclosure of personal health information from patients to agencies like PHOs are meant to be custodians of their data • Unauthorised disclosure of practice related financial data • Trust in security of data held by agencies that are not GP practices e.g. PHOs • Trust in security when sharing data with external agencies and other health providers • Security of own practice systems • That actions are being taken to address this problem and what actions the practice may need to take if any
Tū Ora Board	• Unauthorised Disclosure of my personal health information • Unauthorised Disclosure of personal health information of staff employed at the PHO • That providers will be confident to continue sharing data with PHOs for analysis • Security of PHO systems and especially the move to Azure • That actions are being taken to address this problem • Reputation of Tū Ora and members of the Board
THINK Hauora Board	• Unauthorised Disclosure of my personal health information • Unauthorised Disclosure of personal health information of staff employed at the PHO • That providers will be confident to continue sharing data with PHOs for analysis • Security of PHO systems • That actions are being taken to address this problem and what actions the Board may need to take if any • Reputation of Think Hauora and members of the Board
PHOs directly impacted THINK Hauora	• Unauthorised Disclosure of personal health information of staff employed at the PHO or sub contracting organisations

Te Awakairangi Health Network, Ora Toa and Cosine and any sub-contractors	• Unauthorised Disclosure of personal health information from patients that agencies are meant to be custodians of their data • Providers not wanting to trust sharing data with PHOs for analysis • Security of PHO systems • That actions are being taken to address this problem and what actions the PHO may need to take if any
C&CDHB, WDHB, MDHB, HVDHB	• Unauthorised Disclosure of personal health information of staff employed at the DHB • That providers will be confident to continue sharing data with PHOs for analysis • Security of PHO systems • Security of DHB systems • That actions are being taken to address this problem and what actions the DHB may need to take if any
other PHO's and DHBs	• That providers will be confident to continue sharing data with PHOs for analysis and between providers for patient care • Security of PHO systems • Security of DHB systems • and what actions the PHO/DHB may need to take if any
Ministry of Health	• Unauthorised Disclosure of personal health information of staff employed at the Ministry • That providers will be confident to continue sharing data with PHOs for analysis and between providers for patient care • Security of PHO systems • Security of DHB systems • Security of Ministry systems • Actions and investment that may be required across the wider health sector to reduce risk
Other non government medical agencies such as Royal New Zealand College of GPs, GPNZ	• Unauthorised Disclosure of personal health information of staff employed by agencies • That providers will be confident to continue sharing data with PHOs for analysis and between providers for patient care • Security of PHO systems • Security of DHB systems • Security of Ministry systems • Actions and investment that may be required across the wider health sector to reduce risk
Other central agencies	• Risks to wider New Zealand core agency infrastructure and data from this event • Actions and investment that may be required across core agency infrastructure to reduce risk
Health and Disability Commissioner and Children's Commissioner	• Dealing with complaints about the event

12. Approach

Principles and Guidelines

Generally our communications plan is underpinned with the principles of risk communications:

1) https://emergency.cdc.gov/cerc/resources/pdf/cerccheckliist.pdf
2) https://emergency.cdc.gov/cerc/resources/pdf/leaders.pdf

Our communications are primarily focused on the public release of information through the media, websites and social media. An option under consideration is an open letter to patients in newspapers. Our primary approach is to communicate in ways that build and maintain trust. To do this we will be guided by the following:

1) **Announcing early**. Providing information promptly and regularly
   Using credible spokespeople
2) **Transparency.** Be candid about what we can and can't say; what process we are following to provide answers to questions we can't currently answer; and when we expect to be able to give more information
3) **Listening and responding.** Ensuring a good feedback loop with MoH Call centre, Healthline; social media about any issues and use this information to assist the Ministry and agencies in responding appropriately.
4) **Refining plans.** As issues and concerns arise we will be refining our plans to respond.
5) **Timeliness.** Quickness and appropriateness of our response underpins all actions planned here.
6) **Flexibility.** In any significant event we know information can change rapidly. Further, to manage an unexpected release there is an emergency **response in appendix 7**

We have endeavoured to provide detail as well as flexibility in our planning to date. We acknowledge that there are many agencies involved in this issue and our planning is likely to continue to evolve to reflect the different expertise and decisions made.

The following guidelines apply to this specific communications plan and the core interest of personal health data. They are sourced from the Office of the Privacy Commissioner's website (OPC), from two discussions with the OPC and discussions with the Ministry of Health;

1) It's a good idea to be open about what's happened and the steps you're taking to fix it

2) If there's no likely consequences from the breach, or if telling people would cause more worry and harm than not telling them, it may be acceptable not to tell affected individuals

3) If the people could suffer harm and need to act to protect themselves, for instance by changing their passwords or monitoring their bank accounts for malicious activity, then you should probably tell them about the breach and steps you are taking to mitigate it

4) Lessons learned and what people can do to stay safe online are important and use other existing agencies to help propagate what has been learned and what individuals and organisations should do

5) Messaging will be kept in scope as defined in this communication plan. Broadly speaking:

    a. Tū Ora will communicate and respond to:

        i. enquiries around the event and its remediation

        ii. advice on where to get information such as Tū Ora website and 0800 number

        iii. the potential for unauthorised access to personal health data between July 2016 and February 2019

        iv. advice around what actions an individual may want to take e.g. staying safe online as per CERT NZ advice and

        v. advice on seeking support if distressed e.g. refer 1737

    b. Central agencies will communicate and respond to enquiries around wider impacts to the health sector e.g.

        i. what is the level of security risk across the health sector and what is happening to remediate that

        ii. maintaining trust amongst service providers to share clinical data for patient care and reporting purposes and

        iii. wider New Zealand interests in general such as the general cyber threat to New Zealand

Communication Model

The communications model noted in figure 1 will filter parties to the right level of information for the information they need and questions they may have. It is anticipated that responsible disclosure can be managed with a media release, access to FAQs via the Tū Ora website and access to an 0800 number for more information.

Some people may need support if they are feeling distressed by it, in addition to information via the 0800 number these people will be able to seek support from the national 1737 mental health support line.

Some people and organisations e.g. media and political organisations may want to have detailed information about wider risk to New Zealand Health sector and other New Zealand related cyber interests.

It is expected that Tū Ora and the Ministry of Health will focus on the left side of the filter as this will relate to individuals and their data, while the Ministry of Health and other central agencies will respond more to wider health sector and New Zealand interests on the right.

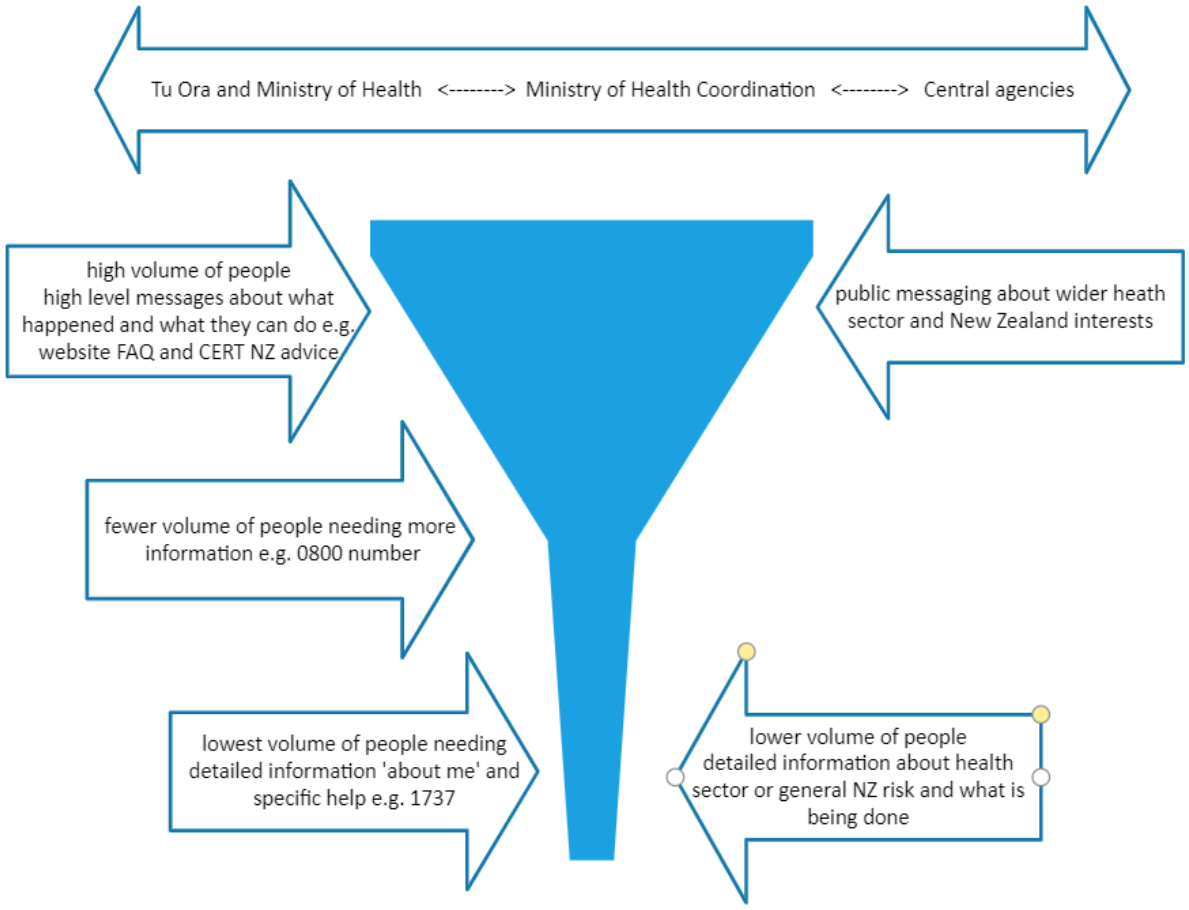


Figure 1 - high level communications model

Support Model for Public

Figure 2 describes the high level model for public information and support

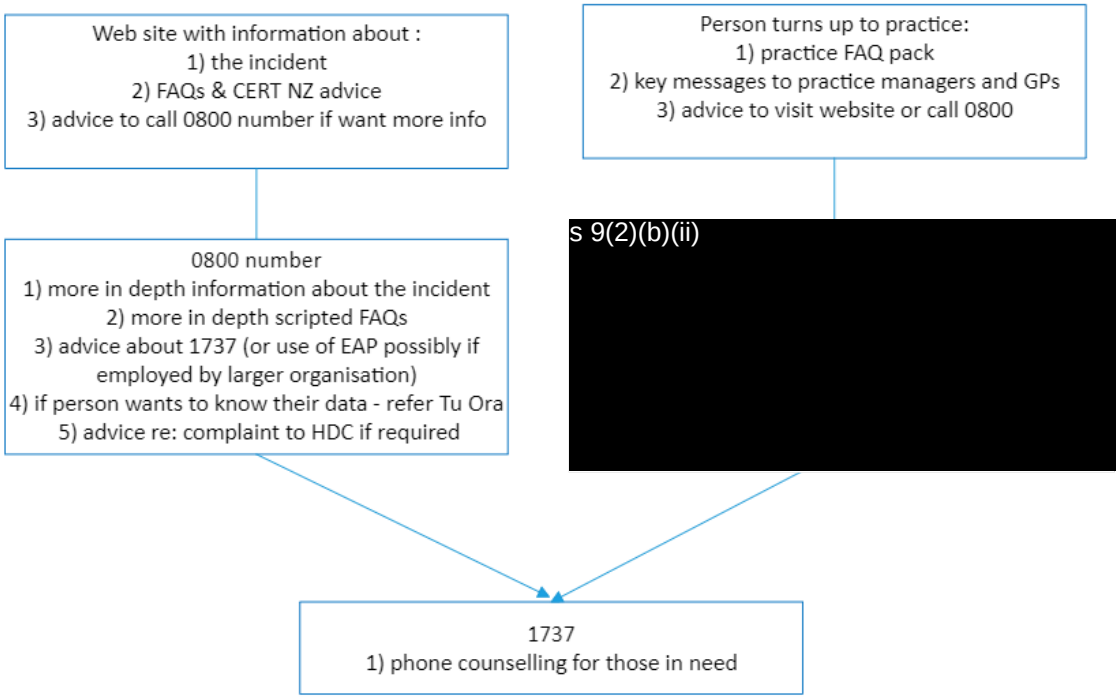
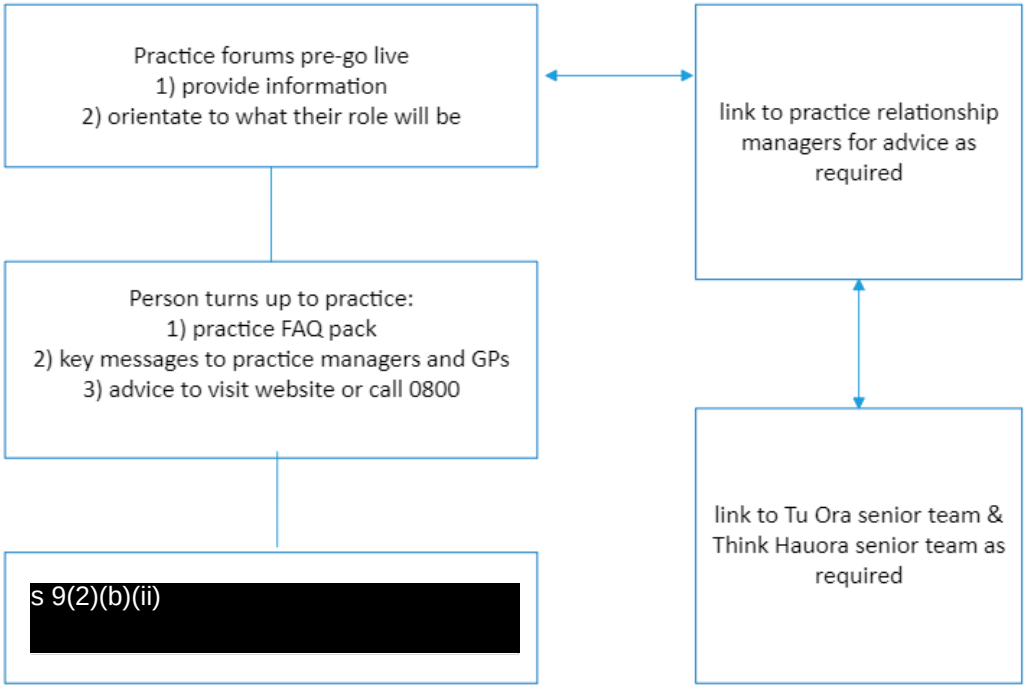


Figure 2 high level public support

Practice Support Model



Scope Statement

The activities outlined in this communications plan are primarily targeted to:

1) The population of the greater Wellington, Wairarapa and Manawatu regions who were enrolled with a GP between 2002 and 2019, whose data has been shared with Tū Ora via their general practice.
2) Contracted providers to PHOs including GP practices and other service providers in the same geographic area noted in (1)
3) The PHOs and DHBs that cover the same population in (1)
4) Other key stakeholder groups like Ministry of Health and Office of the Privacy Commissioner

The following table outlines the overall scope that this communication plan covers, and which group is broadly responsible for communications and responding to queries

In scope	**Primary information**	**Tū Ora**	**Central agencies**
enquiries around the event and its remediation	Refer to key messages and media statement in appendix 3 Refer FAQs in appendix 4 - 7	Primary lead	
the potential unauthorised access to data between July 2016 and February 2019	Refer to key messages and media statement in appendix 3 Refer FAQs in appendix 4 - 7	Primary lead	
advice around what actions an individual may want to take e.g. staying safe on line as per CERT NZ advice	Refer to key messages and media statement in appendix 3 Refer FAQs in appendix 4 - 7	Primary lead	
Where individuals can go if they want more information e.g. 0800 number	Refer to key messages and media statement in appendix 3 Refer FAQs in appendix 4 - 7	Primary Lead	0800 number and resources to be provided by central agencies
advice on seeking support if distressed e.g. refer 1737	Refer to key messages and media statement in appendix 3 Refer FAQs in appendix 4 - 7	Primary lead	
what is the level of security risk across the health sector and what is happening to remediate that	To be completed by central agencies		Primary lead
maintaining trust amongst service providers to share	To be completed by central agencies		Primary lead

clinical data for patient care and reporting purposes			
wider New Zealand interests in general such as the general cyber threat to New Zealand	To be completed by central agencies		Primary lead
Responding to media enquiries	Depends on assessment as to whether the enquiry is related to the event of more wider nature	Primary lead if related to event	Primary lead if related to wider health sector or New Zealand interests
Responding to Parliamentary questions	To be completed by central agencies with input if required from Tū Ora for the incident and other health sector and government organisations as required for wider perspectives		Primary lead

Out of scope	**Justification**
Disclosing names or any identification of people affected	Privacy of information
Contacting each patient whose data is held	As there are approximately 890,000 people affected this will take too long and we have no systems and resources to complete this in a timely manner. Instead there will be an 0800 number provided and resources by central agencies that will enable any affected individual to contact someone for more detail. We will publish an open letter in the amjor dailies in the area.
Providing copies of data that Tū Ora holds for each patient to them	Tū Ora would also need to implement a failsafe way of ensuring that someone asking for data is truly who they say they are. This would require an application process that may take weeks to process. Tū Ora is currently developing a query and new database to see if data can efficiently and accurately be returned for a single NHI Both of these need to be in place prior to committing to providing data back to those people that wish to understand this.
Disclosing information about sexual assault data	This data is handled and treated separately and generally pseudonymised. That does not rule out any possible risk. Disclosure has a high chance of resulting in harm, hence needs to be appropriately caveated.

13. Key Messages

The key messages are based on the following principles:

1. Being up front and transparent
2. Putting people and their information security first
3. Acknowledging responsibility
4. Taking all appropriate actions

Key messages:

- In August the Tū Ora website was defaced as part of a widespread global cyber incident
- During investigations, it was discovered that our I.T systems had been subjected to prior criminal cyber intrusions dating back to 2016
- It is likely that some patient information may have been accessible to cyber criminals during this time
- We can't say for certain whether unauthorised access has resulted in patient information being taken.
- There is no way of confirming what information was accessed during this time, or what and if anything was taken. We may never know.
- Tū Ora Compass Health holds information on individuals enrolled in the greater Wellington, Wairarapa and Manawatu regions including Danniverke and Paihiatua dating back to 2002.
- This includes those enrolled with Tū Ora, THINK Hauora PHOs.
- Other PHOs less impacted are Te Awakairangi, Cosine and Ora Toa PHOs.
- While the total current enrolled population for these regions is 648,000, we estimate around 913,000 ever enrolled people are potentially affected which includes those living, deceased and having moved in and out of the region during that time. (The number could also be zero as we have no clear evidence that data was removed or taken.)
- Information held could potentially include an individual's National Health Number (NHI), name, DOB, address, ethnicity, gender and GP practice. It could potentially also include lab test results, alcohol or drug use or referrals to counselling or specific services
- Your GP medical record is **not** held by Tu Ora, and is **not** potentially affected and **not** accessible as it sits with the individual medical practice.
- Information on the Patient portal if you use one (eg Managemyhealth) is **not** held by Tu Ora and so not affected.
- Associated information relating to individuals and their health may have been accessible such as booking and referral information to external services.
- We also hold information on services we provide directly.
- We take this seriously and we apologise for any distress this may cause to the public
- As stewards of individuals health information, it was Tū Ora's job to keep that information safe and secure all the time
- We apologise to all the people concerned for our failure to do that
- We take full responsibility for what has happened
- We immediately contained the incident and began to investigate its extent in partnership with the necessary authorities
- On 15 August we publicised what we had become aware of at that time
- There is no way to tell what the motive behind the intrusions may have been

- Police have been informed
- We have subsequently significantly strengthened our system and data security
- We are part way through a digital transformation programme which will provide even more security. Our new platform is built using a range of latest security tools which significantly strengthens our capabilities, guided by international experts and best practice.
- We've been working with experts to understand what happened including the Ministry of Health, Government Communications & Security Bureau (GCSB), the National Cyber Security Centre, and the Privacy commissioner
- Our focus now is to provide support to both medical centres and the public.
- Here's how to access more information and support for people concerned and wanting more support and information....

14. Media Management Post Go Live

All media requests will be forwarded to Peter Abernethy for review.
Peter will review and allocate the responsibility to manage the enquiry to the appropriate communications manager e.g. Ministry of Health or Think Hauora or MDHB or other. The guidelines noted previously will be used to determine the best responder. For example:

- If the query is related to the incident and its management the response will be made by Tū Ora

- If the query is related to wider health sector and New Zealand interests these will be made by Peter Abernethy at the Ministry of Health in the first instance.

15. Resources

0800 number

Item	Cost
0800 number for up to 1 month	TBC
Staffing for 0800 number Assume: • 8:00 – 9.00 pm from 15th October to 15th November • Assume administration level salary	TBC

Unplanned Communications release

Item	Cost
Resourced incident team for 1 week Assume comms managers from Tū Ora , MoH and CCDHB prioritised	Absorbed as this will be managed through communications managers from Ministry, Tū Ora , think Hauora, MDHB and C&CDHB

Support for Practices and Support For People Needing To Talk to Someone and/or Requests for Data

s 9(2)(b)(ii)


s 9(2)(b)(ii)


s 9(2)(b)(ii)

16. Dependencies

As noted previously the main dependencies for a ‘go live’ with this plan are as follows:

- Web site with media release and FAQs
- Resourced 0800 call centre in place
- ‘Response packs’ for practices in place
- 1737 agreement to field calls
- Funding for free GP visit secured
- Invoicing process for free GP visit

17. Risk Assessment

The following table describes some risks associated with delivering this communications plan and their mitigations.

It does not consider the wider risks associated with public or service provider reaction to this release e.g. GP practices decide to withhold data extracts to PHOs until they can be assured that data is as secure as desired. These are hypotheticals and are best dealt with by discussion at a sector level with central agencies to determine how these risks will be managed.

Risk Description		Risk Rating before Mitigations		Risk Level	Mitigations	Risk Rating after Mitigations		Risk Level
		Likelihood	Consequence			Likelihood	Consequence	
1	unplanned release of information from an individual who has been briefed due to high volume of individuals that have information	Likely	Major	High	agree comms plan with central agencies including release date within September have brief communications plan in place to be actioned within 30 minutes	Unlikely	Moderate	Low
2	Ministry of Health unable to resource 0800 number or resource this in a timely manner	Likely	Major	High	agree comms plan with central agencies including release date within September Ministry to confirm resoursing for 0800 number	Unlikely	Moderate	Low
3	Tū Ora unable to provide information to patients on what data is held by Tū Ora due to volume of requests	Likely	Major	High	agree with central agencies that this is not practical response for more than a small number of people i.e. Less than 100 considering resources available and also technical challenges	Unlikely	Moderate	Low

	Consequence	*Minor*	*Moderate*	*Major*	*Severe*
Likelihood					
Almost Certain		Medium	High	Extreme	Extreme
Likely		Low	High	High	Extreme
Possible		Low	Medium	High	High
Unlikely		Very Low	Low	Medium	High
Rare		Very Low	Low	Medium	Medium

Risk level	Definitions
Extreme risk	Will cause project to fail, clients may come to actual harm
High risk	Needs constant governance intervention to avoid project failure. Clients at risk of harm
Medium risk	Needing additional project controls across more than one of schedule, cost and quality
Low risk	Item(s) being dealt with through normal project controls
Very low	Noting only

18. Evaluation

Our communications response will be monitored with feedback from media/social media monitoring, Healthline and website analytics. For example:

1) Effectiveness of funnel model and information provided at each level
    a. Majority of people sourcing information from Tū Ora website
    b. Smaller number of people accessing information from 0800 number
    c. Smallest number of people needing to gain support via 1737
2) Effectiveness of key messages
    a. Enquiries from key stakeholders are similar in nature e.g. media, health sector organisations/colleges
    b. Enquiries from key stakeholders reduce over time at similar rates
    c. Time taken for discussion on this event to change to lessons learned and maintaining individual and organisational cyber-health and activities required to support this

The feedback will allow us to fine-tune our responses. Effectiveness of our communications will be gauged by presence in public comment (spokespeople commenting); prominence (appropriate to the issues presented) and credibility (health agencies are presented as authoritative).

19. Appendix 1 - Summary of events

- Tū Ora Compass Health has updated its website software and is now back online after its website was targeted as part of a widespread global cyber incident in August in which a number of organisations websites were defaced.
- The 5th August events prompted the PHO (primary health organisation) to take its server offline while it undertook a full review into the event.
- The ‘malware’ was removed and a new server provisioned as well as additional protections put in place
- Since this time Tū Ora has continued forensic investigations into the intrusion, working closely with MoH and CCDHB as well as other central agencies
- A Press Release was issued on 15 August 2019.
- Investigation has shown that unauthorised access to our systems occured over a period of time from July 2016 to February 2019
- Tū Ora hold data for approximately 1 million people while there is no evidence that access to patient data has occurred, we cannot rule out the possibility that some data may have been accessed during this period
- It has been agreed that it is in the best interests of transparency to inform key stakeholders (general practices) and their enrolled populations, namely most people living in the Wellington, Kapiti, Porirua, Wellington, Wairarapa, Horowhenua and Palmerston North regions between 2002 and 2019.
- Tū Ora can have a good level of confidence, that access to wider parts of the Health sector was not possible through this intrusion i.e. sideways movement into another organisation from within the Tū Ora network.
- Restoration of services will be completed by 20th September

Refer also Q&A on website and media release

https://www.compasshealth.org.nz/Cyber-Security-Incident

20. Appendix 2 - Key words and Definitions

The following key words and definitions should be used in any and all communications associated with this communications plan. The list is not exhaustive and may be added to by interested agencies as long as the work and definition are approved through both Tū Ora and Central agencies.

The preferred terms to use are:

- Cyber incident - to describe the event
- Unauthorised or illegal access to health information

Key word	**Meaning**
Infrastructure	The technical systems; network, servers, databases etc that Tū Ora uses to run its information technology systems
Cyber Incident(s)	Preferred term to describe the malicious cyber attack(s) on Tū Ora
Malicious actor/group	A broad term to describe a criminal individual or group who target organisation infrastructure and personal technology devices/systems to gain access for criminal purposes
Malware	A piece of software that a malicious actor has placed on a server or network to help achieve criminal objectives like data theft or installing ransom ware
Unauthorised Intrusion	One of several consequences of the incident or event where a malicious actor gained access to the Tū Ora infrastructure– there was an unauthorised intrusion onto the Tū Ora infrastructure
Unauthorised / illegal access to data/information	Access to data without consent of the custodian of that data or the person who the data belongs to
Primary Health Organisation	An organisation that provides services to a GP network such as data analysis and reporting of a subset of a patients medical record e.g. immunisation data. PHOs may also provide clinical services such as mental health counselling where there is not enough volume for this service to be provided sustainably across all GP practices
Personal health data	This refers to identifiable health data classed as medical in confidence

21. Appendix 3 - Media Release

See media release
https://www.compasshealth.org.nz/News/Media-Releases/Cyber-Security-Incident-Media-Release

22. Appendix 4 - Tū Ora Website Cyber Event proactive Q&As page and open letter

Kia ora,

As a Primary Health Organisation, one of our roles is to collect and analyse data that comes from your medical centre. We do this to improve the care people receive. It helps to ensure people get proactive screening for diseases like cancer and get treatment for conditions like diabetes. This saves lives and helps keep people well.

On 5 August, our website was attacked as part of a global cyber incident. As soon as we became aware, our server was taken offline, we strengthened our I.T. security and started an in-depth investigation. The investigation has found previous cyber attacks dating from 2016 to early March 2019. We don't know the motive behind the attacks. We have laid a formal complaint with Police and they are investigating.

We cannot say for certain whether or not the cyber attacks resulted in any patient information being accessed. Experts say it is likely we will never know. However, we have to assume the worst and that is why we are informing people.
Tū Ora holds data on individuals dating back to 2002, from the greater Wellington, Wairarapa and Manawatu regions. Anyone who was enrolled with a medical centre in that period could potentially be affected.

Tū Ora does not hold your GP notes, these are held by individual medical centres. This means the notes made on consultations you have had with your GP are not at risk of being illegally accessed through this cyber attack. We do not hold the data contained in your patient portal if you have one.

As stewards of people's information, data security is of utmost importance to Tū Ora. While this was an illegal attack by cyber criminals, it was our responsibility to keep your data safe and I am very sorry we have failed to do that.

We are now focused on doing everything we can to support people and making sure it can't happen again. We have set up a number (0800 499 500 or +64 6 9276930 if dialling from overseas) for people to call to obtain more information.

While we have no evidence that patient data was accessed, we encourage you to be vigilant to unusual online requests.

Cert NZ has more information about staying safe online on their website at www.cert.govt.nz . Please read our FAQs below for more information.

Again, I want to apologise for this situation and the distress it will cause.

Ngā mihi,
Martin Hefford
Chief Executive
Tū Ora Compass Health

FAQs

What happened?
Tū Ora Compass Health's website was defaced in August 2019 during a widespread global cyber incident, which exploited a vulnerability first identified in early July. The August attack prompted Tū Ora to take our server offline, strengthen our IT security, and an in-depth investigation by the relevant authorities was started. This included the National Cyber Security Centre, Ministry of Health, Police and other agencies.

What became clear during the investigation was evidence of previous attacks by cyber criminals dating back to 2016.

Despite careful investigation, we cannot say for certain whether or not the cyber-attacks resulted in any individual patient information being accessed. It is likely that we will never know.

Who is Tū Ora Compass Health and why does it collect data?
Tū Ora Compass Health is one of 30 Primary Health Organisations (PHO) in New Zealand. One of the roles of a PHO is to collect and analyse general practice data. Medical centres provide PHOs like Tū Ora Compass Health some limited patient data e.g. details of all those who have had immunisations. The data is analysed by Tū Ora and then given back to the medical centres where it is used to help GP teams to provide high quality care e.g. people to contact who have not had immunisations to encourage them to do so.

The reason we collect this information and provide it back to GPs is to improve the care people receive. Ensuring people get proactive screening for diseases like cancer and get treatment for chronic conditions like diabetes. This helps save lives and keep people well.

Tū Ora also delivers some clinical services such as podiatry, mental health, and diabetes care. Patient information collected as part of delivering these clinical services is contained within the Tū Ora IT systems.

Who is potentially affected by this cyber-attack?
People who have been enrolled with a medical centre in the greater Wellington, Wairarapa and Manawatu regions since 2002.

The current population of these areas are around 648,000 people, but including those now deceased or who have moved away from the area, the data covers nearly 1 million people.

Was patient data accessed illegally?
While we have no evidence that access to patient data has occurred, we cannot rule out the

possibility that some patient data may have been accessed during the cyber-attack.

What patient data is held by Tū Ora?
Tū Ora does not hold your GP notes, these are is held by individual medical centres. This means notes made on consultations you have had with your GP are not at risk. We do not hold the data contained in your patient portal if you have one.

We hold data that includes, who is enrolled at which medical centre, their National Health Index Number, name, date of birth, ethnicity and address.

We also hold some medical information provided by medical centres to us that we analyse and provide back to the medical centres to support timely quality care. For instance, Tū Ora provides GPs and practice nurses with information on:
• Which children are due for immunisation
• Whether people with diabetes are up to date with all the checks and are being treated according to best practice
• Whether people aged over 65 have had a flu vaccination yet
• Who has been admitted to hospital for a potentially avoidable condition
• Which women are due to be recalled for cervical screening
• Who is due for a heart and diabetes check.

As part of delivering clinical services such as podiatry, mental health and diabetes care, Tū Ora also holds some patient information required for those services.

We also hold some organisational financial data for the practices and other health care providers that we work with e.g. invoices and account details, that enable us to pay for services delivered.

The Piki youth mental health programme data is not included in the information potentially illegally accessed.

We do not hold ACC claims data.

Is there any other information you may have on me?
We hold no banking, credit card or financial information for patients. We do not hold any information such as passport numbers, driver license numbers, or, tax numbers. We only hold a part of a medical record for data analysis, reporting and specific service delivery purposes.

Why don't you know whether patient data was accessed?
We do not have Audit logs back to 2016.

What is being done to stop this happening again?
As soon as we found out about the August 2019 cyber-attack, we took the affected server offline. We increased security for our systems and contacted relevant authorities

immediately, who began a thorough investigation.

We're currently moving to a new more modern, and more secure digital platform that is in line with international best practice.

Can you guarantee a cyber-attack won't happen again?
While we are committed to using the best, most up to date security, international experience shows that not even the largest corporations or organisations can guarantee they are immune to criminal activity.

What does this mean for me?
While we have no evidence that patient data was accessed, criminals can use personal data to commit crimes such as identity theft and fraud, by combining the data with information stolen from other sources.

Are people affected by this potentially more susceptible to scams now?
Yes. We are advised that cyber criminals, even if they have no actual information, try to scam people by claiming they have it even when they don't. Unfortunately, if they do have it, then there is also the likelihood of more scams or attempts to use any information they hold to get more or to obtain money.

What action do I need to take?
While we have no evidence that patient data was accessed, we encourage you to be vigilant to unusual online requests; never share your passwords or account details and follow good online security practices.

This means:
• keeping software up to date
• regularly changing passwords and
• ensuring that you have different passwords for different activities for all online activities.

Cert NZ has more information about staying safe online here .

How can I get more information and support?
If you want to know more, please call our support line on 0800 499 500. If you are calling from overseas please use +64 6 9276930.

If you are feeling distressed and need support, please call the 1737 mental health support line. 1737 is free to call and doesn't use up any of your mobile data.

How do I report fraud or cybercrime?
Contact the Police if you believe your identity may have already been used in a fraudulent way cybercrime@police.govt.nz

Did I consent for my data to be collected?
Yes. When you enrolled with your GP, the enrolment form includes a consent item around data collection and use of health information.

How can I opt out of my data being collected by my GP?
At the moment is not possible to opt out of this arrangement due to system limitations. But we are working with the Ministry of Health and other agencies to consider this for the future.

Can I trust that information I share with my GP is safe?
GP patient notes are not held by Tū Ora Compass Health. They have not been affected by this cyber-attack. The primary care summary record system that is used by hospital service providers and by after-hours services, is also not affected by this cyber incident.

Cultural concern
If you have specific cultural concerns around health information, please call the support line on 0800 499 500.

Can I find out what information Tū Ora holds on me?
Not yet. We do not store your information as one health record. Information is collected for specific claiming and reporting purposes and we don't have a process to amalgamate the data yet. We are working on this.

What's happening to make Tū Ora data safer in the future?
Tū Ora has already moved its public websites to a new platform, and has strengthened its security measures by:

1) Enhancing its anti-virus and email scanning software
2) Implementing Security Incident and Event Management (SIEM) system
3) Implementing a Web Application Firewall (WAF)
4) Established a Security Operations Centre (SOC) for real time monitoring and resolution of cyber threats

We are also part way through a planned movement to more modern more secure infrastructure using Microsoft Azure. The new Tū Ora Microsoft Azure environment will be fully secured, with a defence in depth approach to protecting all our electronic assets. Microsoft Azure itself is fully compliant with the international ISO 27001 cyber security standard.

Tū Ora will also be using the Advanced Threat Protection features available from our investment in the Microsoft 365 suite of products, including device and application protection, data loss protection and full data encryption.

We expect to have completely moved to the new platform by April 2020.

What about Research Data?
Tū Ora holds data relating to ethics approved research studies conducted with academic institutions. Some of this research includes some notes from some GP consultations from some medical centres for some people. Recent research project topics have included: Influenza like illness prevalence, child health, and osteoarthritis prevalence.

23. Appendix 5 - General public questions and 0800 script

Call centre scripts to be developed by incident response team based on information on https://www.compasshealth.org.nz/Cyber-Security-Incident

.

Open letter publsihed in Dominino Post and Wairarapa Times age as below.

24. Appendix 6 - Emergency Plan For Unscheduled Release

Assumption

If an unplanned release occurs the likely initial contact point for the enquiry will be either Tū Ora , Think Hauora or the Ministry of Health. An enquiry may be made to a GP practice but the GP practice will likely refer to Tū Ora or the Ministry of Health or Think Hauora.This organisation becomes the initial point of contact.

Process

The following steps will be followed regardless of the point of entry of the initial contact. The person taking the enquiry must:

1) Take the name, contact number, organisation and email of the person making the enquiry
2) Specifically enquire if they are from a media organisations and take the name of the media/publishing organisation
3) Detail the enquiry and specific questions
4) Thank the person and advise that they will be contacted again as soon as practicable with advice
5) Do not answer any questions at this point, advise that you will get 'the right information from the right people'
6) Advise the communications manager of the organisation where the enquiry is benig made
7) The communications manager of the organisation taking the call will advise the Ministry Incident manager first and then their relevant CEO
8) The CEO of the organisation taking the call will advise the Director General of Health
9) The communications manager of the organisation taking the call will contact the communications managers from:
    a. Ministry of Health
    b. Tū Ora
    c. Capital and Coast District Health Board
    d. Think Hauora PHO
    e. Mid Central District Health Board
10) The communications managers from the organisations below wil all advise their CEOs and CIOs
    a. Ministry of Health
    b. Tū Ora
    c. Capital and Coast District Health Board
    d. Think Hauora PHO
    e. Mid Central District Health Board
11) The CEOs of all the organisations involved will advise the Chair of their Boards
12) The Chairs of the Boards will advise the rest of the Board members

13) The Ministry Incident manager will assemble the ‘response room’ at the Ministry of health
14) The media response in this appendix will be reviewed by the Tū Ora and Ministry of Health communications managers against the original enquiry, be adjusted if need be and be provided to the original caller as soon as practicable, with any other details as necessary
15) The Ministry incident manager will initiate and manage the planned release process

Key Message

Attribute: Martin Hefford
Chief Executive
Tū Ora Compass Health

Recently we were made aware of unauthorised access to our I.T systems. At this stage we are working with the necessary authorities to understand the full extent of the intrusion.

We will provide a public update shortly.

END
Media contact:
s 9(2)(a)
Communications Advisor
Tū Ora Compass Health
www.compasshealth.org.nz
s 9(2)(a)
s 9(2)(a)

25. Appendix 7 - Draft Communication to Practices

Cyber intrusion update:
Date xxx

Dear Colleagues,

Tū Ora Compass Health: Further evidence of unauthorised cyber access investigated..

As previously notified to you, Tū Ora Compass Health's website was defaced during a widespread global cyber incident in August. The August attack prompted the Wellington-based primary health organisation (PHO) to take its server offline and initiate a thorough systems review.

What has become clear during the subsequent investigation is evidence of prior unauthorized intrusions to our I.T systems dating back to 2016."

Despite careful investigation, we cannot say for certain whether the unauthorised access resulted in any individual information being taken. This means data may have been accessed for up to an estimated 1 million people and could cover data held by the PHO dating back to 2002 for people in the Wellington, Wairarapa and Manawatu regions.

We are sorry for any uncertainty this may cause for our practice teams and people in these regions. We're also apologise for the time it took to detect these criminal attacks to our IT systems.

Tū Ora takes full responsibility for what has happened. As stewards of people's personal health information, data security is of utmost importance to Tū Ora Compass Health and it was our job to keep that information safe at all times. We apologise to all of the people concerned for our failure to do that.

We're doing everything we can to find out what has happened, and we are working with the appropriate authorities to try and find out. We acted immediately to take our systems offline and have significantly strengthened security for our I.T systems.

Our focus now is to provide support to you, our network and the public.

Tū Ora has put support services in place for those people concerned or wanting more information about this issue. (Link)

Response process:
Practice staff are not expected to manage public response, but we are aware there may be some public queries via practices.

We will be holding a joint Press conference with the Ministry of Health and (Security agency name) at (date/time) tomorrow morning. We'll also be publishing a Press Release (date) to inform those enrolled populations living in the Wellington, Wairarapa and Manawatu regions. We have also set up an information webpage and an 0800 helpline for any members of the public who need more information and support. The 1737 line is also available for any people who may feel distressed and require more support.

While we will not be publicising, for any patients distressed and needing a GP visit, we have arranged a free visit which can be claimed to us. (insert details by link?)

We have been working closely with the Ministry of Health and Security agencies who will be supporting this issue with a wider sector response around cyber security assurances.

To support any member of the public easily access the right information, please:

- direct any patient queries directly to our support webpage (insert URL) which will be live (date time)
- 0800 helpline details are also listed on the webpage
- 1737 is also available for people in distress
- any media query can be directly referred to our communications advisor by phone or email - details below.
- to make directing queries easier, we've attached a response prompt to remind practice and partner organisation reception staff where to direct queries on this matter.

For more information and support on this incident, please see our website FAQs below or contact your Tū Ora Compass Health practice relationship manager.

CERT NZ suggests the following simple and practical tips to help keep people safe online.

Sig
Martin Hefford
Chief Executive

END

Media contact:
s 9(2)(a)
Communications Advisor
Tū Ora Compass Health
s 9(2)(a)
s 9(2)(a)

Tū Ora Website Cyber Event Q&A information

INSERT PUBLIC FAQS HERE - APPENDIX 4

Reminder comms for practice reception staff or partner organisational staff (PHOs) on where to direct enquiries?

Reminder – Where should I direct calls/enquiries about the Tū Ora cyber intrusions?

Type of Query	**Where to direct query**
Practice or organisation wanting more information?	Tū Ora practice relationship manager Organisations can contact xyz
Patient wanting more information?	FAQ support www.compasshealth.org.nz
Patient needing more information after reading FAQs?	Will be prompted to call 0800 helpline from the FAQs webpage 0800 xyz
Patient not satisfied with 0800 helpline responses	0800 team will contact Tū Ora who will triage query and contact patient to direct in the correct way i.e 1737 or complaint
Patient wanting information on medical records?	Speak to practice or check patient portal
Media enquiry?	Direct to Communications advisors 9(2) [redacted]

26. Appendix 8 - Draft Communications to Te Awakairangi, Cosine and Ora Toa PHOs

Dear Colleagues,

Cyber intrusion update:
Date xxx

As you are aware, the Tū Ora Compass Health website was defaced during a widespread global cyber incident in August. The August attack prompted the Wellington-based primary health organisation (PHO) to take its server offline and initiate a thorough systems review.

What has become clear during the investigation is evidence of prior unauthorised intrusions to our I.T systems dating back to 2016.

Despite careful investigation, we cannot say for certain whether the unauthorised access resulted in any individual information being taken. This means data may have been accessed for up to an estimated 1 million people and could cover data held by the PHO dating back to 2002 for people in the Wellington, Wairarapa and Manawatu regions.

We are sorry for any uncertainty this may cause for to you our PHO partners, practice teams and people in these regions. We're also apologise for the time it took to detect these criminal attacks to our IT systems.

Tū Ora takes full responsibility for what has happened. As stewards of people's personal health information, data security is of utmost importance to Tū Ora Compass Health and it was our job to keep that information safe at all times. We apologise to all of the people concerned for our failure to do that.

We're doing everything we can to find out what has happened, and we are working with the appropriate authorities to try and find out. We acted immediately to take our systems offline and have significantly strengthened security for our I.T systems.

Our focus now is to provide support to you, our network and the public.

We have been working closely with the Ministry of Health and Security agencies who will be supporting this issue with a wider sector response around cyber security assurances.

Tū Ora has put support services in place for those people concerned or wanting more information about this issue. (Link)

Response process:

Practice staff are not expected to manage public response, but we are aware there may be some public queries via practices and we have put support packs in place to assist this process.

We will be holding a joint Press conference with the Ministry of Health and (Security agency name) at (date/time) tomorrow morning. We'll also be publishing a Press Release (date) to inform those enrolled populations living in the Wellington, Wairarapa and Manawatu regions.

We have also set up an information webpage and an 0800 helpline for any members of the public who need more information and support. The 1737 line is also available for any people who may feel distressed and require more support.

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

To support any member of the public easily access the right information, please:

- direct any patient queries directly to our support webpage (insert URL) which will be live (date time)
- 0800 helpline details are also listed on the webpage
- 1737 is also available for people in distress
- any media query can be directly referred to our communications advisor by phone or email - details below.
- to make directing queries easier, we've attached a response prompt to remind practice and partner organisation reception staff where to direct queries on this matter.

For more information and support on this incident, please see our website FAQs below.

CERT NZ suggests the following simple and practical tips to help keep people safe online.

Sig
Martin Hefford
Chief Executive

END

Reminder comms for practice reception staff or partner organisational staff (PHOs) on where to direct enquiries?

Reminder – Where should I direct calls/enquiries about the Tū Ora cyber intrusions?

Type of Query	**Where to direct query**
Practice or organisation wanting more information?	Tū Ora practice relationship manager Organisations can contact xyz
Patient wanting more information?	FAQ support www.compasshealth.org.nz

Patient needing more information after reading FAQs?	Will be prompted to call 0800 helpline from the FAQs webpage 0800 xyz
Patient not satisfied with 0800 helpline responses	0800 team will contact Tū Ora who will triage query and contact patient to direct in the correct way i.e 1737 or complaint
Patient wanting information on medical records?	Speak to practice or check patient portal
Media enquiry?	Direct to Communications advisor s 9(2) [redacted]

Tū Ora Website Cyber Event Q&A information

INSERT PUBLIC FAQS HERE - APPENDIX 4

27. Appendix 10 - Communication to GPNZ CE and Chair and RNZCGP, N4 CEs, Other PHOs – Brief Summary

- PHOs like Tu Ora hold a small subset of your personal health data, your GP practice asks us to collect this from your medical record in order to do analysis and reporting for quality improvement purposes for them
    - The sort of data we hold can vary but is simple things like immunisation history, smoking history and if you have any conditions like diabetes
- We had a website hack on 5th August and our investigation has shown that there were intrusions to our systems prior to this going back to 2016
- It is possible that the patient data that we hold may have been accessed during these prior intrusions though we have no evidence that this was the case
- We take this seriously and we apologise for any distress this may cause to the public
- We removed the 'malware' and have significantly strengthened the security of our system and security
- Our website has more information and there are also details on an 0800 number that people can call if they want more information
- Importnatly your medical record at your GP practice has not been affected by this and your GP practice was not the cause of this situation
- The best thing you can do now is to:
    - Read the 11 top tips for staying safe on liine from NZ CERT
    - Be aware that scammers take advantage of news like this. You'll need to be wary of any unsolicited or suspicious emails with links in them or phone calls that:
        - Try to sell you health products based on any conditions that you have
        - Suggest that someone has your health information and that you should pay them money to stop them releasing it
        - May be subject to scamming as a result of this disclosure

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

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

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

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

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

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