

# Situation Report #2

## Data Breach

*Confidential and not for further distribution*

<b>Date:</b> 1 December 2023	<b>Time:</b> 18.00pm
<b>Event Name:</b> Data Breach	<b>Prepared by:</b> S9(2)(a)
<b>Incident Controller/SRO:</b> Sue Gordon	<b>Contact Details:</b> S 9(2)(a)

### Background

This Situation Report (SitRep) provides an update on our response to an employee using and commenting on data publicly, including an email to a wide range of MPs. The employee has also made public a video with S6(c). The employee is alleging that COVID vaccinations have been responsible for a large number of deaths; the assertions are not correct and have no scientific validity.

We are closely monitoring this situation and will keep in close contact with the Minister’s Office throughout the weekend. An update will also be provided in our officials meeting on Monday at 9.00am. We are running this as an incident management response. There are a number of workstreams currently underway.

### Workstreams

Function	Update	Next steps
Communications	<p><b>As at 1700 Monitoring Social Media and news media.</b></p> <p>Public: Our proactive media statement, released on Friday at 2.00pm, is attached and provides information on our response to, and management of, the incident. Margie Apa is the overall spokesperson and will be supported by S9(2)(a) for public health messaging. We will continue to provide support and liaison to the Minister’s Office as required</p> <p>Internal: We have met with the employee’s team to advise them of the situation at a high level, and offered appropriate support.</p>	<p><b>Update by exception. Provide reactive statements as required.</b></p> <p>Margie Apa will be appearing on One News and RNZ Checkpoint today. The media team will field media queries over the weekend and will keep the Minister’s Office informed.</p> <p>We are not intending any further internal communications at this stage</p>
Employment matters	<p>S9(2)(a)</p> <p>S9(2)(a)</p>	<p>S9(2)(a)</p>

	<p>S9(2)(a)</p> <p>[Redacted]</p>	
<p>Information security</p>	<p>We have sought and expect to receive late Friday an injunction against use and/or sharing of the information (and returning all information, materials and equipment) from the Employment Relations Authority. This covers the employee and also includes a wider prohibition on use and sharing of the information by other parties (such as media outlets). This now provides a basis to legally enforce the injunction if information is used or shared.</p> <p>The Cyber IMT was activated in support of this event.</p> <p>There are three workstreams of activity:</p> <p>S6(c)</p> <p>[Redacted]</p>	<p>Injunction proceedings underway as at 1700. Indications are most requests are likely to be approved.</p> <p>Once the injunction is granted, we will enforce it as appropriate</p> <p>All employee access blocked.</p> <p>Forensic investigator engaged to assist data and digital investigation.</p> <p>S6(c)</p> <p>[Redacted]</p>
<p>Privacy</p>	<p>Given peoples' personal information is involved – both the threat to release information and inappropriate use by employee – we have registered this incident as a privacy breach with the Office of the Privacy Commissioner.</p>	<p>Our protocols for managing and responding to privacy breaches, including related to information security, will be followed.</p>
<p>Key stakeholders</p>	<p>S6(d)</p> <p>[Redacted]</p>	<p>S6(d)</p> <p>[Redacted]</p>

	<p>S6(d) [Redacted]</p> <p>[Redacted]</p>	<p>S6(d) [Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>[Redacted]</p> <p>Debrief from engagements at 4.00pm</p>
--	---	---

**Next steps**

The next response briefing is planned for 1100 2 December 2023. Te Whatu Ora will provide an update no later 1500 02 December 2023.

# Situation Report #2

## Data Breach

*Confidential and not for further distribution*

<b>Date:</b> 1 December 2023		<b>Time:</b> <b>18.00pm</b>
<b>Event Name:</b> Data Breach	<b>Prepared by:</b> S9(2)(a)	
<b>Incident Controller/SRO:</b> Sue Gordon	<b>Contact Details:</b> S 9(2)(a)	

### Background

This Situation Report (SitRep) provides an update on our response to an employee taking data without authorisation and using it to spread misinformation on excess deaths from COVID19 vaccination. This includes email to a wide range of MPs. The employee has also made public a video available online. The employee is alleging that COVID vaccinations have been responsible for a large number of deaths; the assertions are not correct and have no scientific validity. **Red is update from Sitrep #1.**

### Workstreams

Function	Update	Next steps
Communications	<p><b>As at 1700 Monitoring Social Media and news media.</b></p> <p>Public: Our proactive media statement, released on Friday at 2.00pm, is attached and provides information on our response to, and management of, the incident. Margie Apa is the overall spokesperson and will be supported by S9(2)(a) for public health messaging. We will continue to provide support and liaison to the Minister's Office as required</p> <p>Internal: We have met with the employee's team to advise them of the situation at a high level, and offered appropriate support.</p>	<p><b>Update by exception. Provide reactive statements as required.</b></p> <p>CEO did 3 media interviews - One News, RNZ Checkpoint and Mediawatch. The media team will field media queries over the weekend.</p> <p>We are not intending any further internal communications at this stage</p>
Employment matters	<p>S9(2)(a)</p> <p>From Thursday 30 November S9(2)(a)</p>	
Information security	<p>We have sought and expect to receive late Friday an injunction against use and/or sharing of the information (and returning all information, materials and equipment)</p>	<p><b>Injunction proceedings endorsed by ERA as at 1700.</b></p>

	<p>from the Employment Relations Authority. This covers the employee and also includes a wider prohibition on use and sharing of the information by other parties (such as media outlets). This now provides a basis to legally enforce the injunction if information is used or shared.</p> <p>The Cyber Incident Management Team is activated. There are three workstreams of activity:</p> <p>S6(c)</p>	<p>Forensic investigator engaged to assist data and digital investigation on data that may have been extracted without authorisation.</p> <p>S6(c)</p>
<p>Privacy</p>	<p>Given peoples' personal information is involved – both the threat to release information and inappropriate use by employee – we have registered this incident as a privacy breach with the Office of the Privacy Commissioner.</p>	<p>Our protocols for managing and responding to privacy breaches activated.</p>
<p>Key stakeholders</p>	<p>S6(d)</p>	<p>S6(d)</p> <p>Debrief from engagements at 4.00pm</p>







































Next steps

The next response briefing is planned for 1100 2 December 2023. Te Whatu Ora will provide an update no later 1500 02 December 2023.

S6(d)





	<p>from the Employment Relations Authority. This covers the employee and also includes a wider prohibition on use and sharing of the information by other parties (such as media outlets). This now provides a basis to legally enforce the injunction if information is used or shared.</p> <p>The Cyber Incident Management Team is activated. There are three workstreams of activity:</p> <p>S6(c)</p> 	<p>Forensic investigator engaged to assist data and digital investigation on data that may have been extracted without authorisation.</p> <p>S6(c)</p>   
<p>Privacy</p>	<p>Given peoples' personal information is involved – both the threat to release information and inappropriate use by employee – we have registered this incident as a privacy breach with the Office of the Privacy Commissioner.</p>	<p>Our protocols for managing and responding to privacy breaches activated.</p>
<p>Key stakeholders</p>	<p>S6(d)</p>                	<p>S6(d)</p>                   <p>Debrief from engagements at 4.00pm</p>

Next steps

The next response briefing is planned for 1100 2 December 2023. Te Whatu Ora will provide an update no later 1500 02 December 2023.

S6(d)



# Situation Report #3

## Data Breach

*Confidential and not for further distribution*

<b>Date:</b> 02 December 2023	<b>Time:</b> 1700hrs
<b>Event Name:</b> Data Breach	<b>Approved by:</b> S9(2)(a)
<b>Incident Controller/SRO:</b> Sue Gordon	<b>Contact Details:</b> S 9(2)(a)

### Background

This Situation Report (SitRep) provides an update on the health system response to an employee (referred to as POI) taking data without authorisation and using it to spread misinformation on excess deaths from COVID19 vaccination. This includes email to a wide range of MPs. The POI has also made public a video available online. The POI is alleging that COVID vaccinations have been responsible for many deaths; the assertions are not correct and have no scientific validity. Red is update from Sitrep #1.

### Workstreams

Function	Update	Next steps
Communications	<p>A proactive media statement, released on 01 December at 1400hrs, provided information on Te Whatu Ora’s response to, and management of, the incident.</p> <p>Margie Apa is the organisational spokesperson and will be supported by Andrew Old for public health messaging.</p> <p>On 01 December 2023, Margie Apa completed 3 media interviews. The media team will field media queries over the weekend.</p>	<p>News and social media continue to be monitored for any emerging issues or heightened interest.</p> <p>Ongoing development of a proactive media release over the next 24hrs (as situation develops).</p> <p>Support and liaison to the Minister’s Office will continue to be provided as required.</p>
Employment matters	<p>S9(2)(a)</p> <p>S9(2)(a)</p> <p>S6(c)</p> <p>Injunctions to prohibit use or sharing of information, return information and equipment and to delete information were served by email as of 01</p>	<p>S9(2)(a)</p> <p>S6(c)</p> <p>S9(2)(a)</p>





S6(d)



S6(d)



S6(d)



# Situation Report #4

## Data Breach

*Confidential and not for further distribution*

<b>Date:</b> 03 December 2023		<b>Time:</b> 1330hrs
<b>Event Name:</b> Data Breach	<b>Approved by:</b> S9(2)(a)	
<b>Incident Controller/SRO:</b> Sue Gordon	<b>Contact Details:</b> S 9(2)(a)	

### Background

This Situation Report (SitRep) provides an update on the health system response to an employee (referred to as POI) taking data without authorisation and using it to spread misinformation on excess deaths from COVID19 vaccination. This includes email to a wide range of MPs. The POI has also made public a video available online. The POI is alleging that COVID vaccinations have been responsible for many deaths; the assertions are not correct and have no scientific validity. Red is update from Sitrep #1.

### Workstreams

Function	Update	Next steps
Communications	<p>***Press release update to come***, this includes an update on where Te Whatu Ora are on their response to the POIs actions, as well as clear reassurance regarding the use of vaccines.</p>	<p>News and social media continue to be monitored for any emerging issues or heightened interest. As of 1200hrs 03 December, there has been no noticeable increase in anti-vaccination rhetoric linked to this breach.</p> <p>Support and liaison to the Minister's Office will continue to be provided as required.</p>
Employment matters	<p>The Person of Interest</p> <ul style="list-style-type: none"> <li>S9(2)(a)</li> <li>All external access to systems and processes has been removed. S9(2)(a)</li> <li>Physical and emailed injunction have been served (as of 02 December 2023).</li> <li>S6(c)</li> </ul>	<p>S9(2)(h)</p> <p>S9(2)(h)</p> <p>S6(c)</p>

	<p>S6(c)</p> <p>[Redacted]</p> <ul style="list-style-type: none"> <li>As of 02 December, People and Capability are liaising with Simpson and Grierson to ensure all legal options are explored.</li> <li>S6(c)</li> </ul> <p>S9(2)(a)</p> <ul style="list-style-type: none"> <li>[Redacted]</li> <li>[Redacted]</li> </ul> <p>Wider Data Sharing</p> <ul style="list-style-type: none"> <li>Injunctions to prohibit use or sharing of information, return information and equipment and to delete information were served by email as of 01 December evening. It covers the POI, S6(c), and any other parties with access to or involved in accessing and releasing data.</li> <li>S6(c)</li> </ul>	<p>S6(c)</p> <p>[Redacted]</p>
<p>Information security</p>	<p>The Cyber Incident Management Team is activated. There are three workstreams of activity:</p> <p>S6(c)</p> <p>[Redacted]</p>	<p>Forensic investigator engaged to assist data and digital investigation on data that may have been extracted without authorisation.</p> <p>S6(c)</p> <p>[Redacted]</p> <p>S6(c)</p> <p>[Redacted]</p> <p>S6(c)</p> <p>[Redacted]</p>



Key stakeholders	S6(d) [Redacted]	S6(d) [Redacted] S6(c) [Redacted]

S6(d)



# Situation Report #4

## Data Breach




*Confidential and not for further distribution*

<b>Date:</b> 03 December 2023	<b>Time:</b> 1700hrs
<b>Event Name:</b> Data Breach	<b>Approved by:</b> S9(2)(a)
<b>Incident Controller/SRO:</b> Sue Gordon	<b>Contact Details:</b> S9(2)(a)

### Background

This Situation Report (SitRep) provides an update on the health system response to an employee (referred to as POI) taking data without authorisation and using it to spread misinformation on excess deaths from COVID19 vaccination. This includes email to a wide range of MPs. The POI has also made public a video available online. The POI is alleging that COVID vaccinations have been responsible for many deaths; the assertions are not correct and have no scientific validity. Red is update from Sitrep #1.

### Workstreams

Function	Update	Next steps
Communications	<p>Proactive press release PM 03 December 24, this includes an update on where Te Whatu Ora are on their response to the POIs actions, as well as clear reassurance regarding the use of vaccines.</p>	<p>News and social media continue to be monitored for any emerging issues or heightened interest. As of 1200hrs 03 December, there has been no noticeable increase in anti-vaccination rhetoric linked to this breach.</p> <p>Support and liaison to the Minister's Office will continue to be provided as required.</p> <p>Notably:</p> <p>S6(c)</p> 
Employment matters	<p>The Person of Interest</p> <ul style="list-style-type: none"><li>S9(2)(a), S6(c)</li></ul> 	<p>S9(2)(h)</p> 

	<p>S9(2)(a), S6(c) [redacted]</p> <ul style="list-style-type: none"> <li>• S9(2)(a) [redacted]</li> <li>• All external access to systems and processes has been removed. S9(2)(a) [redacted]</li> <li>• Physical and emailed injunction have been served (as of 02 December 2023).</li> <li>• S6(c) [redacted] <ul style="list-style-type: none"> <li>■ [redacted]</li> </ul> </li> <li>• As of 02 December, People and Capability are liaising with Simpson and Grierson to ensure all legal options are explored.</li> <li>• S6(c) [redacted] <ul style="list-style-type: none"> <li>■ [redacted]</li> </ul> </li> </ul> <p>S9(2)(a) [redacted]</p> <ul style="list-style-type: none"> <li>■ [redacted]</li> <li>■ [redacted]</li> </ul> <p>Wider Data Sharing</p> <ul style="list-style-type: none"> <li>• Injunctions to prohibit use or sharing of information, return information and equipment and to delete information were served by email as of 01 December evening. It covers the POI, S6(c) [redacted], and any other parties with access to or involved in accessing and releasing data.</li> <li>• S6(c) [redacted]</li> </ul>	<p>Take-down orders will continue to be issued to any sites that publish the data or information taken from HNZ servers.</p> <p>S6(c) [redacted]</p>
Information security	The Cyber Incident Management Team is activated. There are three workstreams of activity:	Forensic investigator engaged to assist data and digital investigation

S6(c)



on data that may have been extracted without authorisation.

S6(c) [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

S6(c) [Redacted]  
[Redacted]  
[Redacted]

S6(c) [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

- | [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

- | [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

- | [Redacted]  
[Redacted]

S6(c) [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

Privacy

S6(c)



	<p>S6(c) [redacted] [redacted] [redacted]</p> <p>S9(2)(ba)(i) [redacted] [redacted]</p> <p>[redacted]</p> <p>Protocols for managing and responding to privacy breaches activated.</p>	<p>- S9(2)(h) [redacted] [redacted] [redacted]</p> <p>Remains risk of data re-emerging internationally given it was able to be downloaded.</p> <p>Although papers have been served via email, as of 1200hrs 03 December, S6(c), S9(2)(a) [redacted] [redacted] [redacted]</p>
Key stakeholders	<p>S6(d) [redacted] [redacted] [redacted] [redacted] [redacted]</p> <p>[redacted] [redacted] [redacted]</p> <p>[redacted] [redacted]</p>	<p>S6(d) [redacted] [redacted] [redacted] [redacted]</p> <p>[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]</p> <p>S6(c) [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]</p>

S6(d)



# Situation Report #5

## Data Breach

*Confidential and not for further distribution*

<b>Date:</b> 04 December 2023	<b>Time:</b> 1700hrs
<b>Event Name:</b> Data Breach	<b>Approved by:</b> S9(2)(a)
<b>Incident Controller/SRO:</b> S9(2)(a)	<b>Contact Details:</b> S9(2)(a)

### Background

This Situation Report (SitRep) provides an update on the health system response to an employee (referred to as POI) taking data without authorisation and using it to spread misinformation on excess deaths from COVID19 vaccination. This includes email to a wide range of MPs. The POI has also made public a video available online. The POI is alleging that COVID vaccinations have been responsible for many deaths; the assertions are not correct and have no scientific validity. Red is update from Sitrep #1.

### Workstreams

Function	Update	Next steps
Communications	<p><b>Te Whatu Ora Chief Executive is due to complete further interviews 04 December. The Ministers office is aware.</b></p>	<p><b>Communications team continue to monitor the POIs court appearance today, as well as any resulting discourse surrounding these proceeds.</b></p>
Employment matters	<p>The Person of Interest S6(c), S9(2)(a)</p> <p>Wider Data Sharing</p> <ul style="list-style-type: none"><li>• Injunctions to prohibit use or sharing of information by any other parties with access to or involved in accessing and releasing data continue to be utilised.</li><li>• A decision has been made not to serve injunction to conspiracy groups sharing this information online, as there were concerns this would encourage the spread of this inaccurate narrative.</li></ul> <p>S9(2)(a), S6(c)</p>	<p>S9(2)(a), S6(c)</p> <p>S6(c)</p> <p>S9(2)(a)</p>

	<p>S9(2)(a) [redacted]  [redacted]  [redacted]</p>	<p>S9(2)(a), S9(2)(h) [redacted]</p>
<p>Information security</p>	<p>S6(c) [redacted]</p>	<p>Data and Digital have initiated work regarding future protections and improvements, looking at measures to prevent or mitigate future risks.</p> <p>S6(c) [redacted]</p>
<p>Privacy</p>	<p>S9(2)(a), S6(c) [redacted]</p>	
<p>Key stakeholders</p>	<p>S6(d) [redacted]  [redacted]  [redacted]</p>	<p>S6(d) [redacted]  [redacted]</p>

	S6(d)	S6(d)
		S6(d)
		S6(c)

S6(d)



## Cyber IMT Situation Report – IN-CONFIDENCE

*New information in red text*

Incident Name: <b>Data Breach</b>		Controller: S9(2)(a)	
		Technical Lead: S9(2)(a)	
		<b>Privacy Lead: Viv Kerr</b>	
Date: 01 Dec 2023	Time: <b>1400 hrs</b>	SitRep No: 1	Response Day: 1
Prepared by: S9(2)(a)		Ph.: S9(2)(a)	
Approved by: S9(2)(a)		Ph.: S9(2)(a)	
Situation Report circulated to: Leigh Donoghue, Michael Dreyer, Andrew Slater, Sonny Taite, Sue Gordon, Viv Kerr, S9(2)(a)			
Response Objectives (Mission):			
<ul style="list-style-type: none"> <li>To support the National Health Coordination Centre in managing the ongoing <b>Data Breach</b></li> <li>S6(c)</li> </ul>			

### KEY UPDATES TODAY

- The **Cyber IMT** was activated to coordinate **Data & Digital** activity in support of the **National Health Coordination Centre**

S6(c)

### INVESTIGATION CONTEXT

- On **30 Nov 2023**, a video was posted on the **New Zealand Loyal** site (and multiple other sites) containing evidence of a significant data breach concerning **Covid-19** vaccination records and mortality data. Emails were sent to **Te Whatu Ora & Te Aka Whai Ora** leadership, as well as **New Zealand Members of Government** notifying them of the video on **30 Nov**.
- An investigation was launched by the **Cyber Security Incident Response** team on **30 Nov**. The **Cyber Incident Management Team** was partially activated on **30 Nov**.

S6(c)

### FUNCTIONAL AREA UPDATE

#### RESPONSE MANAGER

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

<i>Situation Context</i>	<ul style="list-style-type: none"> <li>• The Cyber Incident Management Team was activated on 30 Nov</li> <li>• The Cyber Controller on standby to support the National Health Coordination Centre to maintain alignment and share updates from the lead team</li> </ul>
<i>Actions taken:</i>	<ul style="list-style-type: none"> <li>• Activated Cyber IMT</li> </ul>
<i>Actions to be completed:</i>	<ul style="list-style-type: none"> <li>• Cadence of operations between IMT and CSIRT being established</li> <li>• Weekend roster being established</li> </ul>
<i>Outstanding issue(s) requiring decisions:</i>	<ul style="list-style-type: none"> <li>• No current issues</li> </ul>



<i>Actions to be completed:</i>	<ul style="list-style-type: none"> <li>•</li> </ul>
<i>Outstanding issue(s) requiring decisions:</i>	<ul style="list-style-type: none"> <li>•</li> </ul>
<b>COMMS</b>	
<i>Situation Context</i>	<ul style="list-style-type: none"> <li>• National Comms are leading the communications</li> <li>•</li> </ul>
<i>Actions taken:</i>	<ul style="list-style-type: none"> <li>• D&amp;D Function on Standby</li> </ul>
<i>Actions to be completed:</i>	<ul style="list-style-type: none"> <li>•</li> </ul>
<i>Outstanding issue(s) requiring decisions:</i>	
<b>OPERATIONS</b>	

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

S6(c)



**PLANNING / PRIVACY / LEGAL**

<i>Situation Context</i>	The Controller is engaging with Privacy and Legal teams to provide any intel or support as required.
<i>Actions taken:</i>	<ul style="list-style-type: none"><li>• Confirmed any support required from Cyber IMT</li><li>• Confirmed key contacts and team members to work with</li><li>• Established meetings</li><li>• Agreed tracking of staff briefed into this event</li></ul>
<i>Actions to be completed:</i>	<ul style="list-style-type: none"><li>• An initial set of questions from privacy has been logged for review with the team, these questions will prepare us for any discussions with OPC</li></ul>
<i>Outstanding issue(s) requiring decisions:</i>	<ul style="list-style-type: none"><li>•</li></ul>

**LOGISTICS AND WELFARE**

<i>Situation Context</i>	<ul style="list-style-type: none"><li>• Remaining mindful of any staffing requirements and welfare concerns</li></ul>
--------------------------	---

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

Actions taken:	<ul style="list-style-type: none"> <li>S6(c) [REDACTED]</li> </ul>
Actions to be completed:	<ul style="list-style-type: none"> <li></li> </ul>
Outstanding issue(s) requiring decisions:	
<b>RECOVERY</b>	
Situation Context	
Actions taken:	<ul style="list-style-type: none"> <li>Function on Standby</li> </ul>
Actions to be completed:	<ul style="list-style-type: none"> <li></li> </ul>
Outstanding issue(s) requiring decisions:	

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

## Cyber IMT Situation Report – IN-CONFIDENCE

*New information in red text*

Incident Name: Data Breach		Controller: S9(2)(a)	
		Technical Lead: S9(2)(a)	
		Privacy Lead: Viv Kerr	
Date: 02 Dec 2023	Time: 1000 hrs	SitRep No: 2	Response Day: 3
Prepared by: S9(2)(a)		Ph.: S9(2)(a)	
Approved by: S9(2)(a)		Ph.: S9(2)(a)	
Situation Report circulated to: Leigh Donoghue, Michael Dreyer, Andrew Slater, Sonny Taite, Sue Gordon, Viv Kerr			
Response Objectives (Mission):			
<ul style="list-style-type: none"> <li>To support the National Health Coordination Centre in managing the ongoing Data Breach</li> <li>S6(c)</li> </ul>			

### KEY UPDATES TODAY

- The Cyber IMT was activated to coordinate Data & Digital activity in support of the National Health Coordination Centre

S6(c)

S6(c)

### INVESTIGATION CONTEXT

- On 30 Nov 2023, a video was posted on the New Zealand Loyal site (and multiple other sites) containing evidence of a significant data breach concerning Covid-19 vaccination records and mortality data. Emails were sent to Te Whatu Ora & Te Aka Whai Ora leadership, as well as New Zealand Members of Government notifying them of the video on 30 Nov.

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

S6(c)

- The Data Breach videos have been shared with parties in New Zealand and internationally. Additional videos and presentations are being shared publicly. S6(c)

## FUNCTIONAL AREA UPDATE

### RESPONSE MANAGER

<i>Situation Context</i>	<ul style="list-style-type: none"><li>• The Cyber Incident Management Team was activated on 30 Nov</li><li>• The Cyber Controller on standby to support the National Health Coordination Centre to maintain alignment and share updates from the lead team</li></ul>
<i>Actions taken:</i>	<ul style="list-style-type: none"><li>• Activated Cyber IMT</li><li>• Cadence of operations between IMT and CSIRT being established</li><li>• Weekend roster being established</li><li>•</li></ul>
<i>Actions to be completed:</i>	<ul style="list-style-type: none"><li>•</li></ul>
<i>Outstanding issue(s) requiring decisions:</i>	<ul style="list-style-type: none"><li>• No current issues</li></ul>

S6(c)

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

S6(c)



**COMMS**

<b>COMMS</b>	
<i>Situation Context</i>	<ul style="list-style-type: none"><li>• National Comms are leading the communications</li><li>•</li></ul>
<i>Actions taken:</i>	<ul style="list-style-type: none"><li>• D&amp;D Function on Standby</li></ul>
<i>Actions to be completed:</i>	<ul style="list-style-type: none"><li>•</li></ul>
<i>Outstanding issue(s) requiring decisions:</i>	

S6(c)



*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

<i>Outstanding issue(s) requiring decisions:</i>	•
<b>PLANNING / PRIVACY / LEGAL</b>	
<i>Situation Context</i>	<ul style="list-style-type: none"> <li>• The Controller is engaging with Privacy and Legal teams to provide any intel or support as required.</li> </ul>
<i>Actions taken:</i>	<ul style="list-style-type: none"> <li>• Confirmed any support required from Cyber IMT</li> <li>• Confirmed key contacts and team members to work with</li> <li>• Established meetings</li> <li>• Agreed tracking of staff briefed into this event</li> <li>• <b>Filed an injunction to protect breach from being reported through the mainstream media</b></li> </ul>
<i>Actions to be completed:</i>	<ul style="list-style-type: none"> <li>• An initial set of questions from privacy has been logged for review with the team, these questions will prepare us for any discussions with OPC</li> <li>• <b>Provide support to the OIA requested</b></li> </ul>
<i>Outstanding issue(s) requiring decisions:</i>	•
<b>LOGISTICS AND WELFARE</b>	

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

<i>Situation Context</i>	<ul style="list-style-type: none"> <li>• Remaining mindful of any staffing requirements and welfare concerns</li> </ul>
<i>Actions taken:</i>	<ul style="list-style-type: none"> <li>• S6(c) [REDACTED]</li> <li>• S6(c) [REDACTED]</li> </ul>
<i>Actions to be completed:</i>	<ul style="list-style-type: none"> <li>• Tracking hours for staff working within each function</li> </ul>
<i>Outstanding issue(s) requiring decisions:</i>	
<b>RECOVERY</b>	
<i>Situation Context</i>	
<i>Actions taken:</i>	<ul style="list-style-type: none"> <li>• Function on Standby</li> </ul>
<i>Actions to be completed:</i>	<ul style="list-style-type: none"> <li>•</li> </ul>
<i>Outstanding issue(s) requiring decisions:</i>	

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

## Cyber IMT Situation Report – IN-CONFIDENCE

*New information in red text*

Incident Name: Data Breach		Controller: S9(2)(a)	
		Technical Lead: S9(2)(a)	
Date: 03 Dec 2023	Time: 1000 hrs	SitRep No: 3	Response Day: 4
Prepared by: S9(2)(a)		Ph.: S9(2)(a)	
Approved by: S9(2)(a)		Ph.: S9(2)(a)	
Situation Report circulated to: Leigh Donoghue, Michael Dreyer, Andrew Slater, Sonny Taite, Sue Gordon, Viv Kerr, S9(2)(a)			
Response Objectives (Mission):			
<ul style="list-style-type: none"> <li>To support the National Health Coordination Centre in managing the ongoing Data Breach</li> <li>S6(c)</li> </ul>			

### KEY UPDATES TODAY

- The Cyber IMT was activated to coordinate Data & Digital activity in support of the National Health Coordination Centre

S6(c), S9(2)(h)

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

S6(c)

### INVESTIGATION CONTEXT

- On 30 Nov 2023, a video was posted on the New Zealand Loyal site (and multiple other sites) containing evidence of a significant data breach concerning Covid-19 vaccination records and mortality data. Emails were sent to Te Whatu Ora & Te Aka Whai Ora leadership, as well as New Zealand Members of Government notifying them of the video on 30 Nov.

S6(c)

- The Data Breach has been shared with parties in New Zealand and internationally. Additional videos and presentations are being shared publicly. S6(c)
- An injunction was granted last night which establishes protections over the data breach being reported in mainstream media sources.

S6(c)

### FUNCTIONAL AREA UPDATE

#### RESPONSE MANAGER

##### *Situation Context*

- The Cyber Incident Management Team was activated on 30 Nov
- The Cyber Controller on standby to support the National Health Coordination Centre to maintain alignment and share updates from the lead team
- S9(2)(h)

S6(d)

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

<i>Actions to be completed:</i>	<ul style="list-style-type: none"> <li>•</li> </ul>
<i>Outstanding issue(s) requiring decisions:</i>	<ul style="list-style-type: none"> <li>• No current issues</li> </ul>

S6(c), S6(d)



<i>Actions to be completed:</i>	<ul style="list-style-type: none"> <li>• Full report on all videos and contents</li> <li>• Review and provide response if appropriate to the OIA received. To take place on Monday.</li> </ul>
<i>Outstanding issue(s) requiring decisions:</i>	<ul style="list-style-type: none"> <li>•</li> </ul>

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

<b>COMMS</b>	
<i>Situation Context</i>	<ul style="list-style-type: none"> <li>National Comms are leading the communications</li> <li><b>D&amp;D Communications support has been requested and approved</b></li> </ul>
<i>Actions taken:</i>	<ul style="list-style-type: none"> <li>D&amp;D Function on Standby</li> </ul>
<i>Actions to be completed:</i>	<ul style="list-style-type: none"> <li></li> </ul>
<i>Outstanding issue(s) requiring decisions:</i>	

S6(c)



*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

Outstanding issue(s) requiring decisions:	<ul style="list-style-type: none"> <li>•</li> </ul>
<b>PLANNING / PRIVACY / LEGAL</b>	
Situation Context	<ul style="list-style-type: none"> <li>• The Controller is engaging with Privacy and Legal teams to provide any intel or support as required.</li> <li>• An injunction was granted last night which establishes protections over the data breach being reported in mainstream media sources</li> <li>• <b>The injunction has been used to remove links to a data set being shared across multiple platforms.</b></li> </ul>
Actions taken:	<ul style="list-style-type: none"> <li>• Confirmed any support required from Cyber IMT</li> <li>• Confirmed key contacts and team members to work with</li> <li>• Established meetings</li> <li>• Agreed tracking of staff briefed into this event</li> <li>• Filed an injunction to protect breach from being reported through the mainstream media</li> <li>• <b>Working closely with the OPC to keep them updated on the situation.</b></li> </ul>
Actions to be completed:	<ul style="list-style-type: none"> <li>• An initial set of questions from privacy has been logged for review with the team, these questions will prepare us for any discussions with OPC</li> <li>• Provide support to the OIA requested</li> </ul>

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

Outstanding issue(s) requiring decisions:	•
<b>LOGISTICS AND WELFARE</b>	
Situation Context	<ul style="list-style-type: none"> <li>• Remaining mindful of any staffing requirements and welfare concerns</li> <li>• S9(2)(h) [REDACTED]</li> </ul>
Actions taken:	<ul style="list-style-type: none"> <li>• S6(c) [REDACTED]</li> <li>• S6(c) [REDACTED]</li> <li>• Tracking hours for staff working within each function</li> <li>• S9(2)(h) [REDACTED]</li> </ul>
Actions to be completed:	<ul style="list-style-type: none"> <li>• Awaiting additional resource requests to be actioned</li> </ul>
Outstanding issue(s) requiring decisions:	
<b>RECOVERY</b>	
Situation Context	
Actions taken:	<ul style="list-style-type: none"> <li>• Function on Standby</li> </ul>
Actions to be completed:	•
Outstanding issue(s) requiring decisions:	

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

## Cyber IMT Situation Report – IN-CONFIDENCE

*New information in red text*

Incident Name: Data Breach		Controller: S9(2)(a)	
		Technical Lead: S9(2)(a)	
Date: 04 Dec 2023	Time: 1000 hrs	SitRep No: 4	Response Day: 5
Prepared by: S9(2)(a)		Ph.: S9(2)(a)	
Approved by: S9(2)(a)		Ph.: S9(2)(a)	
Situation Report circulated to: Leigh Donoghue, Michael Dreyer, Andrew Slater, Sonny Taite, Sue Gordon, Viv Kerr, S9(2)(a)			
Response Objectives (Mission):			
<ul style="list-style-type: none"> <li>To support the National Health Coordination Centre in managing the ongoing Data Breach</li> <li>To investigate and uncover any evidence available in Data and Digital systems</li> </ul>			

### KEY UPDATES TODAY

S6(c)

- The Cyber IMT was activated to coordinate Data & Digital activity in support of the National Health Coordination Centre

S6(c), S6(d)

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

S6(c), S6(d)

### INVESTIGATION CONTEXT

- On 30 Nov 2023, a video was posted on the New Zealand Loyal site (and multiple other sites) containing evidence of a significant data breach concerning Covid-19 vaccination records and mortality data. Emails were sent to Te Whatu Ora & Te Aka Whai Ora leadership, as well as New

S6(c)

- The Data Breach has been shared with parties in New Zealand and internationally. Additional videos and presentations are being shared publicly. S6(c)
- An injunction was granted last night which establishes protections over the data breach being reported in mainstream media sources.

S6(c)

### FUNCTIONAL AREA UPDATE

#### RESPONSE MANAGER

##### *Situation Context*

- The Cyber Incident Management Team was activated on 30 Nov
- The Cyber Controller on standby to support the National Health Coordination Centre to maintain alignment and share updates from the lead team

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

	<ul style="list-style-type: none"> <li>• S9(2)(h)</li> <li>• From 4 Dec, the response has shifted into Phase 2 which implements a risk-based, proactive response. Key priorities of this phase include: <ul style="list-style-type: none"> <li>○ S6(c)</li> <li>○ Engaging with other Crown Agencies as required</li> <li>○ Allocating additional resources to meet operational requirements</li> </ul> </li> </ul>
--	---

S6(d)

<p><i>Actions to be completed:</i></p>	<ul style="list-style-type: none"> <li>•</li> </ul>
<p><i>Outstanding issue(s) requiring decisions:</i></p>	<ul style="list-style-type: none"> <li>• No current issues</li> </ul>

S6(c), S6(d)

*This report was current at the time of distribution.*  
*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

<i>Actions to be completed:</i>	<ul style="list-style-type: none"> <li>• Full report on all videos and contents</li> <li>• Review and provide response if appropriate to the OIA received. To take place on Monday.</li> </ul>
<i>Outstanding issue(s) requiring decisions:</i>	<ul style="list-style-type: none"> <li>•</li> </ul>
<b>COMMS</b>	
<i>Situation Context</i>	<ul style="list-style-type: none"> <li>• National Comms are leading the communications</li> <li>• D&amp;D Communications support has been requested and approved</li> </ul>
<i>Actions taken:</i>	<ul style="list-style-type: none"> <li>• D&amp;D Function on Standby</li> <li>• <b>Established contact with NCSC Comms support</b></li> </ul>
<i>Actions to be completed:</i>	<ul style="list-style-type: none"> <li>•</li> </ul>
<i>Outstanding issue(s) requiring decisions:</i>	

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

S6(c)



*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*



<i>Outstanding issue(s) requiring decisions:</i>	<ul style="list-style-type: none"> <li>•</li> </ul>
<b>PLANNING / PRIVACY / LEGAL</b>	
<i>Situation Context</i>	<ul style="list-style-type: none"> <li>• The Controller is engaging with Privacy and Legal teams to provide any intel or support as required.</li> <li>• An injunction was granted last night which establishes protections over the data breach being reported in mainstream media sources</li> <li>• The injunction has been used to remove links to a data set being shared across multiple platforms.</li> </ul>
<i>Actions taken:</i>	<ul style="list-style-type: none"> <li>• Confirmed any support required from Cyber IMT</li> <li>• Confirmed key contacts and team members to work with</li> <li>• Established meetings</li> <li>• Agreed tracking of staff briefed into this event</li> <li>• Filed an injunction to protect breach from being reported through the mainstream media</li> <li>• Working closely with the OPC to keep them updated on the situation.</li> </ul>
<i>Actions to be completed:</i>	<ul style="list-style-type: none"> <li>• An initial set of questions from privacy has been logged for review with the team, these questions will prepare us for any discussions with OPC</li> <li>• Provide support to the OIA requested</li> <li>• S6(c)</li> </ul>

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*

Outstanding issue(s) requiring decisions:	•
<b>LOGISTICS AND WELFARE</b>	
Situation Context	<ul style="list-style-type: none"> <li>Remaining mindful of any staffing requirements and welfare concerns</li> <li>S9(2)(h) [REDACTED]</li> </ul>
Actions taken:	<ul style="list-style-type: none"> <li>S6(c) [REDACTED]</li> <li>S6(c) [REDACTED]</li> <li>Tracking hours for staff working within each function</li> <li>S9(2)(h) [REDACTED]</li> <li></li> </ul>
Actions to be completed:	<ul style="list-style-type: none"> <li>Awaiting additional resource requests to be actioned</li> </ul>
Outstanding issue(s) requiring decisions:	
<b>RECOVERY</b>	
Situation Context	
Actions taken:	<ul style="list-style-type: none"> <li>Function on Standby</li> </ul>
Actions to be completed:	<ul style="list-style-type: none"> <li></li> </ul>
Outstanding issue(s) requiring decisions:	

*This report was current at the time of distribution.*

*IN-CONFIDENCE: This information can only be disseminated or duplicated with the express permission of Te Whatu Ora Health New Zealand. This document contains confidential information, and must be handled, stored, and transferred appropriately, including not making it available outside of the primary recipient list.*