MINISTRY OF HEALTH
MANATŪ HAUORA

Cyber Security Communications Strategy

Created by	**In Consultation with**
Mary Baines, Senior Communications Advisor, Ministry of Health	Matt Lord, Security Manager, Ministry of Health
	Signoff Emma Blackmore, External Communications and Engagement Manager, Ministry of Health

Purpose

This document sets out how the Ministry of Health will ensure there is a coordinated approach to managing communications about cyber events in the health and disability sector. The purpose of this plan is to:

- outline the Ministry's communications and stakeholder engagement approach when responding to a cyber incident;
- provide a list of potential stakeholders and audiences and provide a guide on how to communicate with them;
- provide a scalable list of outputs and actions that should be produced or taken at different phases of a cyber security incident response; and
- identify and mitigate any communications-related risks.

This strategy sits alongside and aligns with the New Zealand Health Sector Cyber Event Response Plan (February 2019). This document is for use by the Ministry of Health and an affected health sector entity.

Context

The global health sector has experienced an increasing trend of major cyber events, security incidents and data breaches in recent years. The New Zealand health and disability sector has also been impacted by cyber events, including when in May 2021, the Waikato District Health Board was struck by a ransomware attack. The incident affected IT systems, hospitals' service delivery and privacy for staff and patients.

Attempted cyberattacks on the health and disability sector are a constant threat. While the vast majority are prevented from impacting IT networks and systems and the provision of healthcare to New Zealanders, it is important the sector is prepared for potential future incidents.

When dealing with cyber security incidents, responding to the technical issues is only part of the response effort. A major component of a cyber security issue response is how well an organisation communicates with staff, people who may have been affected, the general public, and internal and external stakeholders about what is going on, how it is affecting the organisation and how it could affect them.

Communications objectives

The objectives of this plan are to ensure:

- timely and accurate information is delivered to key audiences;
- internal and external stakeholders are kept informed; and
- consistent messaging and appropriate sequencing of information is delivered during a cyber security incident.

Communications and engagement approach

Good communication, whether it's with staff, customers, the media or the public is a key component of managing a cyber security incident. Each cyber security incident is different, so the communication approach used will differ. In some circumstances, proactive communication will need to be assessed against other factors such as the nature of the cyber security event and where known, the nature and capability of the actors behind it.

However, the following key principles guide the Ministry of Health's communications and engagement approach to managing cyber events.

- **Proactiveness:** When managing a cyber event issue, proactive communication with staff, affected people and the media is normally the most effective approach. Even if only limited information is available to be shared, it is important to let people know that an incident is occurring.
- **Transparency:** Sharing updates with stakeholders in an open and transparent way (which does not include information that could aid the malicious actors) is key to managing reputational risk and preserving public trust and confidence. An information vacuum can lead to speculation and misinformation.
- **Timeliness:** Prompt action is essential for shaping and getting ahead of a developing story. Knowing what to say and when to say it can make a big difference to the perception of how well the incident is being managed.
- **Collaboration:** Relevant entities across the health and disability sector have a responsibility to work collaboratively when dealing with a cyber issue, including ensuring regular information sharing and sticking to agreed messaging.

Roles and responsibilities

As per the Response Plan, during a cyber security incident, the health and disability sector may be working with government agencies like CERT NZ or the National Cyber Security Centre (NCSC). The affected organisation (e.g. Ministry of Health or a health sector entity – depending on the nature of the incident) is the lead for communications.

The roles and responsibilities of each organisation who are involved in communications and stakeholder engagement are outlined below.

Organisation	Role	Responsibilities
Ministry of Health	To coordinate external communications, stakeholder engagement and strategic advice regarding the incident, and on behalf of, the health sector entity.	• To support the affected health sector entity in its external communications and engagement regarding the event. • To lead the provision of advice to the Minister(s) in partnership with the affected health sector entity and NCSC/CERT NZ. • To protect and preserve critical national digital health systems and capabilities. • To work collaboratively with, and in support of, the affected health sector entity.
Affected health sector entity	To communicate with staff, affected people and the community about the incident.	• To provide internal updates/communications to staff. • To fulfil any privacy obligations in notifying affected individuals. • To engage with media regarding the event (i.e. manage press conferences, media requests (unless sent directly to the Ministry of Health) and press releases).

National Cyber Security Centre (NCSC)	To provide incident response including on-the-ground support, forensic analysis, mitigation advice and communications advice.	• Given the varied nature of cyber security emergencies, and size and mandate of various health sector entities, the operational lead agency may vary but could be NCSC or CERT NZ. • To provide specialist technical cyber security incident response capabilities (NCSC only). • To input into communications and advisory activities undertaken by the Ministry of Health and/or the health sector entity. • To review affected entity's/Ministry of Health's messaging.
CERT NZ	To promote awareness of good cyber security practice, support response advice for potentially high or national impact cyber security events, and situational awareness and information sharing.	

Communicating with key stakeholders and audiences

The stakeholders and audiences and how to communicate with them will vary between incidents but will be both internal and external. However, in general terms:

- The staff of the affected health sector entity will need to know how this incident will impact their work; if they need to change the way they are working; what actions they can take to protect themselves; what they can say if they get questions; and what they can expect to happen next.
- The public will need to know how this may impact them; what is being done; what actions they can take to protect themselves; how they will know if they have been affected; and next steps.

Government

Audience/stakeholder	Channel/method
Minister(s)	• Situational reports • Communication Line Book • Regular meetings • Ministerial Reports
Agencies involved in the cyber incident response (e.g. CertNZ, NCSC, vendors or other security service providers)	• Situational reports • Communication Line Book • Regular meetings
Government agencies that have an interest due to the nature of their work (e.g. Privacy Commissioner, ACC, DIA, IDCare, NetSafe)	• Key messages document, sent via email

Internal

Audience/stakeholder	Channel/method
Staff from affected health sector entity	• Internal communications channels including email, printed copies, intranet, phone/video calls
Other health entities (who were not directly affected but are feeling impact)	• Updates via regular meetings • Key message document
Ministry of Health staff	• Internal communications channels including DG updates and intranet
Ministry of Health's Executive Leadership Team and DDG	• Regular meetings with the Ministry of Health's response lead

External

Audience/stakeholder	Channel/method
Members of the public who have been affected by the cyber incident	• Direct contact (phone, letter or email by affected health sector entity)
Media	• Press conferences

	• Press releases • Media advisories • Proactive conversations • Reactive responses – statements and interviews
General public	• National and local media channels • Public information campaigns via local advertising (print, digital, radio) • Social media posts from Ministry of Health and/or affected health sector entity

Key messages

Approach

The key messages for each incident will vary depending on its nature, severity and impacts.

Internal and external messaging should include what has happened, when it happened, and what the next steps are. If there are gaps in the information about the incident, it should be stated that the situation is being investigated and that the public will be updated when more information becomes available.

When framing the message:

- **Base all information on facts:** In the first few days after a cyber incident, it's difficult to know its full scale and impact. Double check that everything you are saying is factually correct.
- **Accept responsibility:** The affected health sector entity is responsible for its network and data.
- **Avoid downplaying:** This may be seen as not taking the incident seriously.
- **Address feelings of vulnerability:** While doing so, identify ways people can protect themselves.
- **Keep the messages clear and easy to understand:** Avoid jargon and keep the message simple.
- **Make it clear that it takes time to assess and recover from these incidents:** Provide timelines where possible. Do not feel tempted to give an answer or say you are on top of the situation, as there is likely to be more information to come to light.

It is important to note that cyber criminals can monitor media commentary relating to an incident and may change their behaviour based on that commentary. Certain words and nuances in language may unintentionally inform the attackers. All messaging must therefore be reviewed by NCSC and/or CERT NZ.

Skeleton messaging

The below skeleton messaging can be adapted for different cyber incidents.

- We have been made aware that a cyber security incident is affecting the organisation's IT environment.
- We are in the early stages of identifying what has happened. An investigation is underway.
- We have a plan in place for when these kinds of incidents occur. We are following our processes set out in our plan.
- We have engaged external assistance to help us address the incident.
- We will keep the public and our stakeholders updated as the situation develops.

General key messages about cyber security

- Attempted cyberattacks on the health and disability sector are a constant and ever-evolving threat. The vast majority are prevented from impacting IT networks and systems and the provision of healthcare to New Zealanders.
- The health and disability system has robust processes in place to allow it to continue providing services in a variety of situations.
- All organisations need to continually review and improve cyber security protections. Cyber criminals continue to pose a threat to the security of the health sector, which is why there is ongoing investment in new security protections.
- In Budget 2021, the Government announced investment of up to $385 million over four years to improve health sector data and digital infrastructure and capability.

General key messages about keeping personal data safe

- Please be wary of any unsolicited communications claiming to be from a Government organisation or private company like a bank. Unusual activity can include:
  - contact that is out of the blue via phone, email, on social media or even by mail
  - being asked to verify your account or personal details
  - being asked for remote access to your device
  - being told there's a problem with your phone, laptop or internet connection
  - someone pressuring you to make a decision quickly
- The latest known scams are recorded by Scamwatch at Consumer Protection and can be viewed here - www.consumerprotection.govt.nz.
- There are a number of ways you can protect your personal information and data, including:
  - regularly changing passwords
  - avoiding opening attachments from unknown sources
  - having up-to-date antivirus tools for all of your devices that access the internet
  - keeping your electronic devices and applications up to date
  - talking to your bank about additional security you can put on your accounts.
- If you have concerns about the safety of your information or are seeking additional ways to protect yourself, you may wish to visit IDCARE, New Zealand's national identity and cyber support community service - www.idcare.org. IDCARE is a registered New Zealand charity that specialises in working with community members to protect and respond to personal information risks.
- If you are concerned your privacy has been breached, you can make a complaint via the Privacy Commissioner here - www.privacy.org.nz.

Spokesperson

It is usually best practice to use the same spokespeople throughout the incident. Even if there may be not much information to share, the public can feel more reassured if the same people are speaking about the incident. Who is put forward as a spokesperson will depend on the nature of the incident, but spokespeople could include:

- The CE of the affected health sector entity;
- Subject matter experts in IT restoration, privacy and clinical service delivery from the health sector entity; and/or
- The Deputy Director General Data and Digital, Ministry of Health.

An external media professional can be useful to test spokespeople's understanding of the complex issues before fronting for the media.

Standard operating procedures

This section lays out the specific communications actions that should be taken before, during and after the New Zealand Health Sector Cyber Event Response Plan (February 2019) is activated. The Response Plan is activated when a cyber event affecting a local health sector entity is escalated to the Ministry due to its potential to have severe consequences at a national level.

Objective	Actions	Lead	Notes
Phase 1: Local health sector entity cyber response and severity impact assessment As per the Response Plan, an affected health sector entity must activate its internal event response plan and make an assessment as to the potential sector-wide impacts. Depending on the outcome of this severity assessment process, the incident will either remain categorised as a localised event that is being responded to solely by the affected health sector entity or be assessed as having potential consequences to multiple entities or wider public health safety. If the second action pathway is identified as the most likely the affected health sector must immediately contact the Ministry of Health.			
Groundwork is laid so the Ministry is prepared to respond to a local cyber security issue, if Phase 2 is activated	Ministry of Health spokesperson identified and briefed	Ministry of Health's communication team	-
	Holding messages developed in anticipation of escalation	Ministry of Health's communication team	-
Phase 2: Responding to a cyber security incident If the Response Plan has been activated, Phase 2 begins. It is at this point that the affected health sector entity in partnership with Ministry of Health (and NCSC/CERT NZ if necessary, as set out in Annex D of the Response Plan) assesses the potential severity of the technical, personal health information, clinical, legal, financial and policy/reputational impact(s) of the cyber event. As per the response plan, during Phase 2, the Ministry's core function is to coordinate external communications, stakeholder engagement and provide strategic-level advice. All actions will be taken collaboratively with, and in support of, the affected health sector entity.			
First 24 hours			
Communications coordination structure established	Ministry of Health comms lead and Communications Manager from affected health sector entity connect to discuss requirements, approach, role and responsibilities and agree next steps	Communications lead, Ministry of Health	-

	Ministry of Health comms lead connects with relevant Government communications leads (e.g. NCSC) to discuss roles and responsibilities and agree next steps	Communications lead, Ministry of Health	-
Staff from affected health entity notified and feel informed	Staff from affected health sector entity notified about incident, provided with information on how to keep their information safe and given guidance on next steps and expected timeframes	Communications Manager, affected health sector entity	During the Waikato DHB IT outage, staff were notified about the incident via email, text, phone calls and printed copies of updates distributed throughout facilities
	Key messages, reactive lines and FAQ documents specific to internal audiences/affected staff developed	Communications Manager, affected health sector entity	-
Incident communicated externally	Media advisory or press release issued as required	Communications lead, Ministry of Health and Communications Manager, affected health sector entity	-
	Social media update posted by affected health entity or Ministry of Health as required	Communications lead, Ministry of Health and Communications Manager, affected health sector entity	-
	External messaging and reactive lines developed	Communications lead, Ministry of Health	Review required from NCSC or CERT NZ to ensure language does not aid malicious actors
Media management	Media alerts set up to monitor and track stories	Communications lead, Ministry of Health	Via media monitoring provider
	Media requests sent to Ministry or affected health sector entity responded to	Media team, Ministry of Health and Communications Manager, affected health sector entity	-

Internal and external stakeholders communicated with and feel informed	Ministry of Health's DG and ELT updated and informed via written and oral updates	Ministry of Health's response lead	-
	Relevant Minister(s) updated and informed via written and oral updates	Ministry of Health's response lead	-
	First sitrep sent	Ministry of Health's Intel lead	If an EMT/CIMS structure is set up to respond to the cyber incident, the Intelligence function will issue daily situational reports (sitreps) to key stakeholders including Ministers, Ministry leadership and key Government stakeholders
	First communication line book sent	Communications lead, Ministry of Health	If an EMT/CIMS structure is set up to respond to the cyber incident, the Communications/PIMS function will issue daily communication line books/key messages to Ministers and key Government stakeholders
Ongoing response (Day 2 until recovery phase)			
Staff from affected health entity updated regularly and kept informed of developing situation	Regular communications issued to affected staff as required via email, text, phone/video call, print copies, outlining updates and guidance across all services, as required	Communications Manager, affected health sector entity	During the Waikato DHB IT outage response phase, staff received two daily updates (AM and PM) via email, a printed daily staff update distributed across all facilities, and emails and text messages for urgent updates requiring immediate response

Ongoing communication to the public about the incident	Public information management campaign started	Communications lead, Ministry of Health and Communications Manager, affected health sector entity	A public information campaign could include digital, print or radio advertising and focus on issues including keeping the community updated on service restoration or privacy issues. During the Waikato DHB IT outage, there was a public information campaign on personal data and privacy including advertising in the local newspaper
	Social media updates, as required	Communications lead, Ministry of Health and Communications Manager, affected health sector entity	During the Waikato DHB IT outage, social media updates on protecting personal data were posted on both the DHB's and the Ministry's accounts as part of the public information campaign
Media management	Proactive media as required via press conferences and media releases, as required	Communications lead, Ministry of Health and Communications Manager, affected health sector entity	During the Waikato DHB IT outage, the DHB held daily press conferences and issued daily press releases every day for the first three weeks. This was scaled back to three times weekly then weekly
	Media requests responded to, as required	Media team, Ministry of Health and Communications Manager, affected health sector entity	-
	Media advisories reminding journalists of obligations (e.g. around publishing private information) issued as required	Communications lead, Ministry of Health and Communications Manager, affected health sector entity	Advisories may be sent from Privacy Commissioner or CERT NZ, with support from the Ministry or the affected health sector entity

	Reactive messaging on emerging issues developed, as required	Communications lead, Ministry of Health and Communications Manager, affected health sector entity	-
Internal and external stakeholders communicated with regularly	Daily meeting between Ministry's communications team, affected entity's communications team and supporting comms people (e.g. NCSC or CERT NZ)	Communications lead, Ministry of Health	-
	Daily Situational report issued	Ministry of Health's Intel lead	If If an EMT/CIMS structure is set up to respond to the cyber incident, the Intelligence function will issue daily situational reports (sitreps) to key stakeholders including Ministers, MoH leadership and key Government stakeholders
	Media scan email (collated from alerts) sent to internal stakeholders and leadership daily	Communications lead, Ministry of Health	Email outlining key media topics and emerging risks
	Daily meeting with Minister' Office to provide updates	Ministry of Health's response lead	-
	Daily communication line book issued	Communications lead, Ministry of Health	If an EMT/CIMS structure is set up to respond to the cyber incident, the Communications/PIMS function will issue daily communication line books/key messages to Ministers and key Government stakeholders
	Weekly Ministerial Report sent to Minister's Office		If an EMT/CIMS structure is set up to respond to the cyber incident, the response

			lead will send a weekly report to Ministers outlining key and emerging issues
	Twice-weekly key messages document sent to stakeholders	Communications lead, Ministry of Health	The key messages document is a scaled back version of the communication line book and can be sent to Government agencies that have an interest in the response (e.g. Privacy Commissioner, Net Safe)
Phase 3: Recovery phase			
Staff from affected health entity updated regularly	Twice-weekly communications to staff outlining guidance on service delivery, recovery planning and progress updates	Communications Manager, affected health sector entity	During the recovery phase, Waikato DHB staff received twice-weekly updates via email and print. Further communications occurred to advise staff of potential privacy impacts.
Ongoing communication to the public about the incident	Public information campaign continued as required	Communications lead, Ministry of Health and Communications Manager, affected health sector entity	-
Media management	Proactive media as required via press conferences and media releases, as required	Communications lead, Ministry of Health	-
	Reactive messaging on emerging issues developed, as required	Communications lead, Ministry of Health and Communications Manager, affected health sector entity	-
	Media requests managed as required	Media team, Ministry of Health and Communications Manager, affected health sector entity	-

Internal and external stakeholders communicated with regularly	Weekly Ministerial Report to Minister’s office	Ministry of Health’s response lead	-
	Situational reports sent three-times weekly	Ministry of Health’s Intel lead	-
	Communications Line book sent weekly	Communications lead, Ministry of Health	-
	Key messages sent to stakeholders as and when issues emerge	Communications lead, Ministry of Health	-
	Media scan email sent to key internal stakeholders as and when issues emerge	Communications lead, Ministry of Health	-

Communications risks and issues

Issue/Risk	Mitigation
Lack of coordination between communications people from different organisations involved in the response	• Clear structure defining roles and responsibilities of each organisation defined at the beginning of the response • Regular meetings set up between all communications people involved in the response
Staff of affected health entity not feeling informed	• Regular updates sent to staff of affected health entity via different means including email, text, printed copies and phone calls
Public not feeling informed about situation	• Public information campaign launched providing information on key issues (e.g. services available, privacy)
Stakeholders not feeling informed	• Situational report and communication line book sent daily • Key messages document sent to key stakeholders in government twice weekly during response phase and as and when required during recovery phase
Minister(s) not feeling informed	• Regular meetings set up with relevant Minister's office • Situational report and communication line book sent daily • Ministerial report sent weekly
Negative media coverage	• Transparent and open relationship with journalists • Regular press conferences and press releases • Media advisories sent to provide additional support to journalists • Timeliness in responding to media requests
Information or wording provided to media may aid or inform malicious actors (the use of certain words may unintentionally inform the attackers)	• All messaging and nuance in language reviewed by NCSC or CERT NZ

ENDS