New Zealand Health Sector Cyber Event Response Plan

February 2019

Purpose

1. The purpose of this plan is to outline the New Zealand health and disability sector's process for managing and containing major cyber events; and to minimise their impact on locally and nationally critical operational; clinical; and patient data sets, and information technology systems, in order to maintain the delivery of "front-line" health services, while preserving public trust and confidence.

   *NOTE: this plan is marked as **TLP AMBER**. This means that recipients of this plan may only share it with members of their own organisation who need to know, and only as widely as necessary to act on it.*

Context

2. Over the recent period, the global health sector has experienced an increasing trend of major cyber events, security incidents, and data breaches; industry predictions suggest ransomware attacks on healthcare organisations — the No. 1 cyber-attacked industry — will quadruple by 2020[1]. In past year, the most notable of these incidents was the global "Wanna Cry" ransomware outbreak in May 2017; this cyber event almost operationally crippled the UK's National Health Service. Closer to home, the New Zealand health sector has also recently been impacted by cyber events.

3. It should be noted that a security incident is considered to be one of a range of cyber events that is covered under this plan. Various examples of health sector-wide cyber events that fall within the scope of this document may include:

   - major disruption to operationally vital or critical local or national digital health systems (i.e. ransomware, or Internet connectivity failure);
   - attempts to gain unauthorised access to national digital health systems (e.g. hacking);
   - nationally critical health data-sets (e.g. National Health Index) are altered or deleted without authorisation by the data "owner";
   - virus or other malicious malware attacks (suspected or actual) that prevent the delivery of public-facing front-line clinical services; or
   - damage or loss of access to critical national digital health systems due to theft; fire; natural disaster; or catastrophic systems/physical infrastructure failure.

New Zealand health sector-wide cyber event response plan

4. An effectively implemented, resourced and tested health sector wide cyber event response plan is a vital part of maintaining maintain public trust in the health sector; and the security, privacy, and availability of New Zealand's digital health systems.

   NOTE: this plan should not be used to manage sector-level privacy breaches; the process required to manage this type of incident is distinctly different. Furthermore, it should also be

[1] https://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics.html

noted that this plan is not intended to replace the already nationally embedded Coordinated Incident Management System (CIMS) health sector-wide model of emergency management; rather it is expected that plan will form a context-specific response model within the wider CIMS framework.

5. The New Zealand health sector-wide cyber event response plan consists of two phases:

    i. Phase One: local/organisational-level cyber event response, and national sector-level impact assessment; and

    ii. Phase Two: local cyber event severity escalation to the national-level, and health sector cyber event plan activation.

Phase One: local health sector entity cyber event response and severity impact assessment

6. Each health sector entity must have an established and tested internal cyber event response plan in place so that the potential severity of an incident can be triaged as early as possible. (Core requirements for an effective cyber event response plan appear at Annex B).

7. Typically all cyber events will initially present themselves as local issues. On this basis, every potentially affected health sector entity will immediately triage each cyber event they experience, and respond to it in accordance with their own internal event response plan.

8. As part of this local incident triaging process, the affected health sector entity must also simultaneously consider the following sector-wide impact criteria:

    i. does this event also have the ability to compromise the *confidentiality* of patient identifiable or clinical information held within critical local or national digital health systems[2]?; or

    ii. does this event have the ability to compromise the *integrity* of information required to deliver local or national public-facing/front-line operational or clinical services?; or

    iii. does this event have the ability to materially affect the *availability* of either locally or nationally critical digital health data or information and systems required to deliver public-facing/front-line operational or clinical services?; or

    iv. does this event have the ability to compromise the *trust and confidence* of the public in relation of the affected health sector entity's ability to deliver operational or clinical services?;

    v. does this event have the ability to potentially *involve the use of public funding* in relation to cyber-crime activities (i.e., the payment of ransomware)?;

[2] Examples of a national digital health system would be NHI; HPI; NBSP; NSS; or Connected Health.

vi. is it possible this event could separately present itself again in a similar fashion *elsewhere* in the health sector?; or

vii. does this event have the ability to attract *public attention* in the near-term to the extent that it could lead to Chief Executive or Ministerial-level interaction with the media?

9. Depending on the outcome of this severity assessment process, two action pathways will emerge:

i. the incident remains categorised as a localised event that is being responded to solely by the affected health sector entity, and the NCSC/CERT NZ and MoH are notified for situational awareness only; or

ii. one or more of the sector-wide impact criteria listed above are met, meaning the incident is assessed to be of sufficient severity and potential consequence that it could represent a potential threat to multiples DHBs or wider public health and safety.

10. Should the second action pathway be initially identified as the most likely, the affected health sector entity will immediately contact the relevant MoH POC(s) listed at Annex C. Furthermore, should the event also be considered a possible cyber *security* incident, the specified NCSC/CERT NZ POCs [listed at Annex C] will also be contacted.

Phase Two: activation of the New Zealand health sector cyber response plan

11. At this point, the affected health sector entity in partnership with MoH [and NCSC/CERT NZ if necessary] will further assess the potential severity of the technical, personal health information, clinical, legal, financial, and policy/reputational impact(s) of the cyber event at hand.

12. If the cyber event continues to be assessed at sufficient severity and potential consequence that it could represent a potential threat to multiple DHBs/PHOs/NGOs, or wider public health and safety, the RACI table at Annex A will be utilised to guide the joint decision-making required to collectively manage the cyber event at a sector-level.

13. Within the context of the RACI table-led approach, MoH's core function will be to co-ordinate external communications; stake-holder engagement; and strategic-level advice regarding the incident across, and on behalf of, the health sector. These objectives will be achieved by:

a. supporting the affected health sector in its external communications and engagement regarding the event;

b. leading the provision of advice to the Minister(s) (in partnership with the affected health sector [and the NCSC/CERT NZ if necessary]); and

c. acting to protect and preserve critical national digital health systems and capabilities.

It is important to note these MoH functions will be undertaken collaboratively with, and in support of, the affected health sector entity. (It is not intended that the MoH will carry out an operational role.)

14. Beyond the affected health sector entity(s) and MoH, other parties likely engaged within a health sector cyber event will be as follows:

Organisation	Role	Responsibilities
National Cyber Security Centre	to protect and respond to cyber incidents affecting important information infrastructures, cyber incidents that pose a threat to New Zealand's national security, cyber incidents, and cyber incidents that have been perpetrated by an advanced persistent threat actor.	• given the varied nature of cyber security emergencies, and size and mandate of various health sector entities, the operational lead agency will vary, but will typically be NCSC or CERT NZ; • input into communications and advisory activities undertaken by MoH and/or the affected health sector entity; • provide specialist technical cyber security incident response capabilities [NCSC only]
CERT NZ	to undertake New Zealand-wide incident response and triage, situational awareness and information sharing, advice and outreach, and coordination of serious cyber security incidents.	
National Cyber Policy Office [DPMC]	to provide policy advice to Ministers regarding national-level cyber incidents.	• provide advice to Ministers regarding cyber incident communications, and ministerial involvement require to help response efforts.
Government Chief Digital Office [ICT Assurance]	provides government and the public with assurance and confidence that ICT risks and processes in the State services are identified and managed effectively.	• leads the delivery of ICT 'system-wide' assurance and advice across government, as part of government's overall assurance framework; and • provide assurance oversight of District Health Boards' ICT capability programmes.

15. Assessing the potential severity of a health sector cyber event will require equal consider both its technical and non-technical attributes. To this end, the following factors should be considered:

- Are there any risks to public health and/or safety?;
- How clinically/commercially/personally sensitive is the information?;
- What is the context of the information involved?;
- Was the information encrypted or otherwise inaccessible?;
- How might the compromised information be used?;
    - could it be used for fraudulent or harmful purposes?;
- Was any third-party information involved?;
- Is there a risk of ongoing breaches?
- What is the number and nature of affected persons that could be affected?;
- Might the information have been lost or stolen?;
- Has the information or item been recovered?;
- Could the data have been tampered with?;

- Is this an isolated event, or could it be a symptom of a wider systemic problem?;
- Does this event create a litigious issue that now needs to be managed?; and
- Does this event involve financial loss?

"All-of-Government" national response to a health sector cyber security event: National Cyber Security Emergency Plan (CSERP) activation

NOTE: if a health sector cyber event is confirmed as a cyber *security* incident, the following supplementary escalation pathway will likely be followed:

16. At the outset, it is not the intention of the CSERP to remove the decision-making ability of MoH or affected health agencies; it is designed to be enabling and provide a framework for coordinated responses. In other words, MoH and the affected health sector agency should always retain the right to take all event response decisions as they relate to clinical systems and patient safety.

17. If a confirmed health sector cyber security incident is mutually triaged at a LOW or MEDIUM[3] level, the operational response by central government agencies [beyond MoH] will be limited to technical advice and assistance from CERT NZ or NCSC.

18. Due to the dynamic nature of cyber security events, the categorisation may change throughout its "life". If at any stage a health sector cyber security event is re-triaged at HIGH, a National Cyber Incident Coordination Group meeting being should convened. These Groups are cyber-security focused, and sit below the activation of the National Security System.

19. National Cyber Incident Coordination Group meetings are typically chaired by Director: CERT NZ, Director-General: GCSB, or Director: National Cyber Policy Office, or by a senior representative from New Zealand Police (or by suitable delegates). The MoH will likely attend as a representing the affected national sector in the form of the MoH's Group Manager: National Digital Systems and/or Group Manager: Digital Strategy and Investment. It is at this point where it is also likely that the Minister of Health [and Minister Responsible for the GCSB potentially also] would be formally briefed on this development.

20. If the incident is triaged at CRITICAL, the National Security System may be triggered in the form of activating the CSERP. This involves a series of formal national-level coordination, response, advisory, and communications activities. These actions would include the convening a Watch Group and possibly CE-level Officials Domestic and External Security Committee meetings.

21. Further detail on the activation of the National Cyber Security Emergency Response Plan is held by the National Cyber Policy Office.

[3] Definitions of these ratings can be found at Annex D, and are drawn from the National Cyber Security Emergency Response Plan.

Annex A

Organisation	Role		Tasks								
		Decision to activate health sector cyber plan	Request assistance from NCSC/CERT NZ	Advise/brief Minister of Health	Engage with media on cyber event	Respond to incident	Identify clinical impact	Decision to use public funding in relation to cyber-crime activities	Determine National Digital Systems integrity	Escalation to National Security Event	National Security System Response
Health Sector Representation	CE(s) of affected health sector entity(s) affected by cyber event [or suitably empowered delegate]	A	A	A^2	A^2	C	A^2	R^2	C	C	C
	CIO/CISO/functional equivalent of health sector entity affected by cyber event [or suitably empowered delegate]	R^1	R	R^2	I	R	I	C	C	R	R
	CMO/functional equivalent of health sector entity affected by cyber event [or suitably empowered delegate]	C	I	C	C	I	C	I	I	C	C
	communications representative of the health sector entity(s) affected by cyber event	I	I	I	R^2	I	I	I	I	I	I
	Chair of DHB CIOs forum [or suitably empowered alternate]	I	I	I	I	I	I	I	I	C	C
	incumbent Chair of PHO CIOs forum [or suitably empowered alternate]	I	I	I	I	I	I	I	I	C	C

	incumbent Chair of NGO Council [or suitably empowered alternate]	I	I	I	I	I	I	I	I	C	C
	legal representative of the health sector entity affected by cyber event	I	C	C	C	I	I	C	I	I	I
Ministry of Health	Director-General of Health [or suitably empowered delegate];	I	I	A[1]	A[1]	C	A[1]	R[1]	A	A	A
	Deputy Director-General (Data and Digital)	A	I	R[1]	C	C	C	C	R	R	R
	Group Manager (Digital Strategy and Investment) / Group Manager (National Digital Services) [or suitably empowered delegate]	C	C	C	C	C	C	C	C	R	R
	Chief Security Advisor/ Information Technology Security Manager (National Digital Services)	R[2]	C	C	I	R	I	C	C	R	R
	Director Emergency Management [or current National Health Coordination Centre (NHCC) Duty Officer]	I	I	C	I	R	C	I	C	R	R
	Chief Medical Officer [or suitably empowered delegate]	C	I	C	C	I	A[1]	I	I	C	C
	Chief Privacy Officer [or suitably empowered delegate]	I	I	C	C	C	I	C	I	I	I

	Corporate Communications Team;	I	I	C	R^1	I	I	C	I	I	I
	Group Manager (Business Performance, Technology and Digital Services) [or suitably empowered delegate]	I	I	C	C	I	I	I	C	C	C
	Manager Corporate Security	I	I	I	I	I	I	I	I	I	I
All-of-Govt.	a representative from the NCSC or CERT NZ [if appropriate]	I	C	C	C	C	I	C	I	R	R
	a representative from the NCPO [if appropriate]	I	I	C	C	I	I	C	I	A	A
	a representative from the GCDO [if appropriate]	I	C	C	I	I	I	I	I	C	C
	a representative from the Privacy Commission [if appropriate].	I	I	I	I	I	I	I	I	I	I
	Minister [or Associate Minister] of Health	I	I	I		I	I	A	I	C	A

- **Responsible:** person who performs an activity or does the work;
- **Accountable:** person who is ultimately accountable and has Yes/No/Veto;
- **Consulted:** person that needs to feedback and contribute to the activity; and
- **Informed:** person that needs to know of the decision or action.

NOTE: where varied sector or MoH roles bear joint accountability or responsibility for undertaking a particular action together, these combined decision-making requirements appear will be indicated within the RACI table by a superscripted indicator (examples would be A^1; A^2; R^1; or R^2).

Annex B

Criterion of a good cyber event response plan

When developing an internal cyber event response plan, the following components should be included within it:

- analysis of the threat environment including the likelihood and severity of potential incidents. Consider industry specific threats, the type and value of data you hold, third party networks and cyber resilience posture of your networks;
- identification of key assets, data and critical systems. What are you working to protect and why does it need protecting?;
- plans for each major incident type and different types of data that could be compromised. For example, the theft of personnel data would have a very different response to a ransomware attack. These plans should include timeframes and objectives;
- key roles and responsibilities of management and staff. It's crucial all parties involved understand the reporting lines—who will be making decisions, what the decision thresholds are, what involvement there is from senior management, and when to engage with MoH and NCSC/CERT NZ;
- key tools including contact lists, checklists and guides for use during the response;
- a process for alerting necessary stakeholders, including the Ministry of Health, and the NCSC/CERT NZ, suppliers and external agencies that may be impacted;
- public relations and media management. What advice can you give your customers/clients? Who is the media spokesperson and what can be said to the media? If businesses fails to manage this well, the reputational damage can far outweigh the actual business cost of the incident;
- arrangements to regularly review and exercise the plan. A plan might look good on paper but it regularly needs to be exercised to ensure it is effective. Make sure there is a review schedule that considers the frequency of changes to the organisation or the threat environment. For example - for a large organisation that has frequent structural changes or new platforms, consider reviewing every three months. For a smaller organisation, perhaps every six months; and
- post-incident review and reporting. It's important to document the incident details and response actions, collect the lessons learned and update the incident response plan to improve future responses.

Other useful resources that can utilised in developing an effective cyber-event response plan include:

- NCSC NZ – "The New Zealand Security Incident Management Guide for Computer Security Incident Response Teams (CSIRTs);
- NIST – "Computer Security Incident Handling Guide"; and
- UK NHS Digital – "Information security incident: good practice guide".

Annex C

Key Health Sector Cyber Event Contacts

a. External technical guidance, assistance and support

National Cyber Security Centre
Ph: 04-498-7654,
E-mail: incidents@ncsc.govt.nz

CERT NZ
Ph: 0800-237-869,
URL: https://www.cert.govt.nz/it-specialists/report-an-incident/

b. MoH sector-wide cyber event response leads

Matthew Lord
Information Technology Security Manager
Data and Digital – Ministry of Health
Mobile: s 9(2)(a)
E-mail: matthew.lord@health.govt.nz or itsecurity@health.govt.nz

Annex D

National Cyber Security Incident Emergency Response Plan:
Incident Categorisation Matrix

Severity	Illustrative description of the incident	Possible features	Incident management
LOW	**Incidents with a severity rating of LOW may be monitored but will not trigger an AoG response**		
	Span: The incident may have an impact on the information infrastructure of one or more government agency, NGO or private entity of national significance. **Resolution**: The impacted organisation is assessed to be capable of resolving the incident independently, or with minimal external support.	**Technical impact**: There may be limited impact on discrete parts of the organisation's information infrastructure. **Impact on Service Provision**: There are no, or minimal, disruptions to service delivery. **Communications**: There is no, or minimal, public awareness of the incident. There is no, or minimal, media interest. **Second and third order effects**: There are assessed to be no, or minimal, second and third order effects.	**Operational Lead**: The impacted organisation retains the lead for resolving the incident. **Policy Lead**: AoG policy coordination would not usually be required for an incident with a severity rating of LOW. **Additional Support**: CERT NZ, NCSC or the Police Cyber Crime Unit may be requested to provide subject matter expertise to the impacted organisation. When appropriate, the organisation may be referred to an alternative source of assistance or advice. **Communications Lead:** communications will typically be led by the operational lead. **Coordination Measures**: Incidents will be reported as part of routine reporting. CERT NZ, the NCSC or NZ Police will coordinate the government response if required.
MEDIUM	**Incidents with a severity rating of MEDIUM may be monitored but will not trigger an AoG response**		
	Span: The incident has a limited impact on the information infrastructure of one or more government agency, NGO or private entity of national significance. **Resolution**: The impacted organisation is assessed to be	**Technical impact**: There is a limited impact on discrete parts of the organisation's information infrastructure. **Impact on Service Provision**: There are no, or minimal, disruptions to service delivery.	**Operational Lead**: The impacted organisation retains the lead for resolving the incident. **Policy Lead**: AoG policy coordination would not usually be required for an incident with a severity rating of MEDIUM **Additional Support**: CERT NZ, NCSC or the Police Cyber Crime Unit may be requested to provide subject matter expertise to the impacted organisation. When appropriate, the organisation may be referred to an alternative source of assistance or advice. **Communications Lead:** communications will typically be led by the operational lead.

Severity	Illustrative description of the incident	Possible features	Incident management
	capable of resolving the incident independently, or with limited external support.	**Communications**: There is no, or minimal, public awareness of the incident. There is no, or minimal, media interest. **Second and third order effects**: There are assessed to be no, or minimal, second and third order effects.	**Coordination Measures**: Incidents will be reported as part of routine reporting. CERT NZ, the NCSC or NZ Police will coordinate the government response if required.
HIGH	**Incidents with a severity rating of HIGH may require a coordinated AoG response to achieve resolution**		
	Span: The incident impacts the information infrastructure of one or more government agency, NGO or private entity of national significance. **Resolution**: The impacted organisation(s) will require a range of support measures varying from technical advice to operational intervention.	**Technical impact**: There are detrimental effects on information infrastructures and dependant services. **Impact on Service Provision**: Service delivery may be impeded or even stopped temporarily. **Communications**: The public may be aware that an incident is occurring. Action may need to be taken to retain confidence in government's ability to contain / resolve the incident. There may be media scrutiny of the handling of the incident. This scrutiny will intensify in proportion to the time taken to achieve a visible resolution or as a result of attribution concerns. **Second and third order effects**: There may be wider, but limited, detrimental implications for national interests: economic, security, public health and safety, confidence in government, and international relations.	**Operational Lead**: NCSC, NZ Police or CERT NZ will lead the operational response to the incident **Policy Lead**: NCPO may, in consultation with other government agencies, coordinate an AoG policy response to the incident if required. **Additional Support**: Other agencies or entities may be requested to provide subject matter expertise to the impacted organisation(s). **Communications Lead:** communications will typically be led by the operational lead or determined by a Cyber Incident Coordination Group if convened. **Coordination Measures**: Subject matter expertise from the policy, communications and technical fields may be drawn upon as required. A Cyber Incident Coordination Group may meet to manage the government's initial response to the incident if additional (to agency led) coordination is required. A Cyber Incident Coordination Group will draw on subject matter expertise from the public and private sector as required.

Severity	Illustrative description of the incident	Possible features	Incident management
CRITICAL	**Incidents with a severity rating of CRITICAL are designated as cyber security emergencies. They typically require a coordinated AoG response and extensive support to achieve resolution**		
	Span: The incident solely, or in combination, severely impacts the information infrastructures and services of a government organisation, numerous government organisations, a private entity of national significance, or numerous private entities of national significance. **Resolution**: The impacted organisations will require extensive support varying from technical advice to operational intervention. The incident is complex, potentially difficult to contain, and there is significant uncertainty associated with it.	**Technical impact**: Critical information infrastructures and services are severely disrupted or have stopped functioning. **Impact on Service Provision**: Service delivery is severely impeded or has been stopped. Government decision-making and those services critical for the functioning of national security, law and order or public health and safety, have either solely, or in combination, been heavily disrupted. **Communications**: Public, business, and foreign investor confidence may be shaken. NZ's international relations or reputation is threatened. There is intense media scrutiny. **Second and third order effects**: The emergency has significant detrimental implications for national interests: economic, security, public health and safety, confidence in government, or international relations.	**Operational Lead**: The National Security System will identify the operational lead for the incident (typically the NCSC). **Policy Lead** : NCPO will coordinate the AoG policy response to the incident in consultation with other government agencies. **Additional Support**: Agencies will be requested to provide subject matter expertise to the impacted organisation(s) as needed. External support may be required from the private sector to resolve the emergency. **Communications Lead:** The National Security System will identify the communications lead for the incident. **Coordination Measures**: The National Security System will be activated and a Watch Group established. ODESC and NSC will also meet if required.