Re-connecting to the Digital Health Ecosystem – June 25 2021

Document purpose:

To communicate the WDHB's intent and understanding of risk associated with the proposed reconnection to the wider Health sector and seek understanding and acknowledgement of this from the MoH as a key stakeholder to the approach outlined in this document.

It is noted that specific communication and agreement will be sought in addition from the relevant party 9(2)(k), 9(2)(c) [redacted] This is to be included as part of the change process for each service. The approach proposed, does not seek a blanket or unilateral approval for services that are not controlled by the WDHB, nor seeks to transfer risk to those parties.

The approach is proposed on the basis that the controls are sustained and agreed actions are completed within the timeframes committed.

Approved by: 9(2)(k) [redacted]

____

Acknowledged by: 9(2)(k) [redacted]

____

The problem statement

As the DHB has brought servers and the application services online internal to the DHB within in a "Hard Shell", the high-level of dependence of the application services upon external websites and external digital services has become apparent. Most services are now not considered clinically viable without connectivity.

The time and complexity to understand each service in detail, explore risks, and propose and implement solutions to reduce risk would significantly delay the restoration of clinical services – for both the WDHB and other DHB's that depend upon the digital and clinical services that the DHB provides.

The risks are a mix of previously known and unknown, however, the urgency to address them and the magnitude has been amplified by the cyber-attack. There is no simple way to short-cut the analysis, nor in many cases develop viable alternatives in the short-term.

These technical risks are contrasted against the increasing patient risk relating to timely access to services, results and reports and staff risks associated with fatigue and manual processes due to the lack of integration or fully functional integrated applications within the "Hard Shell".

The ATO and the "Hard Shell"

As part of its Authority to Operate ('ATO') on the 11th June 2021, the Waikato DHB agreed to adopt a "Hard Shell" approach for the restoration of its digital services.

The "Hard Shell" is to protect the WDHB, its patients and staff and the wider health system by maintaining minimal connectivity with other entities via the internet or proprietary networks such as 9(2)(k)

This was proposed and agreed on the assumption that this state would be maintained for approximately a month, over which time, improvements would be made to further strengthen the DHB's security (of which work remains ongoing).

Since this time as the DHB has worked to restore more of its systems following the ATO, the level of digital co-dependence with external health providers and the dependence on the Waikato DHB by other DHB's (for example 9(2)) has been brought to the surface – highlighting a significant issue for the DHB to address; the ability to sustain the "Hard Shell" given the now apparent and increasing clinical risks associated without having the previous restricted levels of connectivity. After nine days of use of 9(2)(k) applications in a degraded state, networked services that were considered peripheral at launch are now better understood and considered critical given manual processes and overall organisational fatigue.

The Waikato DHB also hosts a number of services for other DHB's such as 9(2)(k)

Examples of services that are dependent on connectivity include the Waikato's 9(2) (k)

Further there are now 9(2)(k) that are considered essential for clinical services. As work progresses, more and more web sites are surfaced.

9(2)(k), 9(2)(c)

9(2)(k), 9(2)(c) [redacted]

Proposal

Given the controls implemented and the ongoing work to refine and further strengthen those controls, a balance of cyber risk against patient and employee safety is sought associated with the prolonged outage and disconnection of application services.

On balance, it is not considered feasible to assess each and every service upfront, nor likely that changes to mitigate risk are able to be achieved in a reasonable time period (for example many firewall restrictive controls breach contractual agreements for use).

It is therefore proposed to address the WDHB connectivity needs (all subject to post-incident security controls and technical change control). 9(2)(c), 9(2)(k), 9(2)(e) [redacted]

9(2)(c), 9(2)(k), 9(2)(e) [redacted]

The overall objective is to progressively restore health network services to the status prior to the event and strengthen where required. Note that this strategy is to be read in conjunction with the risk section of "Reconnecting to the Digital Health Ecosystem_Technical Risks.docx".

Specific actions:

9(2)(k), 9(2)(e), 9(2)(c) [redacted]

9(2)(k), 9(2)(e), 9(2)(c) [redacted]

Related activities and considerations include:

- In parallel, review each service to assess its risk, propose and consider effective treatments for those risks and implement in a considered manner – 9(2)(k), 9(2)(e), 9(2)(c) [redacted]

9(2)(k) [redacted]

9(2)(k), 9(2)(e), 9(2)(c) [redacted]

- 9(2)(k) [redacted] This action is with the Director of Business Services.

- 9(2)(k), 9(2)(e), 9(2)(c) [redacted] This action is with the Director of Business Services.

- 9(2)(k), 9(2)(e), 9(2)(c) [redacted] Action with CISO and Director Business Services.

Conceptually this is all represented in the following diagram:

9(2)(k), 9(2)(e), 9(2)(c) [redacted]

Risk position
As part of the ATO, the DHB has adopted several controls to manage and reduce cyber and continuity risk.

The technical controls include the below. We are working with our response and assurance partners to ensure the effectiveness and coverage of these controls.

9(2)(k), 9(2)(e), 9(2)(c) [redacted]

9(2)(k), 9(2)(e), 9(2)(c)

[redacted]

Although no evidence has been found within the Medical network of malware or the actor having traversed into this network, the WDHB cannot categorically discount this

It is noted however, that there has been no evidence found to date of residual malware, nor of the Cyber Actor being resident in the network. We are monitoring for any re-emergence of known indicators of compromise.

There also has been no evidence found of a breach into the medical networks from the corporate networks. It is noted that the Cyber Actor appears to only have gained access to the corporate network, not the beyond into the medical network. It is noted that forensic activities are ongoing and as more analysis is conducted the understanding may change.

The controls have also highlighted the many points of interconnection with the rest of the health sector and the deep clinical integration.

It also as expected has highlighted risks associated with the nature of the inter-connectivity, particularly associated with the medical domain, which operates in a high trust mode across the sector. This has also shown the material amount of engineering required to achieve acceptable levels of connectivity and risk associated with these legacy services (for example reducing ports and connectivity).

The challenge that is being worked through is many of the digital services were implemented and designed to operate in closed and highly trusted networks. Most of these solutions were implemented many years ago and carry with them the residual risks associated with the cyber security practices of the time

All take time to understand and explore and adopt feasible constraints. Technical solutions may cut across commercial and certifications in place.

Risk statement summary: We are opening up network connectivity, as such we are expanding the present narrow attack surface.

Risk summary

The overall objective of the actions proposed above is to allow the organisation to move forward, balancing cyber-risk, employee / contractor fatigue, and patient safety.

9(2)(k), 9(2)(e), 9(2)(c)

[redacted]

We note that for each risk a detailed analysis and workstream related is committed by the WDHB to assess and address the specific risks within each category below.

9(2)(k), 9(2)(e), 9(2)(c)

[redacted]

9(2)(k), 9(2)(e), 9(2)(c)

[redacted]

9(2)(k), 9(2)(e), 9(2)(c)

[redacted]

9(2)(k), 9(2)(e), 9(2)(c)

[redacted]

9(2)(k), 9(2)(e), 9(2)(c)

[redacted]