May 2021 Waikato District Health Board Cyber incident response – key learnings from the InPhySec analysis

The Privacy Foundation's Hauora Health Privacy Working Group has considered the final published independent report that examined the incident and assesses key learnings. These comments are focused specifically on the independent report that Manatū Hauora | Ministry of Health was instructed to commission.

Further, at the direction of the Minister of Health, Te Whatu Ora subsequently publicly released sets of documents that provide the briefings and situation reports in relation to the incident. The Working Group separately considered those documents, assessing the privacy insights.

Background-

The Waikato District Health Board's ((Waikato DHB) now Te Whatu Ora | Health New Zealand Waikato District) information systems were affected by a cyber security incident on 18 May 2021. The incident, through a ransomware attack, had widespread impact, and met the threshold for serious harm under the notifiable data breach provisions of the Privacy Act 2020. Sensitive and identifiable personal health data of patients (and other sensitive information of Waikato DHB staff) were released into the public domain on the internet impacting affected individuals' privacy.

An independent report was commissioned to review what occurred and provide advice for future mitigation and response. Recommendations were largely directed to the then newly established Te Whatu Ora and its current and future health data ecosystem.

The final report[1] (version 0.5) authored by InPhySec Security, was released in September 2022. The report writers are cyber and information security consultants, rather than privacy specialists. Although not unexpected in this context, we argue that privacy expertise should still have been included in any post-incident review as personal and health information considerations cannot be ignored.

Significant sections of the report are redacted, and information is withheld under the Official Information Act 1982. This presents limitations in our fully understanding what occurred and how and gaining certain insights on agency and system wide response. In this commentary, we set out details on certain findings of note and consider the implications for the health sector.

Privacy in the context of the final report-

How privacy was managed in the incident was specifically excluded from the scope of the report - the focus was on the IT impacts. This obviously leads to limitations in a health information privacy context. We believe the privacy dimension should still be incorporated in the post incident review. In collecting, managing, and protecting personal health information, it is critical that privacy and confidentiality, and the reconciliation of security and privacy interests, are considered by Te Whatu Ora.

Whilst there was no reference made to the Health Information Privacy Code 2020, some attention was paid to Information Privacy Principle 5 of the Privacy Act 2020 in the overall writing of the report, with the intention that the security recommendations made were fit for purpose and would reasonably operate "*in a manner consistent with the Act's provisions".* The comment was made "*that balance between security and thus privacy on the one hand, and effective clinical services on the other turns out to be a central question in this case*."

[1] WDHB-Final-Report-2.0-redacted.pdf (tewhatuora.govt.nz)

Privacy was specifically mentioned when looking at the consequences of the release of data and information to the media under the incident. The report writers considered whether there was merit in Te Whatu Ora seeking to engage with the Office of the Privacy Commissioner (OPC) to develop a Code that would help guide a response to significant disclosure events but concluded this would not be necessary as the Privacy Act gives the OPC "*sufficient scope to both respond and to support Te Whatu Ora as required".*

While privacy was out of scope overall, its inclusion in the report here reflects the breach notification and response obligations that the Privacy Act 2020 could trigger in in the event of an IT or data breach. Engagement with the OPC was deemed unnecessary because of the powers OPC could invoke under the Act.

When assessing the media response (which involved both Manatū Hauora and Te Whatu Ora) it was explicitly noted that taking an overly optimistic stance must be avoided. Commentary and briefing to the media need to be realistic about the situation, recognising that more often than not the response, recovery and restoration phases can take far longer than expected and new issues invariably arise.

This is relevant also to Privacy Act 2020 section 117 requirements for notification with respect to affected individuals - considering the content of what needs to be included in a breach notification to the public to explain the steps taken, or intended to be taken, by the agency in response to the privacy breach.

PwC review of Ireland's HSE incident

The Waikato DHB report was prepared within the context of Ireland's healthcare system as it had been affected by a similar cyber incident. The Health Services Executive (HSE), providing Irish public health services including secondary care in hospitals, was subject to ransomware attacks in May 2021. In December 2021 the HSE released a report[2] from PwC following an independent review.

The report specifically commented that the HSE situation highlighted common themes with the Waikato DHB experience. These included:

- Teams that included cybersecurity in their remit were under-resourced.
- Technology growing organically and becoming overly complex.
- The importance of effective security monitoring capability to detect, investigate and respond to security alerts.
- Testing of cyber incident response plans.

Comments on the report's recommendations -

Recommendations for Te Whatu Ora were provided intermittently throughout the 51-page report in bold text. They were not presented in summary form at any point to support understanding. Neither were there indications of whether each of these recommendations (or the issues identified) were agreed or accepted.

Despite this, we note in the concluding section recommendations were broadly grouped into four categories – architecture, keeping up to date, active defence and practice.

Below we highlight and summarise certain recommendations that we believe Te Whatu Ora should be committed to action, with an undertaking to keep the public informed of progress. In some cases, we provide additional comment and/or further recommendations.

[2] conti-cyber-attack-on-the-hse-full-report.pdf

1. *Cyber Security Incident Response Plans should be tested and regularly practised*

It was noted that the Waikato DHB had an IT incident response plan with clear roles and responsibilities, but it had never been tested in a practice environment.

It is critical that all organisations actively test and regularly practise incident plans over time to ensure they are adequate for the current digital environment and cyber risk threat landscape. It is also necessary to support internal respondents in their management of any incidents.

2. *System wide response planning and approach – test, train, and practise at a national level*

The report commented that Te Whatu Ora needs to be able to respond to future incidents/events seamlessly, drawing upon multiple national resources. Incident response plans should consider occurrences or impacts at a national level, and test, train and practise accordingly.

Waikato DHB had a Co-ordinated Incident Management System (CIMS) arrangement consistent with the New Zealand wide, all-of-government approach to command, co-ordinate, and control incidents. The report found that while the CIMS structure appeared to work well, it lacks an IT/cyber element. It recommended that CIMS be updated to include the digital environment.

We strongly urge this recommendation be accepted and actioned promptly. Appropriate consideration for IT and cyber factors (including ransomware) would be prudent given the rise of online and cyber incidents in the New Zealand environment. We note the OPC has reported the increasing impact these have had on reported privacy breaches that have met requirements for mandatory notification.[3]

There should be commitment to completing at least one system-wide test per year, to support tests against current likely risk events. An assessment of the ongoing effectiveness of these tests should be reported and evaluated with all relevant system entities.

3. *Security of legacy systems – dependent on "high trust" environments*

A comment was made in the report that "*there are a lot of legacy systems in use that are important but have low security (they're often referred to as being in 'high trust' environments). High trust is good for people but not for IT as the trust level has, invariably, not been validated. As Te Whatu Ora integrates and consolidates, it will want to ensure it does not inadvertently create a larger and more attractive target, in particular by making assumptions with respect to trust*."

We note that current cybersecurity trends are recommending 'zero-trust' models as good practice, and we comment on this further below. In general, we believe the continued dependence on 'high trust' of internal and external users within the broader environment of Te Whatu Ora's health data ecosystem is not protective. It will increasingly threaten New Zealand's health system and infrastructure, the resilience of its health services and the security and privacy of personal health information.

[3] https://www.privacy.org.nz/publications/statements-media-releases/notable-increase-in-data-breaches-reported/

4. ***Information Classification Systems should be implemented to inform information management***

A recommendation was that there should also be an information classification system from the outset, with associated governance and protection guidelines and a framework for the storage and management of different kinds of data. We note this recommendation was limited to an information classification system, without explicitly recommending a corresponding controls framework to support the management and security of information.

Therefore, we further recommend that Te Whatu Ora extends the scope of this action to implement an information classification and controls system. This should include guidance or any requirements for the use of encryption, password policies, multi-factor authentication, service provider requirements (e.g. ISO certified), role based access controls, retention policies, staff and contractor training and other due diligence assurances etc.

5. ***Mandated Logging and Monitoring should be implemented across systems***

The report was clear that logging and monitoring for possible threats and attacks should be mandated across Te Whatu Ora systems, including those that are legacy – "*As the Te Whatu Ora data ecosystem becomes more integrated, the risks arising from cyber intrusions grow, and so defences need to be taken ever more seriously. For logging, secure systems must be built that can ingest information relevant for security teams, without also taking in sensitive information*." Logging and monitoring would support incident forensics and inform responses. It is expected that this also includes use and functionality to support proactive awareness and investigation of possible threats in a timely manner.

6. ***Demilitarised zones (DMZ) and Segment networks should be considered for implementation***

A DMZ network provides a buffer between the internet and an organisation's private network and acts as an extra layer of security. The comment was made that "*The complexity of health data systems mean segmentation will always be complex and difficult to enable proactively. But the benefits are very real."*

The report recommended Te Whatu Ora should be looking at the use of DMZs and other forms of network segmentation to reduce the impact of compromise***.*** Increasingly, segmenting networks is considered good and necessary practice, and we are therefore of the view that this should absolutely be implemented. We expect this would be a good step towards supporting a zero-trust approach.

7. ***Access and Authentication – consider multi-factor authentication***

It was considered that there was a real opportunity for Te Whatu Ora to look at new technologies for multi-factor authentication within the specific context of the clinical environment, so that the right operational fit is found.

We strongly agree with this recommendation and believe it needs critical focus. At minimum, multi-factor authentication should be implemented, not just considered.

8. Cyber Security Skills capability – build and maintain

The report found that it was essential that Te Whatu Ora has its own capability to respond to incidents. It was recommended that Te Whatu Ora should, as a priority, build and maintain "*a national skills capability (perhaps as a centre of excellence) for health-related security expertise."* We recommend this is continuously assessed with a KPI(s) that Te Whatu Ora proactively measures and reports against.

We expect the action of this recommendation to extend beyond IT roles to those responsible for incident response. It should include capability of all staff and users who may have a role in interacting with systems and supporting incident responses. Over time as capability grows, front line staff can then be supported to understand their role in incident response and what is required of them by the incident response team.

Lessons for the Wider Sector detailed in the report-

Towards the end of the report, some advice was provided for the health sector. It was underscored that a significant cultural shift needs to occur with these:

- Logs and monitoring are of limited use if there is no permission or requirement to act 'in the moment' on an alert of a possible issue. IT teams need to be empowered with the authority and ability to act even if it means there will be disruption to services. The report observed that IT security and the need to act becomes even more critical with national joined up health systems.
- In the event of an incident, the move to a recovery phase needs to be "intelligence-led." This means that the incident response leaders can use the information they have to make assessments and draw inferences about the possible behaviours of malicious threat actors and make the call for recovery and restoration of systems.
- System wide planning for incidents needs to occur, and co-operation needs to factor in and/or require everyone following rules in connected systems and accessing data. The comment was made that "*Without that co-operation, any plan will be dangerously unconnected from the reality of the systems it seeks to protect."*

Our concluding comments-

1. Lack of visibility of incident root cause and response activities

Post incident we are still lacking specific details as to how the incident occurred. Te Whatu Ora commented that whilst it wanted to be transparent, given the risk the malicious actors could target other agencies, details of investigative findings would be withheld. It is disappointing that significant sections of the report were withheld.

Added to this disappointment, the Waikato DHB analysis produced during the incident, "Reconnecting the Digital Health Ecosystem", and described in the independent report *as one of the single most important documents of the incident and required reading for anyone looking to prepare for or manage*

health IT and privacy incidents, was released under the Official Information Act with approximately half of it redacted[4].

Shared understanding and knowledge building is critical to an all-of-sector approach to cyber security. Transparency is also necessary to support accountability and scrutiny with regards to public management of individuals' personal health information. Te Whatu Ora has a real opportunity to be a leader in health information protection, security, and privacy within the New Zealand healthcare environment, and to support other local health sector agencies in a meaningful way.

We recommend that learnings, and approaches to support future incidents, are shared with the public to guide further incident responses in the clinical environment and to give confidence about the management of health information and data in the health sector's infrastructure.

2. Cross team collaboration is necessary for balancing health services – there needs to be an agreed and explicit approach which balances all needs

There is often a tendency to view cyber security as solely the domain or problem of IT teams. However, the final report commented that addressing cyber security and clinical services head-on was a turning point in fully understanding the issues that were faced. It is clear that IT teams cannot do this alone, clinicians are required as well. Everyone needs to be working together to understand what data is required clinically, and the priorities to respond, restore and keep certain services available under pressure. To enable this, both groups must share an understanding of their competing needs and expected activities in the event of an incident.

3. Zero-trust needs to be implemented

Zero-trust security models are increasingly seen as good industry practice. Consideration of the interconnectedness of the systems involved (some of which are now old and legacy) and the health system as a whole is critical.

Zero-trust does not mean there is no trust in the management or users involved with systems. However, it provides another layer of technical support by assuming unintended third parties or threat actors may also try to compromise the same controls and processes that are established for trusted users to interact with the system.

As services become increasingly centralised, interconnected, and dependent on internet or cloud-based technologies, zero-trust considerations must be accounted for. At minimum, we expect this to result in multi-factor authentication across the digital environment and DMZ or network segmentation to limit possible risks in the future.

4. Looking to the future

Operationally, the issue here is getting the balance right between a narrow, segmented span of control with high security and an increasingly wider span which will be operationally efficient, but more costly – and risky - to manage as health reform continues. While we agree there may be no 'right' answer, Te Whatu Ora needs to consider this inevitable trade-off explicitly to provide transparency and assurance to the public.

[4] HNZ00008727 Document for release.pdf (fyi.org.nz)

5. Closing the loop

We would like to see the gap in the report regarding personal health information and privacy addressed. Given the context of the incident and impacts to privacy (which resulted in public release of sensitive health information), we see a post-incident review as incomplete without this. A follow up report should be issued which lists the recommendations from InPhySec, states whether these have been accepted or not and gives details on status and progress.

Addendum –

In June 2023 The Hauora Health Privacy Working Group reviewed the set of documentation released by Te Whatu Ora on 2 March 2023, containing situation reports and Ministerial Briefings on the Waikato ransomware incident between 27 May and 25 August 2021. These documents have been considered with respect to privacy and privacy breach/incident management. We provide summary comment as follows:

Taken together, the documents build up a picture of how the privacy situation evolved in the context of the cyber incident, and the considerations for privacy breach management. It is clear that it took considerable time to understand the full privacy position and identify impacted individuals. WDHB sought specialist privacy and legal advice; close contact and consultation was maintained with the Office of the Privacy Commissioner. A dedicated freephone number for the public to call regarding privacy was established, and IDCARE (an organisation providing identity and cyber support) was engaged for consumers who wanted advice independent of Te Whatu Ora.

As is to be expected, the exact totals of exfiltrated data and impacted individuals (being both patients and staff) are redacted from the documentation. However, the Situation Report of 9 July (located in part 3 of the set of documentation released) stated that of the notifications made to that date, 70% of those had been to staff, and 30% to patients. Further, the 21 July 2021 Situation Report (Part 3) stated that at that point in time, further analysis had identified 24 staff and 2 patients as being at risk of potential identity fraud due to the types of information accessed, and notification had been made to all WDHB staff.

It is clear that notification to impacted individuals, and particularly within the context of the mandatory breach notification regime under the Privacy Act 2020, required careful and nuanced consideration. In the final Situation Report (Part 4) of 25 August 2021 (by which time the incident response was in the recovery phase), the approach to notification was ongoing, however we note that the earlier 6 and 9 July 2021 Situation Reports provide the most fulsome information on the approach that was being taken.

The characteristics of the data had to be assessed, data points mapped to each individual, and risk assessments completed. Data was categorised based on whether it met the threshold of serious harm under the Privacy Act, was subject to a legislative exception to notification, and whether it was low, medium or high sensitivity. Medium or high sensitivity data was to be assessed by clinical teams and a patient notification approach taken from there.

Breach response and management also required a multi-agency approach, with the WDHB working with Police, Government Security Communications Bureau (GCSB), National Cyber Security Centre (CSC), banks, Waka Kotahi | New Zealand Transport Agency, Te Tare Taiwhenua | Department of Internal Affairs, and Te Tare Taake | Inland Revenue Department.

Agencies should reflect on lessons learnt from the WDHB and other recent high profile cyber

incidents, ensuring they have carefully considered and clearly documented their privacy breach response plans. The documented plan should include not only the factors that need to be considered to establish whether notification should be made (mandatory, but also still considering voluntary notification as a matter of good privacy practice) but what the notifications need to contain and how they will be made, as well as capturing key partner agency contact points.