

Investigation into COVID-19 active cases privacy breach

29 July 2020



Contents

| | |
|--|----|
| Introduction | 2 |
| Executive Summary | 2 |
| What caused the incident? | 3 |
| Whether any particular individual or individuals were responsible for the incident? | 7 |
| Whether there is a risk of ongoing breaches or further exposure of the information?..... | 7 |
| Whether relevant policies or processes were complied with?..... | 8 |
| Ministry Policy | 9 |
| ARHT Policy | 12 |
| The effectiveness of, and any improvements to, those policies and processes that might prevent similar incidents in the future | 13 |
| Any other relevant matters necessary to provide a complete report on the above? | 13 |

Introduction

1. Early on 4 July 2020 the NZ Herald reported it had received confidential patient details of 18 confirmed cases of COVID-19 on a spreadsheet with names, dates of birth, age and quarantine location. There was immediate public interest in how and why this sensitive personal information was leaked to the media. Radio New Zealand reported that it had “seen a document that includes the full names, addresses, age and the names of the hotel and one hospital the 18 have been quarantining in.”¹ Other media channels also reported having seen the information.
2. On 6 July 2020 I was appointed by the State Services Commissioner to investigate, make findings and report on:
 - a) what caused the incident;
 - b) whether any particular individual or individuals were responsible for the incident; and
 - c) whether there is a risk of ongoing breaches or further exposure of the information.
3. The investigation was also to comment on:
 - a) whether relevant policies or processes were complied with;
 - b) the effectiveness of, and any improvements to, those policies and processes that might prevent similar incidents in the future; and
 - c) any other relevant matters necessary to provide a complete report on the above.
4. I was not tasked with making findings as to liability of any person but can identify further steps that could be taken. Issues relating to containment of the privacy breach and notification of the affected people were to be considered separately.

Executive Summary

5. Ms Boag and Mr Walker were each responsible for the unauthorised disclosure of this sensitive personal information. Their motivations were political. Their actions were not justified or reasonable. Each acknowledged their error publicly and cooperated fully with this inquiry.
6. The Ministry of Health policy and process in notifying emergency services of active cases was a considered response to the pressures arising during the early stages of the crisis. Whether the policy was appropriate in the circumstances applicable in April 2020 will be the subject of further review by the Privacy Commissioner. The policy and process should have been reviewed once there were no longer cases in the community and the dissemination to emergency services of the personal information ought to have stopped. In any event, there ought to have been better protection over the personal information.

¹ Jane Patterson “Details of active Covid-19 cases leaked in privacy breach”, published by RNZ at <https://www.rnz.co.nz/news/political/420490/details-of-active-covid-19-cases-leaked-in-privacy-breach>, 4 July 2020.

What caused the incident?

7. At 11.40am on 2 July 2020 the Ministry of Health (**Ministry**) sent an email to 14 email addresses associated with emergency services. One of those email addresses belonged to Michelle Boag (as acting CEO of the Auckland Rescue Helicopter Trust (**ARHT**)). The email address was as notified to the Ministry.
8. That email address was Ms Boag's business email rather than an organisational address. Ms Boag was the acting CEO of ARHT and did not have an ARHT email address. Emails sent to the ceo@arht address were forwarded to her business email address. Replies would be sent from the business email address. The Ministry advised that it sent the personal information to Ms Boag's business address because that was the email address provided. Ministry emails contain a footer outlining privacy expectations, prohibitions and actions that a recipient must take if they are not the intended recipient.
9. All agree that Ms Boag received the information in her capacity as the acting CEO of ARHT.
10. The email had the subject line "MEDICAL IN CONFIDENCE – Case Notifications 02 July 2020". It attached a spreadsheet containing confirmed COVID-19 case information as of 9am on 2 July 2020 (referred to here as the **personal information**).² The email stated "only active cases are shown in the report". The Ministry confirmed that the cases in the spreadsheet were identifiable by their full name, date of birth, residential address, and quarantine or medical facility address where they were located.
11. On the same day, Ms Boag forwarded that email (and the spreadsheet) to Hamish Walker, MP for Clutha-Southland. Later that day (and on the next) Mr Walker sent that spreadsheet to at least three media organisations (NZ Herald, Radio New Zealand and NZME).
12. On the evening of 7 July 2020, a day after I was appointed, Mr Walker released a press statement taking responsibility for the release of the personal information to the media. It read:

I have spoken to National Party Leader Todd Muller and informed him that I passed to members of the media, by email, information containing Covid-19 patient details that was given to me by a source.

I did this to expose the Government's shortcomings so they would be rectified. It was never intended that the personal details would be made public, and they have not been, either by me or the persons I forwarded them to.

I have received legal advice that I have not committed any criminal offence.

The information that I received was not password protected by the Government. It was not stored on a secure system where authorised people needed to log on. There was no redaction to protect patient details, and no confidentiality statement on the document.

² I have not viewed the spreadsheet. It was not necessary for the purposes of the inquiry and would constitute a further invasion of the privacy of the patients whose details it contains. I have, however, seen the emails to which it was attached and had independent verification (from those who are authorised to see the spreadsheet) that the document emailed by the Ministry was the document that was sent by Ms Boag and Mr Walker.

By exposing a significant privacy issue I hope the Government will improve its protocols and get its safeguards right.

I made serious allegations against the Government's Covid-19 response and passed on this information to prove those allegations.

Private health information does not have basic safeguards in place and the Government needs to immediately change its protocols and store the information on a secure, safe network that at a minimum requires a password.

I sincerely apologise for how I have handled this information and to the individuals impacted by this. I will be fully cooperating with the Michael Heron QC inquiry.

13. Mr Walker has also communicated with me and provided a statement to me. He advised that he leaked the information in an effort to hold the Government to account and to respond to an accusation of racism. He explained how one of his constituents had informed him about a likely influx of people to the constituency from three countries, which was causing concern because of inadequate facilities and preparation for the influx. On 2 July 2020, he had released a press statement in response to that concern. He later explained to me that the 2 July press statement was:

intended to identify the countries the returning New Zealanders were coming from. The three countries are places in the news as having significant outbreaks of COVID-19. I was aware that at least many of the people would be New Zealand citizens or permanent residents and it was not my intention to highlight the race of the people, but simply their country of departure.

14. The 2 July press statement was met with varied reactions, some (including a government Minister) called Mr Walker racist. He said he found that "extremely upsetting" and unfair. He says his "primary concern was the ability to quarantine a significant number of people in the electorate without the appropriate facilities to do so, not the race or ethnicity of the people."

15. He says that, in his distress, he spoke to Ms Boag. He explained:

She forwarded me the email she had received from the Government COVID-19 email address, together with the attachment to the email from the COVID-19 email address. Ms Boag provided me with this information for me to use in my defence against the accusation of racism.

After seeing her email, I could not believe confidential patient information was being sent to a wide range of people from the Government like a school newsletter with no password protection, no system requiring a secure username and password to log on and access the information, no redaction of patient details to protect privacy, and no confidentiality statement on the attachment itself. I saw this as a major Government flaw that I could expose at the same time.

...

This was the only time that Ms Boag gave me official information that she should not have given to me.

I sent the spreadsheet attached to the email from the COVID-19 email address on to various media people on the Thursday evening (2 July 2020) and the Friday (3 July 2020). I did not supply to the media people either the email from the COVID-19 website to Ms Boag or Ms Boag's email to me.

...

I accept that my judgement was impaired due to the pressure and distress of being labelled a racist.

I accept one of the purposes of sending this information on to media people was to respond, while under distress, to accusations of racism. My intention was to show that my initial Press Release was based on fact and was not racially motivated. However, I accept that the spreadsheet sent on did not prove that point as it gave the names of people and not the places they had departed from, to New Zealand.

I did have an additional purpose of showing the information was not being properly protected by the Government.

16. Mr Walker said to me:

MPs receive all sorts of information on a daily basis, including sensitive information. As I have indicated above, I believe there should be systems in place that make it harder for anyone properly receiving such information to forward it to another person.

With the benefit of hindsight, I accept that once I had seen that data I should have immediately disclosed to the Government that the information had been made available to me.

17. On 7 July and shortly after Mr Walker's press release of the same date, Ms Boag released a press statement stating that she was the source of the personal information sent to Mr Walker.

18. On 10 July 2020, she explained her rationale in the following press statement:

Today I am announcing that I have resigned my membership of the NZ National Party.

The last few days have underscored for me the unhealthy relationship I have developed with politics. For 47 years, I have devoted much of my professional and personal life to supporting the party that for me has always represented the ultimate kiwi values of hard work, reward for effort, self-reliance and compassion. Unfortunately this passion has put me on a self-destructive path. This was confirmed for me as I wrote to Michael Heron QC last night to advise him that towards the end of June I had sent several emails to Michael Woodhouse comprising notification of a small number of then new Covid19 cases. My decisions to share this information were wrong, driven by my distorted view that providing that information would help the National Party to hold the Government to account. In fact it was harmful, not helpful, and it is time that the National Party and I parted ways.

Since joining the National Party at 18, I have tried, sometimes way too hard, to support the Party in any way I could. After resigning as President following the 2002 General Election, I continued to defend and advocate for the Party in many forums, including accepting invitations to provide political commentary. In none of those forums was I the official

representative of the National Party, yet media and political opponents saw my comments as “the National Party” and I in turn felt the need to defend any National Party perspective.

My strong sense of obligation to others has manifested itself in extensive work for charities and individuals in need over many years, but in respect of the National Party, my loyalties have severely clouded my judgement. I was always available to defend, to support and to advocate for the Party and its MPs. I have become an unhelpful distraction in the current political environment. I apologise to all those who have been collateral damage in my quest, both inside and outside the Party and I deeply regret my actions.

I hope my resignation will allow the Party to get on with its vital task of setting out its pathway for New Zealand’s future in the upcoming General Election. The governance and direction of New Zealand, its economic stewardship and the wellbeing of all New Zealanders is the most important issue right now.

I am grateful for the many friends I have made through politics and for their recent support for me personally. Right now, my task is to assist the investigation being carried out by Michael Heron QC and face the consequences of my actions.

I will be making no further comment at this time.

19. Ms Boag received the personal information in her (then) capacity as acting CEO of ARHT (a position from which she resigned in the wake of this incident). It was provided to her by the Ministry and she typically sent it on to two senior clinical leads within ARHT who (when the virus was in the community at least) Ms Boag advised needed it for operational purposes.
20. She confirmed to me that she provided the personal information to Mr Walker on 2 July 2020. As has been stated publicly, the motive for doing so was political. She acknowledged that, in retrospect, her motives and thinking around the disclosure were “distorted”. She said she did not anticipate that Mr Walker would provide the information to the media. Her prompt public acknowledgement of her actions and their consequences, and the constructive approach she took to this inquiry suggest that view was sincere.
21. Ms Boag had earlier provided similar personal information (but different spreadsheets) to Michael Woodhouse, MP. I received information relating to those other occasions from Ms Boag and proactively from Mr Woodhouse. Mr Woodhouse advised he did not forward such information on and has now deleted it. I considered whether I should pursue the deletion further with Mr Woodhouse, but ultimately because the information was similar in nature and it was not central to my inquiry, I determined it was not necessary to pursue it. I accept Mr Woodhouse deleted the information. Ideally, he would have counselled Ms Boag not to disclose such information and/or alerted the Ministry or Minister.
22. The statements of Ms Boag and Mr Walker indicate that the cause of the leak was, first and foremost, deliberate and politically motivated. Both have expressed their sincere regret at their poor judgement in distributing this sensitive personal information to others. I was contacted by a COVID-19 patient to convey their shock and dismay that such information would be passed around in this manner. The Ministry was aware of the risks of unauthorised disclosure of such information and the harm that could be caused. Given its sensitivity, disclosure of such personal information requires clear legal authority and careful judgement (discussed further below).

23. It is not my place to comment on civil or criminal liability. Ms Boag and Mr Walker accept their actions fell below the standard New Zealanders expect. I acknowledge, however, their candour and assistance to this inquiry.
24. Questions have been asked about how and why the personal information was being distributed and why Ms Boag and Mr Walker were able to share it with apparent ease.
25. The personal information was released by the Public Health Intelligence unit in the Ministry in accordance with the policy approved by the Director-General on 14 April 2020. The details of the policy and its application are discussed below.
26. In summary, however, the policy was designed for the circumstances existing in April 2020. The release of the personal information was not appropriate for the circumstances existing on 2 July 2020. For reasons discussed below, the policy and the practice of sending of such emails required reconsideration once cases were no longer in the community.

Whether any particular individual or individuals were responsible for the incident?

27. The discussion above answers that question.

Whether there is a risk of ongoing breaches or further exposure of the information?

28. I am assured by Ms Boag and Mr Walker that no further breaches or exposure will occur. Mr Walker told me:

I have deleted the spreadsheet from my computer equipment. I do not precisely recall the information in the spreadsheet and I have no intention of further exposing that information.

29. Ms Boag advised that she has retained material relevant to respond to this inquiry but will destroy it upon confirmation from me that it is no longer needed. I will confirm that to her.
30. The media who received the spreadsheet have not published any identifiable information. I asked to discuss the incident with the NZ Herald reporter concerned and she declined. I did not pursue discussions with other media outlets as there seems minimal (if any) risk of publication or retention of the information by them.
31. Given that the Ministry has suspended its dissemination of patient information in the manner used on 2 July 2020, it appears there is no significant risk of further disclosure.
32. Upon notification of the leak, the Ministry asked those emergency services that had been receiving the personal information whether they continued to require it and if so, to explain what the data was being used for.
33. At the time, Ms Boag responded for ARHT, saying:
 1. If the data is confined to border cases only it is not necessary for ARHT to receive it.

2. If there are outbreaks or clusters in the community we do need to receive the location data because of our need to be prepared.
34. Ms Boag advised, based on the feedback received from the ARHT clinicians, that in neither case did ARHT need patient names.
35. Other emergency services responded stating that the information had been useful for cases in the community but it was not required now that cases were confined to quarantine situations.
36. In respect to the personal information provided to this group of emergency services providers, there is no material further risk of disclosure because the email circulation has ceased. Whether similar emails are being distributed, or should be distributed in future, is something the Ministry is reviewing before determining the appropriate action.
37. I note that the Ministry is reviewing the handling of all personal information that is sent by the Ministry to other parties for managing COVID-19 cases.

Whether relevant policies or processes were complied with?

38. The leak was committed by motivated individuals knowing they had no entitlement to disclose the information they did. It is doubtful whether any policy (or, potentially, security system) could have completely prevented that.
39. Relevant policies are ultimately derived from the law governing disclosure of such personal information, namely the:
 - a) Health Information Privacy Code 1994 (**HIPC**);
 - b) Privacy Act 1993 (**Privacy Act**); and
 - c) Health Act 1956 (**Health Act**).
40. The HIPC and Privacy Act are central. Each protects the sanctity of personal and health information, save for exceptions allowing disclosure in certain circumstances.
41. Both the Privacy Act and the HIPC make allowances for disclosure where necessary to prevent or lessen a serious threat to public health or safety, or the life or health of an individual. This is the exemption which was relied upon by the Ministry in sending the personal information to the emergency services providers (including Ms Boag for ARHT).
42. The HIPC applies to certain information and certain agencies, including health and disability service providers, among others.³ It applies to the Ministry⁴ and ARHT as an agency and health service provider (and Ms Boag in her capacity as acting CEO of ARHT). Each agency must ensure reasonable safeguards exist to protect personal information and must do everything reasonably within its power to prevent unauthorised use or disclosure.
43. The Privacy Act contains “information privacy principles” that apply to agencies such as the Ministry or ARHT. For the purposes of the Act, “an action done by, or information disclosed to, a person employed by, or in the service of, an agency in the performance of the duties of

³ See cl 4.

⁴ See cl 4(2)(p), and Schedule 1.

the person's employment shall be treated as having been done by, or disclosed to, the agency."⁵

44. The Privacy Act is unlikely to apply to Mr Walker in these circumstances. Section 2 of the Act states that an "agency... does not include... a member of Parliament in his or her official capacity." Mr Walker considers he received and disseminated the information in his capacity as an MP. He says and I accept that he sought to hold the Government to account with respect to the countries from which new cases were originating and with respect to the lack of security around personal information. Mr Walker accepted that the spreadsheet did not assist to prove the first point. In my view, however, Mr Walker was acting in his official capacity.

Ministry Policy

45. In April 2020, during which New Zealand was under Alert Level 4 lockdown, Ministry advisors drafted a policy for the provision of information to emergency services providers. The advisors considered what information should be provided and to whom. The position reached was that emergency services providers (including Police and, crucially, ambulance and rescue organisations including ARHT) should be provided with the personal information of COVID-19 patients, so that their organisations and personnel could be equipped to assist those patients (or those in their proximity) as and when needed.
46. That policy went through the Ministry review process, including legal review and approval by the relevant Deputy Director-General. It was approved by the Director General of Health on 14 April 2020.
47. The policy was a considered response to the pressures arising during the early stages of the crisis, in particular when there was community transmission of COVID-19 and apparent potential for significant community outbreak. The policy was drafted in high level terms and dealt with principles and theory; it did not specify operational processes such as methods for transmission and protection of the information.
48. I have not been tasked with determining whether the policy was appropriate at the time, nor was I able to fully explore the thinking and process behind it in the time available. I have consulted with the Privacy Commissioner and understand he is examining this as part of an open inquiry he is pursuing. It is clear, however, that the policy was a considered one and followed an orthodox, but swift, policy process. It would have benefitted from a requirement for more specific consideration of the prevailing circumstances to ensure the "serious threat" exception (to the requirement for consent) continued to apply at the time any patient information was sent out.
49. The Ministry has not made any changes to the policy, which remained in force on 2 July 2020. Initially, the information sent out related to all COVID-19 cases (active and recovered). At some point, the patient list was refined to include only active cases (as it did on 2 July 2020).
50. On 14 May 2020, Ministry Officials wrote to DHBs and some emergency services providers to "clarify the sharing of personal information about COVID-19 cases to emergency services, district health boards and territorial local authorities."

⁵ See s 4.

51. The relevant correspondence noted that the Ministry was “providing identifiable information about COVID-19 cases” to emergency services providers “to help staff to have all the information they need to take extra precautions”. It advised that the personal information provided “remains subject to the Privacy Act 1993.” It gave recipients guidelines on handling data and information in the COVID-19 context and advised recipients to only share as much information as reasonably necessary and to use anonymous information where practical.
52. It also noted that MPs and mayors had been requesting the information, but that the Ministry did not consider it appropriate to share personal details with them as it was outside “the legal grounds for which information may be shared (i.e. it does not meet the requirements of the serious threat exception or other grounds).”

53. The background to the policy states:

One particular mechanism (under both the Privacy Act 1993 and the Health Information Privacy Code 1994) that permits personal information to be shared in the context of the COVID-19 response is the “serious threat exception”, which allows for the use or disclosure of information to prevent or lessen the risk of a serious threat to individual or public safety, wellbeing or health.

Under this exception, the Ministry of Health (the Ministry) is providing identifiable information about COVID-19 cases directly to emergency services providers (ie, Police, Fire and Emergency NZ (FENZ), ambulance service providers) twice daily. This is to enable personnel to be fully informed and to take extra precautions when dealing with callouts that involve confirmed COVID-19 cases (for example, family violence callouts, medical emergencies).

54. Concerns had been raised earlier by DHBs as to the sharing of such information and whether there was adequate protection and control over the information. The policy paper noted those concerns. The risks of unknown exposure and the potential for community transmission resulting from a lack of communication with emergency services was also noted. The Ministry noted that if information was shared inappropriately, there was also a risk that individuals with COVID-19 could be identified by the general public. It was clear from the policy paper that the Ministry was carefully weighing the relevant considerations.

55. The Ministry policy stated:

There is a clear legal basis for sharing relevant personal information in the context of the COVID-19 response to protect public health. The Office of the Privacy Commissioner advises taking a common-sense approach to how much information needs to be disclosed.

Ministry officials consider that it is necessary to disclose identifiable information on COVID-19 cases to emergency services providers. During this stage of the response, it is important that identifiable information continues to be shared with Police, FENZ, and ambulance providers to combat the spread of COVID-19.

Information provided to other emergency services providers to prevent the spread of COVID-19 remains subject to the Privacy Act 1993. Once identifiable information has been disclosed it is the responsibility of that agency (ie, emergency services organisation) to use it appropriately.

The Ministry has in the past established Memorandums of Understanding (MOU) or similar agreements for situations where there is a regular flow of information to other agencies. Officials did not consider it reasonable to initiate this type of process to formalise the disclosure of COVID-19 information given the urgency of action in the pandemic response.

56. It also discussed the position regarding disclosure of personal information to MPs and mayors:

There have also been multiple requests from members of parliament and mayors for personal information about COVID-19 confirmed cases in their respective jurisdictions to be disclosed to them prior to media announcements. It is unclear for what purpose members of parliament and mayors or other officials at the territorial authority level want to receive this information.

Ministry officials consider that sharing identifiable information at this level is not necessary to prevent or lessen the risk of a serious threat to someone's safety, wellbeing or health and therefore does not meet the "serious threat exception".

57. The Ministry noted that a Health Data and Information-Sharing Governance Group for COVID-19 would meet for the first time in the week starting 13 April 2020. I am informed that meeting took place on 15 April 2020. Future guidance on issues related to information sharing was the remit of this group. That Group considered work on guidance and principles on the sharing of information and data within a COVID-19 context, which was then included in the policy. The Group did not, however, review the policy at any time after the country went to Alert Level 1.
58. The policy document went on to detail the work underway to ensure the internal Ministry processes for sharing information were robust. This included a form to record request details, a checklist for sharing identifiable information and a "Health Information Privacy Code in a nutshell" guide to patient privacy considerations.
59. The policy document noted there was also a process underway in the Ministry to ensure there is a secure method for sharing data when needed (with guaranteed end to end encryption). These security measures do not appear to have been in place before the leak occurred.
60. The Director of COVID-19 Hub, which is responsible for collating and distributing case information to various parties, including emergency services providers, reflected there was some unease with the distribution of personal information when community transmission was no longer occurring. This led to a change in practice, after which the Ministry only listed confirmed COVID-19 cases. The Ministry considered it necessary for emergency services to know where active and confirmed cases were located – even if contained within border facilities – in the event their services were required. The option of not disclosing the personal information does not seem to have been considered at that point.
61. I understand, from the Ministry and from the input that the Ministry received from various agencies, that concerns about keeping frontline staff protected and prepared to tackle the challenges of the pandemic were a key factor behind the decision to allow disclosure of patient information to emergency services. Obviously, all involved were acutely aware of the need to minimise the risk of transmitting COVID-19, and the potentially grave consequences that would follow if transmission did occur. Those concerns were very real.

62. The Ministry has advised that the date on which it considered there was no current community transmission of COVID-19 was on 1 May 2020. After that date, it would appear to me to have been unnecessary (and not permissible) to disclose the personal information to emergency services, because the grounds that the Ministry had been relying on would not have applied. In short, there was no longer a serious threat justifying the non-consensual release of personal information such as this. The Ministry policy was expressed as being formulated in urgency for “this stage of the response”, so it was clearly dependent on the circumstances.
63. The Ministry was, however, dealing with a dynamic global pandemic and operating under huge pressure on many fronts. Whilst there was opportunity, it is understandable that the policy and its application was not reviewed because the situation was so dynamic. Given the risks of unauthorised use or disclosure and the “serious threat exception” relied on, best practice would have been for the Ministry to have discontinued sending the information once that threat had lessened. In any event, the information should not have been sent in such an insecure and open manner.
64. The distribution of such information by email with unencrypted or unprotected attachments does not appear to be reasonable in the circumstances, particularly where widespread community transmission was not an immediate risk. Principle Five of the information privacy principles requires an agency to have reasonable security safeguards and to do everything reasonably within its power to prevent unauthorised disclosure. Rule 5 of the HIPC is to the same effect.

ARHT Policy

65. The relationship between the Ministry and ARHT included a contractual requirement that ARHT comply with applicable privacy laws and policies (as noted in the Ministry policy itself).
66. ARHT’s Policy and Procedures Manual (relevantly) states:

We collect personal information from you when you or somebody else calls 111 and we are tasked to respond, your hospital asks us to transport you, or you correspond with us. We may receive your information from a third party if we consider that circumstances make collecting the information from you not practicable.

...

We collect your personal information in order to:

- I. Identify you.
- II. Provide treatment and care.
- III. Keep you informed about our services and products.
- IV. Seek your voluntary support so that the free service we provide remains available to all in our region.”

67. The ARHT policy also deals with confidentiality. It says that if “employees acquire confidential or proprietary information about the Trust, its business associates or donors, such information is to be handled in strict confidence and not to be discussed with people outside the Trust. Employees are also responsible for the internal security of such information.”

68. Ms Boag's actions in disseminating the personal information would not have been compliant with ARHT policy.

The effectiveness of, and any improvements to, those policies and processes that might prevent similar incidents in the future

69. Each of the 18 named individuals appears to have had their personal information disclosed beyond those it was intended for. There was no justification for Ms Boag or Mr Walker sharing it in the way they did. No policy or process can completely prevent such behaviour.

70. The Ministry is now taking stock of all COVID-19 related information that is sent to external stakeholders, determining the purpose of sending the information, and assessing the mechanisms and security in place. The Privacy Commissioner's inquiry will no doubt inform any review of Ministry policy and process.

71. I have already expressed concern at the routine dissemination of this personal information. If it is required to be disseminated, there should be greater security measures and privacy controls in place to protect against misuse. The Ministry is best placed to determine the optimal method of providing better security over this sort of information.

Any other relevant matters necessary to provide a complete report on the above?

72. Ultimately, any system is vulnerable to the deliberate actions of persons who seek to misuse confidential personal information. My comments about the Ministry should not be taken to suggest primary responsibility on its behalf. Ms Boag and Mr Walker have that responsibility and have expressed their sincere regret for their role in causing this incident.

73. Neither Ms Boag, ARHT nor Mr Walker come under the jurisdiction of the State Services Commissioner. The State Services Commissioner could consider a formal referral of Ms Boag and the ARHT to the Privacy Commissioner, who is the appropriate statutory body in their case. The Privacy Commissioner is, however, already reviewing the question of whether the Ministry policy was appropriate and can investigate this matter with or without a referral or complaint. The Speaker of the House and/or the National Party may have jurisdiction over Mr Walker's conduct, but I do not think the Privacy Commissioner does.

74. In summary, it may be that no further action is required given the circumstances and given the jurisdiction of the Privacy Commissioner (who I have consulted in the course of this inquiry). I am grateful for the invaluable assistance of my colleague Charlotte Agnew-Harington, barrister, and Mr James Jong, Chief Internal Auditor, Ministry of Education.

Michael Heron QC
29 July 2020