Privacy Commissioner
Te Mana Mātāpono Matatapu

Inquiry into Ministry of Health disclosure of Covid-19 Patient Information

Report by the Privacy Commissioner
pursuant to section 13(1)(m) of the Privacy Act 1993

September 2020

Privacy Commissioner
Te Mana Mātāpono Matatapu

Table of Contents

Privacy Commissioner
Te Mana Mātāpono Matatapu

Executive summary

This report is the result of my Inquiry into the Ministry of Health's ("the Ministry") disclosure of Covid-19 patient information to Emergency Services. On 29 July the State Services Commissioner referred the Heron QC report on the disclosure of Covid-19 patient information to me.[1] Having considered the matters in Mr Heron's report I decided to conduct an Inquiry under section 13(m) of the Privacy Act 1993 into the Ministry's disclosure of Covid-19 patient information to Police, Fire and Emergency NZ, and ambulance service providers ("Emergency Services").

This Inquiry is split into two parts, and I have assessed whether:

- The Ministry's disclosure of Covid-19 patient information to Emergency Services was compliant with the information privacy principles and rules of the Health Information Privacy Code 1994 ("the Code") and whether the disclosure infringes or may infringe individual privacy; and
- Police's access to and use of Covid-19 patient information was compliant with the privacy principles and rules of the Code, and whether it infringes or may infringe individual privacy.

This Inquiry is an opportunity to provide observations and feedback both on the Ministry's policy and arrangement of sharing patient information to Emergency Services, and Police's access to and use of that information. While I acknowledge these comments are made with the benefit of hindsight, my hope is that they can inform both the Ministry and Police as further cases of Covid-19 inevitably emerge in the community.

Both the Privacy Act and the Code anticipate and allow for a coordinated approach to information sharing – a clear and systematised process from collection and storage, to use and disclosure (and preventing reuse for any further unrelated purpose).

Findings

I **have found** that the Ministry had a clear and measured rationale for its decision to provide patient information to Emergency Services in April 2020 when that decision was initially made. However, I consider that the Ministry should have revisited its decision as New Zealand began to move down alert levels in May 2020.

I **have also found** that Police had legitimate reasons to collect Covid-19 patient information from the Ministry. However, Police should have reviewed its need for patient information as the prevalence of Covid-19 reduced in New Zealand. Further, while it was appropriate for front-line Police staff to access and rely on alerts related to Covid-19 in the National Intelligence Application ("NIA") to assist with or enable them to carry out their pandemic management or general policing duties, I have **found** that Police's use of that information in disclosing it to agencies as part of Police's vetting function, although in only a small number of cases and for a short-lived period, was inappropriate.

[1] https://www.publicservice.govt.nz/assets/SSC-Site-Assets/Investigation-Report-into-Covid-19-active-cases-privacy-breach.pdf

Recommendations

I **recommend** that the Ministry:

- Ensures it appropriately assesses the application of rule 11(2)(d)(i) of the Code before disclosing health information to prevent or lessen a serious threat to public health, including the consideration that patient authorisation is neither practicable nor desirable before relying on the exception.
- Implement appropriate data minimisation and disclosure practices so that only information that is necessary for the public health response is disclosed to Emergency Services.
- Develop a coordinated plan in relation to the sharing of such information to ensure that all recipients are aware of the risks of releasing information that may lead to an individual being identified and ways in which that can be mitigated.
- Assist health agencies administering Covid-19 tests to ensure people taking tests are told of the purposes for which their information will be used, and the intended recipients, as required by rule 3.
- Implement immediate measures to ensure security of health information when disclosing identifiable details to third parties.
- Develop memoranda of understanding between the Ministry and Emergency Services to set clear expectations about the use of patient information by the recipients.

I **recommend** that Police:

- Implement a process to consistently review and revise its need for Covid-19 patient information, so that its assessment of what information is necessary can respond to changing risk levels and dynamic situations.
- Develop its own internal policy on staff access to and use of Covid-19 patient information.
- Develop a memorandum of understanding with the Ministry in line with its review of its own need for patient information and internal policy.

Background

1. In late February 2020, New Zealand confirmed its first positive Covid-19 case. Very shortly after, the Ministry started receiving sporadic requests from Police and other Emergency Service Providers for details of confirmed cases. The Ministry's initial response was to consider those requests on a case-by-case basis, in a measured and considered way. For example, on 28 February, Police contacted the Ministry's National Health Coordination Centre ("NHCC") requesting the address of the first confirmed case. However, the Ministry responded to the NHCC explaining that disclosure to Police would compromise patient privacy.

2. On 29 February, in an email to the NHCC the Ministry recorded the following rationale for disclosing address information of positive Covid-19 cases to Emergency Services:[2]

> The following is a record of the rationale for the release of the address where the family of the confirmed case is residing to emergency services.
>
> - There is a greater health risk for this group in self-isolation given the nature of the close contact that the family members have had with the confirmed case with the new virus
> - The appropriate preventative measures to prevent spread of the virus is the use of PPE
> - In a situation that emergency services are called to the residence, in order to avert the threat to the officers' personal health and safety, it would be necessary for emergency services to be able to protect themselves using appropriate PPE; this can only be achieved by the sharing of the address information.
>
> No other health information will be shared with the emergency services. Information is being provided to the emergency services so that they can meet their health and safety requirements for the staff. The information will be protected by the emergency providers in accordance with relevant legislation.

3. The Ministry has not provided any detail about why it was called upon to provide this information to the NHCC or what request it was answering. I note that all the correspondence the Ministry has provided to this point, referred only to the disclosure of *address information*. This early approach from the Ministry was cautious, case-by-case and proportionate.

4. In early April, Police began requesting further information from NHCC, specifically about individuals who had died as a result of contracting the virus. On 12 April, a Deputy Director at the Ministry confirmed to Police that the Ministry would "add Police in to the notification protocol to receive high level information regarding Covid-19 deaths (age, gender, location). The individual cases will continue to be notified through the intel process already established."

5. On 12 and 13 April, Police asked the NHCC to include the name of the deceased. Police explained they sought this information for the following reasons (the Ministry's response to each point follows in italics):

> 1. That Police are aware of the death and can respond accordingly if required to reactions by family and the public to the death. This includes assisting with family members who may be attempting to be with the deceased in breach of the Level 4 protocols or to calm community concerns at such a time. *This is no different to current situations – L4 restrictions are in place – with gravely ill and sick people. There are strict no travel protocols in place for deaths and tangi. MoH have massive structures in*

[2] Email from MOH's General Manager Government Relations to NHCC. National.Coordinator/MOH@MOH 29 February 2020 at 11.57am "Rationale for releasing address information to Police and other emergency services."

place with welfare and support and coordinate through the NCMC any compassionate ground travel requests.

2. Police have a significant role in providing reassurance to the community during the Pandemic. The Police approach is focused on maintaining public safety, security and public order, providing assurance and re-assurance while maintaining a prevention first focus. Should Covid 19 deaths start to occur in some specific communities Police having a presence will make a significant difference in ensuring that calm is maintained.

3. Being able to provide victim support processes. *MoH have this well in place. Not wanting to be trite, but this is not a 'victim' situation and MoH have protocols in place specifically for this.*

4. That the Police Executive are informed in a timely manner (prior to hearing it via the media).

Please note that all Covid 19 confirmed and probable cases are entered onto the Police NIA database for three months from date of advice as a staff safety perspective for all emergency services. In order to have this entry cancelled as soon as practicable the advising of the personal details for this purpose only would be beneficial for all concerned. *The bubble for the deceased still remains.*

The point being how can we respond to a family if we don't know the family name. I note the last paragraph would be taken care of through the death notification process regardless although if it's not a coroner's matter this could still take some time. *The family will be immediately advised by MoH of the death – so they already have the information of the death.*[3]

6. The NHCC explained to Police *"If you believe the information agreed to at exec level – which is currently being provided is insufficient, then this will need to go higher up the chain from your side."*[4]

Decision to release identifiable patient information to Emergency Services

7. Through March and April, the scale of the Covid-19 pandemic had become evident, and the Ministry changed its approach with regard to requests from Emergency Services for regular updates. Ministry officials prepared a memorandum on the sharing of information, which was reviewed and agreed to by the Director-General of Health on 13 April ('the memorandum').[5]

8. The memorandum indicates that the Ministry considered it was necessary to disclose identifiable information about living individuals who had tested positive for Covid-19, on the basis the disclosure was necessary to lessen or prevent a serious threat to public health. The Ministry was now providing identifiable information about Covid-19 cases to Police, Fire and Emergency NZ, and ambulance service providers ("Emergency Services") and District Health Board's ("DHB") twice daily. I understand

[3] Emails between NHCC Liaison Officer, and MOC Manager at Covid-19 Major Operations Centre dated 13 April 2020 "RE: Death notification protocol."
[4] As above.
[5] The memorandum is attached as Appendix 1.

that around this period, the Ministry also established its Data and Information-Sharing Governance Group for Covid-19.

9. During this time, the Ministry was also receiving pressure from Local Authorities and Members of Parliament seeking identifiable information about individuals who had tested positive for Covid-19 to understand the extent of the disease in their communities. The Ministry appears to have (appropriately) resisted these pressures.

10. I received a statement from a member of the public, which highlights the risk of disclosing patient information in an uncoordinated way:

> Statement for the Privacy Commissioner
>
> I am not one of the cases that had their identity revealed to the media that sparked the need for this enquiry. However, I contracted Covid 19 and myself and my family were identified due to the way the cases were reported and we have experienced harm and distress from this. I believe I can provide some insight into the consequences of a Covid patients privacy being breached. We were absolutely appalled to know that a list of patients had been released to the media and others. We know that at some stage we would have been on one of those lists and we did wonder who had accessed our information and what was in place to make sure that only people who absolutely needed [access] to case details had it. We would never want anyone else to experience what we have been through and still continue to go through. We are still very traumatised by what happened to us and reading about the leaking of details of cases was difficult for us.
>
> Confidentiality
>
> After I was advised of my positive test, when speaking to the person from Public Health, I was genuinely concerned that I would be identified and was assured that my specific town would not be released.
>
> It was known that one of the cases was connected to the Hereford Conference Cluster. We live in a small community, and we are the only Hereford Breeders. This resulted in easy identification. I was absolutely devastated that my location had been released. The rest of my family were also very distressed. The night of the briefing, our phone started ringing and people were asking us if we had the virus. People who were worried about being in contact with us also rang us in a panic and some were terrified they had caught the virus off us.
>
> We were advising people to call Healthline, but it was difficult to get through. All of our close contacts had been traced, and actually none lived in our town. My extended family started to get phone calls from people who didn't want to ring us directly but had heard that I had it. We have a local community Facebook page which had some really unkind stuff, examples being "we need to know where this person has been" "Send them overseas" along with many people tagging others and making comments about it being in their area. I was devastated. This was all happening while I was really sick and we were struggling to deal with that, and we certainly didn't need the community at large to know before we had a chance to get our heads around it. As an acquaintance from another region said, "When I heard it was a case in your town, and it was a Hereford Conference case, it didn't take a rocket scientist to work out who it was."

> Due to social media vitriol and the fear in the Community, we were in a difficult position when it came to get groceries or go to the pharmacy. My daughters were officially recovered the earliest however we did not feel it would be safe for them to go to the local shops as we believed they would be subjected to backlash – small town, everyone knows who you are. We rang our local police officer to ask for permission to travel to the next town to purchase our groceries there. We made the 110 km round trip there. We did try to get online delivery, not easy here.
>
> I officially recovered in April; I couldn't bring myself to go into the local shops until late May. I was too scared of the reaction. The first time I went, I counted five occasions where I was stopped and asked about Covid. Most people are trying to be caring, but I find it overwhelming and intrusive. Every time I go, without fail, I'm asked about it and I avoid going out locally unless I have to.
>
> Even in other towns or if I run in to people who vaguely know me, they come up and ask me. Often, they feel the need to tell me about the complications they have read about covid, recently in one day I was asked by two people if I had heart problems or post viral syndrome.
>
> For me, the choice of who I told, and when, was taken away from me. And I cannot express enough how traumatic and stressful that was. People who we would have told personally found out through other sources.
>
> Covid shouldn't have stigma, but from our experience, it most definitely does. I have had medical appointments cancelled when they have found out I have had covid, even though I'm recovered. I haven't been allowed to go inside the medical centre even when I have been recovered and am seen in the carpark out the back. This isn't private and I have been swabbed twice since recovering and feel like if people notice me out there, they may think I'm still contagious. Some people physically jump back if I for some reason have to advise I have had covid. Dentists, hairdressers have become an ordeal. I just went out of town to see the Hairdresser, so I could go anonymously.
>
> Unfortunately, what has happened to me and my family cannot be undone now, I hope that in time I can feel confident about going to our town again, without being subjected to questions all the time. The fear of this virus and the stigma – albeit unwarranted, means that people diagnosed should have complete confidentiality and it should be their choice as to if and when they tell people.
>
> I do need to state that we also were on the receiving end of some amazing kindness and caring from our community.
>
> Case reporting needs to be done in a way that does not have any potential to identify people. I also believe that emergency services and other organisations do not need lists of every case in NZ, only in their area.

Police's arrangement with the Ministry

11. By late March, Police had set up a dedicated email address to receive Covid-19 patient information from the Ministry. The Ministry and Police established an arrangement whereby each day the Ministry would email a list of all the confirmed (including probable) cases to Police. That list included each confirmed case's name, date of birth and address.

12. On receipt, Police transferred that data into a master spreadsheet, and then uploaded that information into NIA in the form of a note and alert against the affected individual or affected address. Once in NIA, that information became available to all front-line Police staff. The NIA alert was also duplicated on Police Communications Centre's Computer Assisted Dispatch System.

13. Additionally, each week the Ministry would email Police a list of all confirmed and recovered Covid-19 patients. Police would conduct an audit and make changes to its master spreadsheet as appropriate. Once an individual had been classified as a recovered case, Police would expire the NIA alert against that person. Alternatively, the NIA alert would automatically expire three months after it was created.

14. This arrangement remained in place throughout the pandemic response, but some elements were modified at various stages depending on the status of the virus within New Zealand at the time. For instance, when case numbers started to increase, the Ministry would send an updated list to Police (and other Emergency Services) up to twice a day. When compulsory managed isolation requirements were introduced on 10 April 2020, the Ministry also included in its emails to Police the facility the individual was staying at, the date the individual undertook a test, and the date the individual returned a positive result.

15. At no stage did the Ministry and Police enter into or develop a memorandum of understanding between themselves around the sharing of patient information.

Subsequent use of Covid-19 patient information

16. In April 2020. my Office received complaints from individuals indicating that the Police vetting service was disclosing information about patients who had tested positive for Covid-19 to potential employers.

17. On 29 April, I advised the Ministry and Police that I was making preliminary inquiries about the purpose of sharing individuals' health information with Police and Police use of that information within its information systems. As a result of these inquiries, I conveyed to the Director-General of Health and the Police Commissioner some provisional views by letter on 7 July 2020.

The Heron Report and its impact

18. On 30 July, Michael Heron QC published his report following his investigation into the Covid-19 active cases privacy breach. Mr Heron's report found that Michelle Boag and Hamish Walker were responsible for the unauthorised disclosure of Covid-19 patient information to the media. The findings stated that the motivation for each disclosure was political.

19. The Heron Report prompted the Ministry to review its policy and arrangements of sharing information to emergency services, including with Police. At this point, the Ministry reached out to all the Emergency Services to establish whether it still required that information. Police advised the Ministry that, on review, it no longer required this

information at alert level one as confirmed cases were either in managed isolation or quarantine. As such, Police officers were not placed at unnecessary risk of exposure. Consequently, the Ministry ceased disclosing patient information to Police.

20. All NIA alerts that Police hold relating to the first wave of Covid-19 in New Zealand have now expired.

21. Police have not deleted all NIA alerts. If Police obtained information about the Covid-19 status of an individual through its operational deployment rather than through the Ministry, the NIA alert is expired but it remains as a record of Police operational activity. However, if Police created a NIA alert as a result of the information received from the Ministry, and there is no record of Police initiated activity for that individual, the NIA alert has both expired and been deleted by Police.

22. Police have confirmed that the master spreadsheet it holds containing all Covid-19 patient information is password protected and Police will destroy that document at the conclusion of this Inquiry.

This Inquiry

23. The State Services Commissioner referred the matters described in Mr Heron's report to my Office to consider what further action, if any, under the Privacy Act was appropriate.

24. Mr Heron's report raised similar issues to those under consideration in the preliminary inquiry. This led me to widen the preliminary inquiry into the Ministry's disclosures of patient information to Emergency Services more generally.

25. I considered the best approach to address these concerns was under my functions as authorised by section 13 of the Privacy Act and in August 2020, I launched an Inquiry under section 13(1)(m).

Findings and recommendations

26. Having sought and received further information from the Ministry and Police, I consider that while there was community transmission in March and April 2020, the Ministry was justified in providing Covid-19 patient information to Police and Emergency Services. It was necessary that the Ministry move swiftly to take appropriate action for the public health response to Covid-19.

27. I acknowledge Police's concerns that front line staff would contract Covid-19 as a result of coming into contact with people while fulfilling their functions. Considering the impact of Covid-19 on some of Police's international counterparts, these concerns were legitimate.

28. The 13 April memorandum shows a clear and measured rationale behind the Ministry's decision to provide patient information to Emergency Services. It provides an outline

of the issues raised about information-sharing in the context of Covid-19, proposes policy positions on disclosing information on individual cases, and provides a strategy for clarifying the Ministry's position for key stakeholders.

29. Based on the facts as they were understood at the time, I consider that the process set out in the memorandum was understandable and proportionate.

30. However, management of Covid-19 in New Zealand has developed significantly since March and April 2020, moving from an emergency response to a more enduring and coordinated approach. Accordingly, I now **recommend** that the Ministry take the opportunity to review and update its policy of sharing identifiable patient information with third parties for the Covid-19 response.

The Ministry's disclosure of information to Emergency Services

31. The Ministry's disclosure of health information is regulated by the Health Act 1956 (such as sections 22C, 22F and 22H) and the rules of the Code.

32. Authorisation of the individual concerned is a cornerstone of the Health Act and the Code. Both the Act and the Code are anchored in the same public policy that we see across the health sector, which reflects the importance that individual autonomy and authorisation is placed at the centre of personal and public health.[6]

33. The autonomy and authorisation focus in the Health Act creates a privacy protective regime, with appropriate overrides in certain circumstances. The requirements of the Code ensure that individuals are kept informed about the nature of the information being collected from them and given advice as to what will be done with it.

34. On 25 March 2020, the Minister of Civil Defence declared a state of national emergency under the Civil Defence Emergency Act 2002, which triggered the operation of the Civil Defence National Emergencies (Information Sharing) Code 2013 ("the Civil Defence Code"). The activation of the Civil Defence Code permitted agencies to collect, use or disclose (to certain agencies) personal information for purposes directly related to the government's management of the response to, and recovery from, the state of national emergency caused by the Covid-19 pandemic. The Civil Defence Code provides a further exception to the collection, use and disclosure privacy principles that can be used alongside (but does not override) any other exceptions in the information privacy principles or codes of practice, or any other legislative authority. The Civil Defence Code expired on 11 June 2020.

[6] See for example Part 3A of the Health Act and section 92D of the Health Act which notes voluntary compliance should be sought before measures are applied to an individual, section 92E which notes that an individual should be informed of measures taken under Part 3A, the Health and Disability Code of Consumer Rights.

35. As the memorandum makes it clear that the Ministry considered its policy as authorised under the (Health) Code, rather than the Civil Defence Code, I have limited my examination to the Code, rather than the other possible sources of authority discussed above.

36. This Code sets specific rules for agencies in the health sector. It covers health information collected, used, held, and disclosed by health agencies and contains rules which take the place of the information privacy principles.

37. The key rule at issue in this Inquiry is rule 11, which regulates the disclosure of health information. Rule 5, relating to storage and security of health information is also relevant, particularly when disclosing information to agencies who are not subject to the Code. Finally, a clear and systematised process for collecting, using and disclosing patient information also requires individuals to know why their information is being collected and for what purposes, and agencies to know how information disclosed to them can be used.

Disclosure under rule 11 of the Code

38. Rule 11 relevantly provides:

> (1) A health agency that holds health information must not disclose the information unless the agency believes, on reasonable grounds…
>
> (b) that the disclosure is authorised by:
>
> (i) the individual concerned; or…
>
> (c) that the disclosure of the information is one of the purposes in connection with which the information was obtained…
>
> (2) Compliance with paragraph (1)(b) is not necessary if the health agency believes on reasonable grounds that it is either not desirable or not practicable to obtain authorisation from the individual concerned and…
>
> (d) that the disclosure of the information is necessary to prevent or lessen a serious threat to:
>
> (i) public health or public safety; or
>
> (ii) the life or health of the individual concerned or another individual…

39. Rule 11 places limits on the disclosure of information. Rule 11 does not oblige an agency to disclose information. Instead it allows disclosure if an exception to the rule applies. However, an agency may decide not to disclose even though an exception to the rule applies. The decision to disclose, when permitted by the rule, remains within the agency's discretion.

40. On Monday 11 July, the Ministry provided evidence to my Office of its considerations and process prior to concluding that identifiable patient data about those who had tested positive for Covid-19 should be disclosed to Emergency Services.

41. This included the memorandum prepared by officials in April outlined above.

42. I note that I originally asked the Ministry about their process of disclosing patient information to the Police on 29 April 2020. The Ministry did not provide the memorandum to my Office until I launched this formal Inquiry.

Authorisation by the individual concerned is not desirable or practicable

43. The exceptions contained in rule 11(2) are only available once an agency has considered whether it is desirable or practicable to obtain authorisation from the individual concerned.

44. Where an agency can reasonably anticipate disclosure of the information it is collecting, it should be open about that with the individual. While it may not have been practicable or desirable to obtain consent at the time the Ministry was sending the list of positive Covid-19 tests to Emergency Services, the Ministry could reasonably have anticipated disclosure to Emergency Services might be necessary at the time it was collecting the information in the first place. As discussed later at paragraph [73], while the Ministry was not necessarily in contact with the patients, or collecting that information from them, it was coordinating the Covid-19 health response and was therefore best placed to provide guidance to frontline health agencies to ensure they were providing good information to patients about the fact their information might be disclosed. This might have included the potential for disclosure to Emergency Services as a purpose for collecting the information when providing information under rule 3. Prior notification under rule 3 can be a source of authority for disclosure, and as discussed further below, consent may not even be required where the individual is given clear prior notice of the purpose or purposes for collection.

45. In the memorandum the Ministry provided to me, rule 11(2) was referenced once in an appendix. The memorandum did not engage with the requirement in rule 11(2) to first consider obtaining authorisation when discussing its application to the disclosure of patient information to Emergency Services.

46. I **recommend** the Ministry ensure it has appropriately assessed the application of rule 11(2) prior to disclosing information in reliance on rule 11(2)(d)(i), including the consideration that authorisation be neither practicable nor desirable.

A serious threat to public health or safety

47. The starting point under the Code is that, even during an emergency, the privacy principles and rules continue to apply. However, the privacy principles and rules in the Code contain exceptions which recognise that other public interests may require personal information to be collected from sources other than the individual, used for different purposes, and disclosed to other agencies.

48. A key exception in an emergency or crisis is whether the use or disclosure of personal information is necessary to prevent or lessen **a serious threat** to:
    (i) public health or safety; or

(ii) the life or health of the individual concerned or another individual.[7]

49. A serious threat means a threat than an agency reasonably believes to be such, having regard to:
    a) the likelihood of the threat being realised; and
    b) the severity of the consequences if the threat is realised; and
    c) the time at which the threat may be realised.

50. A key consideration for ongoing disclosures is that the nature of the serious threat must be kept under regular review to make sure that the use and disclosure of personal information remains necessary to respond to the nature of the serious threat presenting at the relevant point in time.

51. The public health and safety exception does not offer a wholesale licence to depart from the privacy principles for general operational purposes. It is targeted to the particular threat and the necessity of using or disclosing personal information to prevent or lessen that threat. This limits the agencies that can share and receive personal information under this ground only to those agencies who have a mandate or are in a position to address the serious threat to public health and safety. It also limits the personal information to that which is necessary to prevent or limit the threat. Its application is limited to the time period that the threat remains serious.

Serious threat and Covid-19

52. In the Covid-19 crisis, factor (b), the severity of the consequences if the threat is realised, is the dominant factor present. Factor (a), the likelihood of the threat being realised, is also likely present as worldwide numbers of infections increase, raising the risk that individuals returning to New Zealand may be carrying infection.

53. During alert levels 3 and 4, community transmission of Covid-19 presented a clear threat to public health and safety. At lower alert levels, Covid-19 continues to present a significant risk of the virus being reintroduced via New Zealanders returning from countries with high infection rates. This risk is being managed by the government's isolation and quarantine system for returning travellers.

54. The nature of the serious threat presented by Covid-19 is not static and has changed over the different alert levels, however, the overall level of the threat appears to remain high, given the severity of the consequences if the threat is realised. At current alert levels, this exception may therefore continue to be available to certain agencies in appropriate circumstances if the use or disclosure of personal information is necessary to prevent or lessen such a threat.

[7] From 1 December 2020, the exceptions to the collection principle will be expanded to include collection necessary to prevent or lessen a serious threat to the life or health of the individual concerned or any other individual.

The Ministry's reliance on the memorandum in April 2020

55. I am pleased to see that the Ministry received and engaged with advice about the appropriateness of reliance on the serious threat exception. Although it does not address whether it was not practicable or desirable to obtain authorisation for the disclosure, the memorandum clearly demonstrates that the Ministry carefully considered whether it should be disclosing identifiable patient information and to whom. For instance, the Ministry considered it necessary to provide such information to Emergency Services to combat the spread of Covid-19 (given there was a risk that Emergency Services would be exposed to risk) but did not consider, in my view correctly, that providing it to Members of Parliament or officials of territorial authorities met the requisite threshold for disclosure. Therefore, in the context of dealing with an emergency situation during an emerging pandemic, I consider the Ministry's reliance on rule 11(2)(d)(i) in April 2020 was reasonable in the circumstances, subject to a caveat regarding my comments regarding authorisation by the individual set out at paragraphs [43] – [46] above.

Need for ongoing review of settings to ensure that disclosure is necessary and proportionate

56. However, as indicated above, I consider the advice could have been more fulsome and nuanced in respect of the requirement that authorisation be neither practicable nor desirable (for instance, if an individual is too unwell to consent, authorisation is very likely to be refused, or the information needs to be disclosed very quickly). I also consider the advice could have engaged further with what specific information was necessary to be sent to which Emergency Services.

57. Rule 11(3) says disclosure under subrule (2) is permitted only to the extent necessary for the particular purpose. As the situation evolved, and the Ministry was receiving better information, it was required to turn its mind to the proportionality rule 11(3) mandates. For example, whether an Emergency Service provider without medical expertise, such as the Fire Service, required any information beyond the address of a positive case.

58. The establishment of the Data and Information-Sharing Governance Group for Covid-19 shows the Ministry's recognition of the need for continuing review in this area. However, there is no mention in the documentation I have received of whether, when and how the Ministry's policy and its disclosure arrangements to Emergency Services would be reviewed as circumstances developed.

59. By mid-May, I understand the Ministry's position was still that it should continue to provide patient information to Emergency Services in line with its April policy.[8] This was despite the fact that New Zealand was dropping down the alert levels, and that the last known case of community transmission was in early May.

[8] The Ministry's correspondence on this point was in an undated draft form and as such we have not been able to verify the date.

60. As far as I can see, it was only through the events of early July (which prompted Mr Heron's investigation and report) that initiated the Ministry to review its policy and arrangements. Feedback the Ministry received from several Emergency Services suggests that by this stage, it had already reached a point where it was not necessary for some agencies to be receiving patient information, particularly as there was no community transmission and all confirmed cases were either in managed isolation or quarantine.

61. Ideally, the decreasing number of Covid-19 cases, drop in alert levels, and stamping out of community transmission should have prompted the Ministry's review of its policies and processes to ensure health information was only disclosed in a proportionate manner and only so far as was required, including whether it still had a proper basis to routinely disclose patient details.

62. Should the Ministry consider once again that it is necessary to disclose health information about Covid-19 patients outside of the health sector, I **recommend** it ensures there are appropriate data minimisation and disclosure practices in place so that only what is necessary for the public health response is disclosed in accordance with rule 11(3). For example, the Ministry could consider only disclosing limited data fields, limiting the data to each Emergency Service by region of each patient, or adding agreements or memoranda of understanding to ensure that robust practices are in place at recipient agencies.

63. I also **recommend** the Ministry take some time to review and update its policy now. In particular, the policy should indicate how often it will be reviewed, and by whom. It should cover the different legal bases for disclosing patient information in different contexts within the pandemic – for instance, where there is a widespread outbreak, or where there may be evidence of community transmission but only within a particular region.

Storage and security of health information under rule 5

64. Under rule 5 of the Code, health agencies must take reasonable steps to ensure that there are reasonable safeguards in place to prevent loss, misuse, or disclosure of health information. Rule 5 requires that before sharing this information the Ministry had taken reasonable steps to ensure this information was protected, including putting a process in place to ensure there was a secure method for sharing it.

65. Rule 5 is situational – the security standards in an emergency will obviously be lower than in other circumstances. The Ministry was required to develop a process in haste to get information to agencies that needed it. In an emergency situation, the standards expected were understandably relaxed. Once the dust settled, the security standards expected should have increased again. It is entirely consistent to say that the standards set on 13 April were appropriate but were no longer appropriate by July even though the agencies and information in question remained the same. As the situation evolved, especially as the Ministry started to receive feedback from the recipients that

they no longer needed the information, it became time to reflect on the process in place.

66. In my letter to the Ministry dated 3 August 2020, I sought information regarding the security measures in place to protect the patient information being disclosed.

67. The April memorandum provided by the Ministry shows it was on notice of concerns raised by DHBs about adequate protection of patient privacy when sharing patient information with organisations, such as emergency service providers. In particular, DHBs were concerned "about whether there are sufficient guarantees that emergency services will use identifiable information appropriately, including adequately protecting this information from being disclosed more widely". The April memorandum identified that there were several pieces of guidance in development to ensure the internal Ministry processes were robust, including the development of a process to ensure there was a secure method for sharing data when needed. An example was given of end-to-end encryption of data being sent by the Ministry could be guaranteed regardless of the programmes used by recipients. However, the Ministry has not provided details of any such process. Further, it is apparent from the information we have received, and the Heron report, that the spreadsheets containing patient information were not protected by end-to-end encryption or other security safeguards.

68. The spreadsheets containing patient information were attached to an email with "MEDICAL IN CONFIDENCE" in the subject line. Although this did not provide any technical safeguards to protect patient information, it did signal to Emergency Services that such information was to be kept in confidence.

69. Medical information is inherently sensitive, and information about individuals who had tested positive for Covid-19 more so in the current global climate. As discussed earlier, individuals who have tested positive for Covid-19 in some areas of New Zealand have experienced vitriol, stigmatisation, and have been singled out on social media. Further, because the recipients included Police and other non-health recipients, it is my expectation that additional safeguards would be put in place – medical professionals such as doctors have an additional duty of confidentiality that not all recipients were subject to.

70. Although noting that the information was "MEDICAL IN CONFIDENCE" initially went some way to address security requirements under rule 5 at the outset of the pandemic, this mechanism by itself in my view was not a sufficient or reasonable long-term safeguard or process to protect this information from misuse or disclosure, given the sensitivity of the information involved and the recipients of the information. Once outside the initial emergency response, this information should have been, in my opinion, at the very least password protected or encrypted once the Ministry had the opportunity to put this in place. The apparent lack of appropriate processes in this area after April 2020 fall short of the standard required by rule 5.

71. I **recommend** the Ministry implement immediate measures to ensure security of health information when disclosing identifiable details to third parties.

A coordinated approach to information sharing

Developing a purpose-driven basis for use and disclosure of information under rule 3

72. Rule 3 of the Code says:

> (1) Where a health agency collects health information directly from the individual concerned, or from the individual's representative, the health agency must take such steps as are, in the circumstances, reasonable to ensure that the individual concerned (and the representative if collection is from the representative) is aware of:
>
> (a) the fact that the information is being collected;
> (b) the purpose for which the information is being collected;
> (c) the intended recipients of the information;
> (d) the name and address of:
>
> (i) the health agency that is collecting the information; and
> (ii) the agency that will hold the information;
>
> (e) whether or not the supply of the information is voluntary or mandatory and if mandatory the particular law under which it is required;
> (f) the consequences (if any) for that individual if all or any part of the requested information is not provided; and
> (g) the rights of access to, and correction of, health information provided by rules 6 and 7.

73. The obligations in rule 3 sit with the agency collecting information. In the context of the Covid-19 response, Covid-19 tests are administered through general practitioners and DHBs, which will have the primary responsibility for compliance with rule 3. However, while the Ministry did not have a direct relationship with the patients, it was coordinating the Covid-19 health response and was therefore best placed to provide guidance to frontline health agencies to ensure they were providing good information about where this information was going to be shared.

74. We understand that information being provided to patients does not explain that their information may be disclosed to Emergency Services. Collection is the point at which individuals should receive accurate information about what will be done with their information. I **recommend** the Ministry should assist the collecting agencies to ensure they meet their obligations under rule 3 and that individuals are getting the information which rule 3 requires.

Setting expectations about the use of disclosed patient information under rule 10

75. Various agencies within the health sector had advised the Ministry of concerns about patient privacy. As well as concerns around security of information, DHBs communicated concerns about whether there were sufficient guarantees that Emergency Services would use information appropriately.

76. My Office received complaints from individuals whose Covid-19 results had been received and used by the Police vetting service. The use of patient information by Police forms part of this Inquiry and I have commented on this further later in the report, However, it is my view that it was inappropriate for Police to use Covid-19 testing information as part of the vetting service.

77. The Ministry were certainly aware of this responsibility – the memorandum refers to developing communications and guidance for Emergency Services to ensure they understood their obligations to use the patient information appropriately. However it is not clear when this guidance was produced, or if it was circulated before mid-May[9] when the Ministry emailed the various Emergency Services providing guidance on this point, which highlighted that information was only to be used for the purpose for which it was shared. I have not been provided a copy of this guidance, and so cannot comment on the adequacy or appropriateness of the standards the Ministry set. However, I have seen no evidence to suggest that prior to the Ministry's email in May that the Ministry set or communicated its expectations for use of this information by Emergency Services, which in itself falls short of my expectations, given that this information was being shared with Emergency Services since mid-April.

78. I **recommend** the Ministry develop memoranda of understanding between the Ministry and Emergency Services. These should set clear expectations about appropriate use of the information being disclosed, give clear direction on non-retention beyond clinical relevance, and detail how often the Ministry needs to check in with the relevant Emergency Service to establish whether they still have a legitimate need for the information.

Managing onward disclosures – including public messaging of Covid-19 cases

79. As part of work to revise disclosure practices to Emergency Services, the Ministry could also provide guidance about disclosures that are intended to update the public about Covid-19 more generally, without providing identifiable information.

80. New Zealand has a relatively small population, and in some instances, this can mean that even releasing a small amount of apparently anonymous information can readily lead to identification of individuals with Covid-19. As set out above, one individual has provided submissions to my Office that publication of the town they resided in and their association with a Covid-19 cluster was enough to identify them to people in their locality. That individual and their family suffered significant distress and stigma as a result of this disclosure.

81. This incident highlights the importance of a clear and coordinated approach to sharing information, even where that information is not intended to include identifiable details. I **recommend** the Ministry develop a coordinated plan in relation to the sharing of such information to ensure that all recipients are aware of the risks of releasing information that may lead to an individual being identified and ways in which that can be mitigated. This could take the form of an information strategy, reviewing and expanding on the guidance that is already in place.

[9] A copy of this correspondence provided by the Ministry was in an undated draft form. The Ministry have advised that this was sent in mid-May, however we cannot provide a more accurate date than this based on the information provided.

Police's access to and use of Covid-19 Patient Information

82. The second element of this Inquiry looks at Police's access to and use of Covid-19 patient information.

83. In my view, Police had legitimate concerns about how it was going to manage the Covid-19 response when the virus first emerged in New Zealand, and it had proper reasons to enter the arrangement of the nature it had with the Ministry. However, Police should have reviewed its need for patient information as the prominence of Covid-19 reduced in New Zealand. Further, while it was appropriate for Police to enter patient information into NIA to protect its staff and assist with its pandemic response, I have **found** it was not justified for Police to disclose that same information, although in only a small number of cases and for a short-lived period, to agencies as part of its vetting function.

Basis for entering arrangement with the Ministry

84. The primary reason Police wanted patient information from the Ministry was to protect the health and safety of its front-line staff. Its view was that if its staff knew an individual they would be interacting with was Covid-19 positive, they could take extra precautions or otherwise cater their response as required.

85. When Police first made approaches to the Ministry around the end of February and start of March, the pandemic situation was only just beginning to unfold, but it was developing rapidly. There was an element of the unknown about the virus. No one knew whether it was likely to spread around the country, and to what extent.

86. Police play a critical role in managing a country's pandemic response. This is no different in New Zealand. Here Police were acutely aware that in other countries where the virus had become widespread, for instance in the United Kingdom, many front-line Police staff had been taken out of action due to their potential or actual exposure to the virus. Police here recognised that there was a need to move quickly to try and get ahead of the virus while we still had minimal cases.

87. Eventually Police became responsible for a range of new duties related to the pandemic response, such as compliance and enforcement of government orders. On top of this, Police continued to hold responsibility for general policing duties, enforcing the law and ensuring community safety.

88. By the very nature of their work, front-line Police staff operate in various contexts and locations, and with different levels of engagement and interaction with individuals. In many circumstances, these officers cannot or would not be able to exercise the normal precautions that are encouraged and expected of the general New Zealand public. An example is where officers are required to exercise reasonable use of force.

89. While Police cannot confirm how often its staff accessed NIA for pandemic response purposes, after reviewing its Communication and Resource Deployment System,

Police estimate it attended approximately 200 separate events at confirmed Covid-19 addresses between 23 March and 2 July. The nature of these events covered the full breadth of Police functions, including, for example, bail checks, family harm events, suicide threats and attempts, and trespass issues.

90. Having considered what Police knew at the time and in light of the evolving pandemic context, it is my view that Police had a legitimate reason for entering into this arrangement with the Ministry.

91. That said, it is also my view that there was scope for a more thorough review of this arrangement as circumstances changed, particularly as New Zealand progressed down the alert levels due to fewer cases and there was increasing evidence of no community transmission. This was the perfect opportunity for Police to reflect not only on whether it still had a legitimate need to routinely have access to confirmed Covid-19 patient details at that time, but also whether it would do anything differently if and when Covid-19 re-emerged in the community.

Police use of patient information

92. It was entirely appropriate for front-line Police staff to access and rely on NIA alerts related to Covid-19 to assist with or enable them to carry out their pandemic management or general policing duties. However, Police's use of that information also extended to disclosing it to agencies as part of its vetting function.

93. I have previously expressed reservations about Police disclosing clinical information as part of its vetting function.[10] When conducting a vet, Police disclose information if they consider it relevant to the role the individual concerned is being vetted for. That was the rationale Police cited to the individuals whose Covid-19 status was disclosed as part of the vetting process.

94. The issue is that this means Police vetting staff are effectively making a judgment on the relevance of clinical information without clinical input. It should not be up to Police vetting staff to make this decision where that information is being relied on by the agency to make decisions such as determining a person's suitability for employment.

95. It is my view that Police should leave it to the agency to obtain health information either from the individual directly, or from a relevant health agency that can make an appropriate determination on the relevance of that information to the role.

96. I am pleased that Police have confirmed to me that it immediately stopped disclosing Covid-19 patient information during the vetting process as soon as concerns were raised about the practice.

[10] Email from Privacy Commissioner to Police Commissioner, copied to Judge Colin Doherty, dated 23 April 2020. See also, 2016 IPCA and OPC Public Report, Joint review of the Police Vetting Service.

Conclusion

97. While I accept that the Ministry had a clear and measured rationale for its decision to provide patient information to Emergency Services in April 2020, I recommend the Ministry now ensures it appropriately assesses the application of rule 11(2)(d)(i) of the Code before disclosing health information to prevent or lessen a serious threat to public health, including the consideration that authorisation is neither practicable nor desirable before relying on the exception.

98. I also urge the Ministry to implement appropriate data minimisation and disclosure practices so that it is only disclosing information to Emergency Services that is necessary for the public health response. The Ministry should develop a coordinated plan in relation to the sharing of such information to ensure that all recipients are aware of the risks of releasing information that may lead to an individual being identified and ways in which that risk can be mitigated.

99. In order to comply with its obligations under rule 5 the Ministry needs to implement immediate measures to ensure security of health information when disclosing identifiable details to third parties, and I strongly suggest it develop memoranda of understanding with Police and other Emergency Services to set clear expectations about the use of patient information by the recipients.

Appendix One – The Memorandum

MINISTRY OF HEALTH
MANATŪ HAUORA

Memorandum

Position on the release of COVID-19 patient information

To:	Ashley Bloomfield, Director-General, Ministry of Health
Copy to:	Jane Kelley, National Director COVID-19 Response
From:	Maree Roberts, Deputy Director-General, System Strategy and Policy
Date:	13 April 2020
For your:	Decision

Purpose of report

1. This report:
   a. outlines the issues raised about data sharing in the context of COVID-19
   b. provides or proposes policy positions on sharing information regarding individual confirmed cases of with different stakeholders, and a strategy for clarifying the Ministry's policy position for key stakeholders
   c. outlines the work currently underway to ensure the Ministry's internal COVID-19 data sharing processes are robust.

Background

Regulatory framework for sharing information in the context of COVID-19

2. Under the Privacy Act 1993, agencies can only disclose personal identifiable information in limited circumstances. This includes where the person authorised the disclosure (ie, consent is given), or disclosure is one of the purposes for which the information was collected.
3. There are a number of exceptions which are relevant during a pandemic such as COVID-19 that allow for identifiable information to be shared where this would otherwise not be possible. This includes provisions in the Health Act 1956 and the Health Information Privacy Code 1994. Detail of these provisions is attached as **Appendix One.**
4. 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.

Privacy Commissioner
Te Mana Mātāpono Matatapu

MINISTRY OF HEALTH
MANATŪ HAUORA

5. 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).[1]

6. The Ministry also updates district health boards (DHBs) twice daily with key information about the COVID-19 response.

Issues raised by the sector

7. Civil Defence and Emergency Management (CDEM) officials are concerned that the rationale and urgency of other agencies receiving data about COVID-19 confirmed case locations (as allowed under exception outlined in paragraph 5) is not well understood at the DHB level.

8. DHBs have signalled concern about adequate protection of patient privacy when information about COVID-19 cases is shared with a variety of organisations, including CDEM, emergency services providers, and members of parliament and mayors.

9. In particular, DHBs have communicated concern about whether there are sufficient guarantees that emergency services providers will use identifiable information appropriately, including adequately protecting this information from being disclosed more widely (for example to media organisations). We are not aware of any specific incidences where identifiable information has been shared inappropriately by emergency services providers.

10. The Ministry shares information directly to for emergency services providers, meaning DHB concerns do not affect this data being shared with Police, FENZ, and ambulance providers. However, CDEM is experiencing communication issues with some DHBs. The broader concerns that DHBs have with the management and security of information being shared with emergency services providers may be contributing to some DHB's reluctance to work closely with CDEM branches.

11. There have also been recent media reports about the reluctance by some DHBs' to share information about the breakdown of COVID-19 cases by territorial authority with the relevant local elected officials/mayors. The Ministry releases data by DHB region, but several DHBs such as Bay of Plenty DHB and Lakes District DHB are now providing locality breakdowns by territorial authority-type on their own webpages after your daily 1300hrs media standups.

Risks

12. Limiting the information provided to emergency services providers may increase the risk of unknown exposure to COVID-19 and in turn increase the risk of community transmission (ie, as emergency services personnel do not have information at the front

[1] Emergency services personnel should be using PPE as recommended by the latest government guidelines regardless of whether a callout has been identified as the address of a person with COVID-19.

Privacy Commissioner
Te Mana Mātāpono Matatapu

MINISTRY OF HEALTH
MANATŪ HAUORA

line to enable them to take appropriate precautions). It may also decrease the ability for emergency services personnel to make appropriate decisions about self-isolation.

13. CDEM is concerned that communication issues with DHBs may limit the ability of CDEM to undertake effective contingency planning for cluster response, which may increase the risk of the spread of COVID-19 outside of these clusters.

14. If information is shared inappropriately, there is a risk that individuals with COVID-19 could be identified by the general public. The Ministry continues to see some inappropriate behaviour against people who are being tested or have/had COVID-19 by some parts of the community (including bullying). We need to act to respect patient confidentiality despite the challenges of COVID-19.

Policy position on releasing identifiable information directly to emergency services providers

15. 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.

16. 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.

17. 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.

18. 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.

19. The Ministry has provided general guidance to other government agencies and DHBs on the what the Ministry considers reasonable due diligence when handling information in the context of COVID-19. The guidance that has already been shared is attached at **Appendix Two** for your information.

Policy position on DHB data sharing with different stakeholders

20. Aggregated, non-identifiable information (official information) can always be shared, including the number of cases by territorial local authority and DHB. In addition, health agencies can share information about the presence, location, condition and progress of a patient in a hospital, on the day on which the information is disclosed, and if the disclosure is not contrary to the express request of the individual or their representative. However, this will usually be in response to a request for information about particular patients, rather than being generally disclosed.

MINISTRY OF HEALTH
MANATŪ HAUORA

21. **Ministry officials have provided guidance to DHBs that information about testing and cases (both confirmed and probable) can be released at the DHB and territorial authority level to various other agencies, including Police and CDEM groups.** This guidance notes that the release of territorial authority level information should be exercised with discretion where there is a risk of compromising patient confidentiality, including considering the information that is published on the Ministry's website (which includes the age group, gender, and recent travel details of each case).

22. **Ministry officials consider the administrative burden of sharing information with individual members of parliament and mayors or other officials at the territorial authority level *prior* to your stand ups is not an appropriate use of Ministry or DHB resource during the response to COVID-19.** In addition, it is important to manage the risk of creating confusion about the number of new cases of COVID-19 through sharing the information at different times to different audiences.

23. 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.

24. 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".

25. **Ministry officials recommend personal identifiable information (ie, names and addresses) regarding people confirmed with COVID-19 is not shared with individual members of parliament and mayors or other officials at the territorial authority level at this time.**

agree

Next steps

Ministry mechanism for decision-making on data and information sharing

26. A Ministry of Health Data and Information-Sharing Governance Group for COVID-19 will meet for the first time in the week starting 13 April 2020. Future guidance on issues related to information sharing will be in the remit of this Governance Group. This memo will be shared with the Governance Group to inform initial discussions.

Work underway on ensuring Ministry COVID-19 information-sharing processes are robust

27. There are several pieces of guidance already in development to ensure the internal Ministry processes for sharing information are robust, including:

    a. a form to record:

        i. the origin of the request

        ii. details of data to be shared and with whom

        iii. patient and system outcomes that will be achieved by sharing of the data

        iv. legal mechanism for sharing this data (including ethics and consent processes)

        v. risks of sharing the data

Privacy Commissioner
Te Mana Mātāpono Matatapu

MINISTRY OF HEALTH
MANATŪ HAUORA

vi. impact of not sharing the data

vii. process of sharing the data

b. a checklist for sharing identifiable information to ensure the following requirements are met when sharing unencrypted NHI level health and disability information with health providers and AOG agencies:

i. requests meet the scope defined

ii. approval of requests follows the principles and processes

iii. accurate documentation is kept of all assessment and decisions made

iv. requests are escalated to the Ministry Data and Information-Sharing Governance Group for COVID-19 where a decision by a responsible manager is unable to be reached.

c. a 'Health Information Privacy Code in a nutshell' guide to patient privacy considerations.

28. There is also a process underway in the Ministry to ensure there is a secure method for sharing data available when needed (ie, where end to end encryption of data being sent be the Ministry can be guaranteed regardless of the programmes used by recipients).

Communications strategies for emergency services providers and for DHBs

29. Officials recommend that deliberate communications are developed for:

a. emergency services providers and CDEM, to ensure they understand their obligations to use the identifiable information the Ministry provides appropriately

b. DHBs, to provide reassurance that measures are being taken to ensure this information is handled appropriately.

30. A single contact point has been established for DHBs to communicate specific concerns regarding the privacy of patient information and data sharing and receive guidance (healthlegalexecutiveassistant@health.govt.nz).

31. Subject to your approval, this memo will be shared with the National Health Coordination Centre (NHCC) to clarify the policy position on sharing information with different agencies and requesters. This will enable clear and consistent responses to queries on sharing information as part of the all of government cross-sectoral response to COVID-19.

Recommendations

I recommend that you:

a) **Note** that consistent with legislative mechanisms (Privacy Act 1993 and Health Information Privacy Code 1994) the Ministry of Health is providing identifiable information about COVID-19 cases directly to emergency services providers twice daily, to enable personnel to take appropriate precautions when responding to call outs

Privacy Commissioner
Te Mana Mātāpono Matatapu

MINISTRY OF HEALTH
MANATŪ HAUORA

b) **Note** that concerns have been raised that district health boards are unclear on the Ministry of Health's policy position on sharing information with different stakeholders and are concerned about the risk to privacy for individuals

c) **Note** that there have been requests for personal information regarding people confirmed to have COVID-19 to be shared with members of parliament and territorial authorities

d) **Agree** that the Ministry of Health's policy position is that it is necessary to continue to disclose identifiable information on COVID-19 cases to emergency services providers to combat the spread of COVID-19 **Yes/No**

e) **Agree** that it is not appropriate to share the requested personal information directly with individual members of parliament or individual officials of territorial authorities at this time, as it is not clear why this information is needed or how it would be used **Yes/No**

f) **Agree** that it is not an appropriate use of Ministry or DHB resource to share information with members of parliament or officials of territorial authorities ahead of your media standups **Yes/No**

g) **Note** this report has been shared with the Ministry of Health Data and Information-Sharing Governance Group for COVID-19 to inform discussions on appropriate risk management in this area

h) **Note** there is work underway to ensure the Ministry's COVID-19 data sharing processes are robust

i) **Agree** that further deliberate communications are developed for emergency services providers, CDEM, and DHBs **Yes/No**

j) **Forward** this report to the National Health Coordination Centre to enable consistent messaging to enquiries from DHBs and other sources as per the recommendation above. **Yes/No**

ENDS.

Privacy Commissioner
Te Mana Mātāpono Matatapu

MINISTRY OF HEALTH
MANATŪ HAUORA

Appendix One: Summary of relevant legal provisions for data and information sharing to support pandemic response

What law, regulations and codes can we rely on to enable sharing of data and information during a public health emergency?

Information can always be shared on the following basis:

- by disclosure of non-identifiable data
- for the purpose (or a directly related purpose) for which it was collected
- by the consent of the individual (or their representative) to which the information relates
- by other exceptions under the Information Privacy Principles in the Privacy Act 1993 or the Health Information Privacy Code 1994 (note the Code applies only to certain types of agencies, not all government departments: see cl 4(2) of the Code)
- by other legislative authority (such as the Health Act 1956).

Where disclosure is necessary and is not authorised by the grounds set out above, the "serious threat exception" may enable disclosure of information.

Rule 11(2)(d) of the Health Information Privacy Code 1994 (and its equivalent, Information Privacy Principle 11(f) of the Privacy Act 1993) allows information to be disclosed where it is not desirable or practicable to obtain authorisation from the individual concerned and the disclosure of the information is necessary to prevent or lessen a serious threat to:

- public health or public safety
- the life or health of the individual concerned or another individual.

"Serious threat" means a threat that an agency reasonably believes to be a serious threat in regard to all of the following:

- the likelihood of the threat being realised
- the severity of the consequences if the threat is realised
- the time at which the threat may be realised.

There is a similar provision that allows use of information for purposes other than what it was collected for Rule 10(1)(d) of the Health Information Privacy Code 1994 (and its equivalent, Information Principle 11(e) of the Privacy Act 1993) allows information to be used where the use of the information is necessary to prevent or lessen a serious threat to:

- public health or public safety
- the life or health of the individual concerned or another individual.

In addition, sections 22C and 22F of the Health Act 1956 will also allow disclosure in some cases (without the need to rely on the serious threat exception). For example, under section 22C(2)(f) of the Health Act 1956, the Ministry can disclose information to Police constables for the purposes of exercising their powers, duties, or functions, where required by the constable.

Privacy Commissioner
Te Mana Mātāpono Matatapu

MINISTRY OF HEALTH
MANATŪ HAUORA

Appendix Two: guidance provided to district health boards on handling data and information sharing to support pandemic response

Who is this advice for?

Anyone working with health data or information who is required to access or share personally identifiable and health information as part of the COVID-19 response.

How to think about health information sharing?

Privacy access escalation ladder

Sharing information involves both the collection and disclosure of personal information. Deciding which laws apply and what information to share can be complicated, but there are some guiding rules.

How to use the escalation ladder

Work through from question 1 to question 5 and stop when you can answer 'yes'.

If the answer to all of the five questions is 'no', then disclosure should be unnecessary and should be avoided, at least for now.

Remember that the proportionality principle always applies – you should only provide as much information as is reasonably necessary to achieve your objectives.

Question 1: Can we get by without naming names?

- Use anonymous information where practical.
- Disclosing anonymous information is always okay. (For example, if you have professional supervision, you might be able to discuss a case without referring to any names.)

Question 2: Have they agreed?

- If information is not able to be used anonymously, the best thing is consent from the parties concerned.
- Consent does not need to be written.
- Always record the fact that parties have agreed. Record any limitation or qualification of consent, eg, "please don't involve the church".
- Health agencies can share information in general terms concerning the presence, location, and condition and progress of the patient in a hospital, on the day on which the information is disclosed, and the disclosure is not contrary to the express request of the individual or his or her representative.

Question 3: Have we told them?

- If it is not practicable or desirable to obtain consent, the information may be used or disclosed if it is in line with the purpose for which it was obtained.
- Inform the person affected of this where possible – ideally at the time the information was first collected from them, or soon after that.
- If informing the person would prejudice the purpose of collection, or would be dangerous to any person, then telling the person concerned may be waived in that instance.

Question 4: Is there a serious threat

Privacy Commissioner
Te Mana Mātāpono Matatapu

MINISTRY OF HEALTH
MANATŪ HAUORA

[Will apply to many situations during a pandemic]

Information may be used or disclosed where there is a serious threat.

What is considered serious depends on:

- how soon the threatened event might take place
- how likely it is to occur
- how bad the consequences of the threat eventuating would be.

Question 5: Is there another legal provision we can use?

Many different laws allow personal information to be shared. For instance, health information:

- about the health/safety of a child or young person can always be disclosed to a police officer or social worker
- can be requested by someone who needs it to provide health services
- can be disclosed where necessary to avoid prejudice to the maintenance of the law
- can be shared under an AISA.

If the answer to all of the five questions is 'no', then disclosure should be unnecessary, and should be avoided, at least for now.

What's different during a public health emergency – such as a pandemic response?

Most of the usual enabling provisions and restrictions on information sharing apply during a pandemic. However, a pandemic poses a **serious threat to individual and public health** which may require sharing of personal health information when is otherwise would not be allowed.

For example:

- The pandemic-relevant health status of individuals may be able to be shared.
- Data and information necessary to support the pandemic response should be shared more freely throughout the health system and with other relevant agencies where appropriate.
- Messaging apps and video conferencing options should be used freely to support clinical consultations; however, if possible you should first check with your IT department to confirm the solutions will provide and appropriate balance of accessibility, security, and privacy.
- Working remotely and from personal devices may be required. You should ensure make sure your area is secure and your devices are protected. For example:
    - encrypt your devices and set a strong passcode
    - avoid storing files on your personal devices if you can
    - use a Virtual Private Network (VPN) to access your work files and avoid using open public hotspots if possible
    - lock files out of sight at home, and do not leave files in a vehicle or insecure area.

Please check with your IT department for advice, and also refer to the following sites on staying safe and secure:

https://www.ncsc.govt.nz/newsroom/working-remotely-advice-for-organisations-and-staff/

https://www.cert.govt.nz/about/news/covid-19-supporting-people-to-work-from-home/

https://www.netsafe.org.nz/scam-advice-reporting/

Privacy Commissioner
Te Mana Mātāpono Matatapu

MINISTRY OF HEALTH
MANATŪ HAUORA

Disclaimer

This guidance is intended to provide simple steps and guidance around the sharing of information during the COVID-19 response. This guidance does not overrule any legislation or policies that your organisation may have; however, it may provide a simple framework of what the Ministry of Health would consider reasonable due diligence when handling information in this situation that organisations can adopt.