

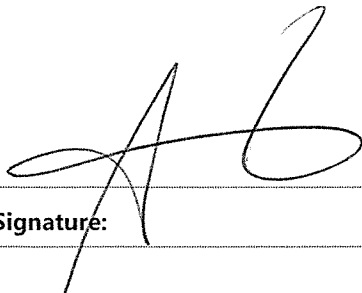
# COVID-19 RESPONSE AUDIT TRAIL AND COMMISSIONING TOOL



Document details			
<b>Document title:</b> COVID 19: Position on the release of COVID-19 patient information		<b>Proactive release:</b> Release	<b>EA / Admin contact:</b>
<b>Date requested by Minister's office:</b> N/A	<b>Date request sent to team:</b> N/A	<b>Date due to Minister:</b> N/A	<b>HR / reference number:</b> N/A
<b>Lotus Notes Database:</b> COVID-19	<b>Lotus Notes Drawer:</b> Intelligence	<b>Lotus Notes Folder:</b> *COVID-19 Intelligence	

Audit trail				
	Name	Title	Date	Signature
Author	Gemma Wong	Policy analyst	4/4/20	By email
SME	Phil Knipe	Chief Legal Advisor	5/4/20	By email/phone
Peer reviewer	Samantha Fitch	Principal policy analyst	9/4/20	By email
Proof-reader	Vera Hennessy	Senior Advisor	9/4/20	By email
Covid-19 lead (tier 3)	Zoe Coulson-Sinclair	Group Manager Policy MFAT secondee)	9/4/20	By email
Deputy Director-General	Maree Roberts	Deputy Director-General	11/4/20	By email

Background for Director-General / additional context

Director-General feedback			
			<b>Noted</b> <input type="checkbox"/>
			<b>Approved</b> <input checked="" type="checkbox"/>
			<b>Needs change</b> <input type="checkbox"/>
			<b>Other (see notes)</b> <input type="checkbox"/>
<b>DG Advisor:</b>	<b>Signature:</b>	<b>Date:</b> 14/5/20	<b>Friday bag:</b> Yes / no


*Back to Maree & cc Jane Keller*

COMMISSIONING TOOL		
		Complete
<b>Date of request</b>		
<b>Due date of final product</b>		
<b>Product and scope</b> (e.g. Health report, Briefing etc)		
<b>Customer:</b> Who is the commissioner and authorising and what is their view and expectation?		
<b>Context</b> What work is required and why? What previous work or decisions have already been made? What are the key relationships to other work? What is Policy's function in this work?		
<b>Risks and issues:</b> What are the key risks and current issues		
<b>Managing variation in scope</b> How will variation in the project be managed - Record of decisions - Record of scope change		
<b>Quality assurance</b> - use peer review roster		
<b>Lotus notes filing</b> - ensure final product is filed in Covid -19 cabinet		

# 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. 

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).<sup>1</sup>
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

---

<sup>1</sup> 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.

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. ✓

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
- ✓

- 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 by 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](mailto: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

- 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.



## 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.

## 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*

[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 an 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/>

## 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.