The release of COVID-19 patient information

Key points

The following points seek to clarify the sharing of personal information about COVID-19 cases to emergency services, district health boards and territorial local authorities.

- Under the Privacy Act 1993 and Health Information Privacy Code 1994, agencies can only disclose personal identifiable information in limited circumstances. However, there are several exceptions relevant during a pandemic such as COVID-19 that allow for identifiable information to be shared where this would otherwise not be possible, particularly the serious threat exception.
- The Ministry of Health is providing identifiable information about COVID-19 cases directly to emergency service providers such as Police, Fire and Emergency NZ twice daily. This is to help staff to have all the information they need to take extra precautions when attending callouts that involve confirmed COVID-19 cases and to combat the spread of the virus. Information provided to other emergency services to prevent the spread of COVID-19 remains subject to the Privacy Act 1993.
- The Ministry also updates district health boards (DHBs) twice daily with key information about the COVID-19 response.
- We have advised DHBs that they can release patient testing and case data at a territorial level to various other agencies, including Police and Civil Defence and Emergency Management groups.
- MPs and mayors have been requesting information about cases prior to daily media stand ups. This is not effective use of Ministry or other response agency resources during the COVID-19 response.
- The Ministry does not consider it is appropriate to share personal information with members of parliament or officials of territorial authorities as it is outside the legal grounds for which information may be shared (ie, it does not meet the requirements of the serious threat exception or other grounds).
- We want to provide the best, most useful information possible to our stakeholders without breaching patient privacy.

Handling data and information to support the COVID-19 response

- We understand this is an extraordinary time and you are receiving patients' health information as part of the COVID-19 response.

- During a public health emergency, such as a pandemic response most of the usual information sharing provisions and restrictions apply. However, a pandemic poses a serious threat to individual and public health which may require sharing

of personal health information when otherwise it wouldn't be allowed. Examples include:

- Information needed to support the response being freely shared throughout the health system and with other relevant agencies as appropriate
- Messaging apps and video conferencing being used freely to support clinical consultations. However, consult your IT department to provide an appropriate balance of accessibility, security and privacy.
- Working remotely and from personal devices may be necessary, however, make sure your area is secure and devices are protected. For example, encrypt devices with a strong passcode, avoid storing files on personal devices if possible, use a virtual private network to access work files and avoid public hot spots if possible. Lock files out of sight at home and do not leave them in vehicles. For further advice talk to your IT department.

- Knowing what information you can share and which laws apply can be complicated but there are rules:

  - You should only share as much information as reasonably necessary. There is a privacy access escalation ladder which can help you.
  - Use anonymous information where practical. This is always okay.
  - Information may be shared if that sharing is for the purpose it was collected.
  - Get consent if practicable. This does not need to be written but record any limitation or qualifications of consent – eg 'please don't involve the church'.
  - 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 and how bad the consequences of the threat eventuating would be.
  - Different legal provisions can sometimes be used. For example, health information about a child or young person can always be disclosed to a police officer or social worker.