



AboutMe had a glitch between 19 Dec – 12 Jan. Please resubmit your request if you made it during this time. [Read more](#).

Ask



Privacy, Covid-19 and the 'Serious Threat to Public Health' exception

 John Edwards

6 November 2020 at 17:28

COVID-19 is often described as an unprecedented threat to public health.

While New Zealand has experienced pandemics in the past, the epidemiological characteristics of this virus, the global nature of its spread and re-spread and the connected nature of our lives domestically and internationally means controlling COVID-19 will require both ongoing vigilance and speed of response to the threat of community re-infection.

Knowing who is potentially at risk, being able to rapidly and effectively locate positive cases (and isolate them and their close contacts) has been critically important in NZ's science-based approach to fighting the virus. This brings personal information and privacy into play.

Serious threat to public health or safety exception

Fortunately, the architects of both the 1993 and 2020 Privacy Act envisaged a scenario where the collection, use and disclosure of personal information would be needed to combat a serious threat to public health or safety.

They designed the **serious threat to public health or safety** ('public health exception') specifically for this purpose. This exception permits the **collection, use and disclosure of personal information where it is necessary to prevent or lessen a serious threat to public health or public safety**^[1]. It is worth noting that the serious threat exception was amended in 2013 to remove the words "and imminent" at the advice of the Law Commission to make it easier for agencies to use.

While the serious threat to public health and safety exception has existed since 1993, it is unsurprisingly (and fortunately) very rarely used. People are more familiar with the parallel exception for a serious threat to the health and safety of an individual. As a consequence, agencies appear to feel uncertain about how to use the public health exception where the threat affects a community or wider section of the population.

Given this and the ongoing nature of the COVID-19 public health risk, I thought it would be useful to provide guidance on how agencies can make use of the public health exception. After all, if you cannot make use an exception designed for a serious threat to public health during a global pandemic, when could you use it?

How can agencies determine whether a public health exception is applicable?

To make use of the Privacy Act's public health exception decision-makers within an agency need to believe, on reasonable grounds, that:

- *a serious threat to public health and safety exists;*
- *that the collection, use or disclosure of personal information is necessary to prevent or lessen the serious threat; and*
- *in the case of health agencies, that it is either not desirable or not practicable to obtain authorisation from the individual concerned*^[2].

The key thing to remember here is that we are talking about **public health**. As such, a decision-maker's "reasonable belief" regarding both the existence of a serious threat and the extent to which the use or disclosure of personal information is necessary to prevent or limit this serious threat should be on made on health grounds and based on current best practice epidemiological or clinical advice.

This makes the serious threat to public health exception an ideal regulatory tool for dealing with a dynamic, evolving public health threat like Covid-19 where the "rules" need to keep adapting to meet live challenges.

The Ministry of Health has the lead role in advising the Government and New Zealand on whether a situation represents a serious threat to public health. The issuing of an epidemic notice and the ongoing advice from the Ministry of Health makes it very clear that Covid-19 represents a serious ongoing threat to public health.

The Ministry of Health is also responsible for coordinating and disseminating best practice scientific advice on what is necessary to prevent or lessen the threat of COVID-19. This by extension includes the information necessary in order to monitor and control the risk to New Zealand from the movement of people across our border, and track, trace, isolate and quarantine infection risk within New Zealand. Agencies are entitled to rely on this advice in making decisions regarding whether the collection, use and sharing of personal information is necessary to prevent or lessen the threat posed by the transmission of Covid-19.

Is information sharing about groups of individuals permitted?

Another question I am regularly asked is whether the public health exception allows for the sharing of aggregated information regarding groups of individuals. The Privacy Act differentiates between serious threats to public health and safety and individual health and safety for a reason.

Public health is, by definition, focussed on keeping the community well and on groups of people rather than individuals. This provides a basis for the collection, use and disclosure of personal information about a **class** of individuals that is reasonably considered to be necessary based on relevant criteria, rather than on an individualised basis. Again, the reasons for sharing aggregated data about a class of individuals (for example people seeking to enter New Zealand or people testing positive and their close contacts, or people working in at-risk situations) should be based on best-practice health advice.

Given the ongoing nature of the threat it is likely that agencies involved in pandemic management will need to continue to share information and will need to make regular assessments of the extent to which the "serious threat to public health and safety" exception still applies as they do so.

Good privacy practice still applies – maintaining trust and confidence is critical

Even where the public health exception is being relied on, good basic privacy practice remains important in order to maintain trust and confidence of the community. Like the *Civil Defence National Emergencies (Information Sharing) Code 2020*, the public health exception applies to the source of personal information (2), use (10) and disclosure (11) information privacy principles. The other principles, including those covering collecting only what is necessary, safe storage and security, access by individuals to their own data, and ensuring accuracy before disclosure still apply.

Maintaining trust and confidence also involves agencies being transparent about what data they're collecting and what it will be used for. If specific data needs to be collected and then shared for the Covid-19 response, best practice would see an agency advising individuals of this at the time of collection or when an individual was signing up for or receiving a service (for example, when making a booking to come to New Zealand). This could also mean that agencies do not need to rely on the public health exception, as onward use or disclosure for Covid-19 purposes was one of the purposes of collecting the information in the first place.

Lessons from the Ministry of Health's recent reliance on the serious threat to public health and safety exception

I recently conducted an [Inquiry into the Ministry of Health's disclosure of Covid-19 patient information](#) to emergency services providers. The Ministry of Health relied on the public health exception to disclose this information. In undertaking this Inquiry, I was mindful of the statutory requirement for the Privacy Commissioner to have regard to the need for "government and businesses being able to achieve their objectives efficiently" (Privacy Act 2020, 21 (a) (iii)). I consider agencies may find my recommendations and findings in that Inquiry useful when considering their use of the public health exception.

First, I found the Ministry appropriately considered the basis on which it disclosed health information about Covid-19 patients to emergency services providers when relying on the serious threat to public health exception. The Ministry made a considered, risk-based assessment based on best scientific information about the nature of the virus and how it was spread, and what was known about its prevalence in the community, and determined that all emergency service providers should receive regular aggregated information regarding positive cases.

Second, I agreed with the Ministry's judgement that the serious threat exception was **not** available as a basis for providing such information to Members of Parliament, or officials of territorial authorities, as sharing identifiable information was not necessary to prevent or lessen the risk of a serious threat (based on scientific evidence) and therefore did not meet the public health exception.

While supporting the Ministry's evidence-based judgement regarding the disclosure of patient information to emergency services providers I made the following recommendations:

- Where a decision has been made to release or share information in order to prevent or lessen the serious threat to public health presented by Covid-19, the need to continue to do so should be regularly reviewed. Agencies should establish processes to ensure these reviews take place regularly and are based on best practice evidence about the virus and its management.
- It is critically important that all parties disclosing, receiving and using the information understand the basis of the information sharing and scope of their obligations in respect of the information. A memorandum of understanding can be a useful way to achieve and record this. Such documents should set clear expectations about the appropriate security and use of the information being disclosed, give clear direction on non-retention beyond clinical relevance and detail how often an

review/assessment needs to be undertaken to ensure that there is still a legitimate reason for the disclosure.

When in doubt – Ask Us

The public health exception is specifically designed to provide agencies with the ability to collect, use and disclose personal information where it is necessary to safeguard the lives of New Zealanders. The principle-based nature of the exception means it is ideally suited to a dynamic, evolving situation like Covid-19. It allows agencies to make risk-based decisions on current best practice advice.

I understand that agencies are unfamiliar with the use of this exception. OPC is available to assist agencies with advice, including peer review of Memoranda of Understanding to provide a framework for disclosures of personal information that are necessary to avoid prevent or lessen a serious threat to public health or public safety.

[1] See Information Privacy Principles 10 (use) and 11 (disclosure). For the avoidance of doubt, from 1 December 2020 the exceptions for principle 2 (source of personal information) are being 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.

[2] Health Information Privacy Code Rule 11(2)

Please visit our [Privacy and COVID-19](#) page for further information on the impact of COVID-19 on privacy in Aotearoa.

◀ Back

◀ Previous Blog Post Next Blog Post ▶

Latest Blog Entries

- [Privacy and employee snooping: The greatest threat in the workplace could be sitting next to you](#)
- [The privacy risks of insurers misusing your genetic testing](#)
- [Social media monitoring: what's happening in New Zealand?](#)
- [Why privacy in New Zealand is such a vital issue](#)
- [Advice for GPs sharing children's information with parents](#)
- [Privacy Week at Foodstuffs](#)
- [Protecting people's privacy means not just our secrets or personal data – but our self-determination and bodily-autonomy](#)
- [Privacy 101 for Charities: A Recap](#)
- [Reporting and avoiding privacy breaches in the health sector](#)

- Analysis: High Court 2021 review of Ministry decisions about Māori vaccination data