

COVID-19: PEOPLE: HANDLING COVID-19 RELATED HEALTH INFORMATION (AUSTRALIA)

02 April 2020 | Australia

Legal Briefings - By **Julian Lincoln, Partner, Kaman Tsoi, Special Counsel, Michelle Curran, Senior Associate and Alida Vandewiele, Solicitor, Audrey Vong, Graduate**

The COVID-19 pandemic has led to information gathering and sharing that has, up until now, not been contemplated by many Australian organisations.

Businesses are dedicating resources to implement essential measures aimed at responding to COVID-19 and protecting the health of their personnel and customers, including by undertaking health monitoring and adhering to government imposed social distancing requirements. Adopting these new measures may involve collecting, using and disclosing health information, for example, information related to whether an individual has been exposed to COVID-19 and the results of screening measures, such as temperature checks.

Organisations would be well aware that sensitive information (such as health information) is subject to more stringent obligations under the *Privacy Act 1988* (Cth) (the **Privacy Act**) than those which apply to personal information generally.

Even where organisations have well-established practices, procedures and systems on how to deal with personal and sensitive information, current circumstances may present novel privacy challenges requiring organisations to reassess and update current practices.

The following questions and answers are intended to assist organisations with planning how they respond to COVID-19 from an Australian privacy perspective and what they should be mindful of when handling COVID-19 related health information related to their employees and customers.

Please note this is general information which does not take into account your specific facts or circumstances. Please contact us for assistance in applying these principles to your organisation or situation.

We are an organisation seeking to collect COVID-19 health information about our employees (e.g. temperature readings, information about where they have travelled or whether they have been exposed to someone with COVID-19). Do Australian privacy laws apply to this information?

Yes, if your organisation is subject to the Privacy Act, then those obligations will continue to apply to any COVID-19 health information that you collect from your employees, and how you subsequently use or disclose it, although some exceptions may be relevant as described further below. In line with guidance issued by the Office of the Australian Information Commissioner (**OAIC**), you should, however, only collect the minimum amount of information that is necessary for your organisation to prevent and manage COVID-19.

You may also have obligations under State laws in Victoria, New South Wales and the ACT that apply specifically to your handling of health information.

The COVID-19 pandemic is an exceptional and life-threatening situation - are there exceptions to compliance with our obligations under the Privacy Act?

Yes. The most relevant to the COVID-19 pandemic is the exception allowing collection, use and disclosure of personal information where necessary to prevent a serious threat to the life, health or safety of any individual, or to public health or safety. An organisation could rely on this exemption, for example, where they need to inform particular employees that they have come into contact with a colleague who has been diagnosed with COVID-19, and it is not practicable to obtain the individual's consent before disclosing such information.

Note that this is not a comprehensive exemption from all of the Australian Privacy Principles (**APPs**). Obligations to take reasonable steps in relation to privacy notices, accuracy of information and data security, for example, will still apply.

In relation to COVID-19 specifically, the OAIC advises only collecting, using and disclosing the minimum amount of personal information reasonably necessary to manage COVID-19. Over time, the application of this health/safety exemption to COVID-19 may change. For example, if a vaccine becomes available for COVID-19, then it may no longer be a 'serious threat'. The OAIC suggests having regard to advice from the Department of Health to help decide what action is necessary from a public health perspective.

Another potentially relevant exemption is where the COVID-19 pandemic is declared an emergency or national disaster by the Federal Government under Part VIA of the Privacy Act. If such an emergency declaration is made, then different obligations will apply to the handling of personal information to the extent required to facilitate responding to the declared emergency or disaster. Note this is different to the emergency declarations that have already been made by some States and Territories.

How does the Privacy Act employee records exemption apply to COVID-19 health information collected from our employees?

For private sector employers, the APPs do not apply to information held in an employee record where the conduct involving that information is directly related to your employment relationship with that employee.

However, there are limitations to reliance on the exemption in the present COVID-19 environment. These include that the exemption only applies to:

- **The employing entity.** This presents challenges for organisations with separate employing entities.
- **Employees.** Many organisations have a mixed workforce including employees, contractors and volunteers.
- **Use and disclosure of information, but not collection.** Whilst the position on this is debatable, a recent case held that the exemption does not apply to the *collection* of personal information, rather only the subsequent handling of that information. This would mean obligations to give privacy notices about collection and to obtain consent before collecting sensitive information would still apply, unless another exception is relevant.

What if we become aware that an employee may have been exposed to COVID-19 or has travelled overseas recently - can we make a record of that information or disclose that information to our employees?

Organisations can collect information about an individual from a third party where it is unreasonable or impracticable to collect that information directly from the relevant individual. It would however be preferable to confirm the information with the affected individual. Doing so will also help you ensure you have accurate, correct and up-to-date information, which is relevant to meeting another APP requirement.

You may also inform affected employees of this information where necessary to manage the serious health threat, as discussed above.

What if we are a customer-facing business and want to collect COVID-19 related health information from customers coming into our shops or offices - will Australian privacy laws apply?

Yes, privacy laws will apply to COVID-19 related health information collected from your customers in the same way that it applies to any other sensitive information collected by you. Of course the employee records exemption will not be relevant, but the other permitted grounds for handling personal information described here will apply.

Is there any COVID-19 related information that the Australian privacy laws will not apply to?

Privacy laws will *not* apply to information that has been effectively de-identified (e.g. aggregated information). Some obligations only apply to personal information that is recorded (e.g. written down, or saved on an electronic file). For example, there may be no collection of personal information where information is not recorded (e.g. a temperature is taken but not recorded) or is recorded in a way where that individual is not identified (e.g. non-symptomatic temperatures are recorded without an identifier).

We would like to proceed with collecting COVID-19 related health information from either our employees or customers. Are we allowed to collect, use and disclose this information?

Yes - in any of the following circumstances:

- If you have consent to do so and where you only collect the minimum necessary amount of information. Consent may be express or implied, such as when an individual provides the information directly or fills out and submits a questionnaire about their health (consent does not have to be in writing).
- If required or authorised by law (e.g. where necessary to comply with work health and safety law or an order made under an emergency declaration).
- If consent is impractical and the collection, use or disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety, or to public health or safety (see above).
- Where the employee records exemption applies (see above).
- In respect of use and disclosure within Australia, where the use or disclosure is for the primary purpose for which the information was collected, or a related purpose (directly related for sensitive information) within the individual's reasonable expectations.

Are there any other impacts on my privacy obligations that relate to COVID-19?

Not specifically – the privacy obligations that your organisation is subject to will continue to apply. For example, you must:

- take reasonable steps to ensure the security of personal information, including by destroying or de-identifying the COVID-19 related information when it is no longer needed;
- reasonably maintain the quality of that information so that it is accurate, up to date and complete; and
- allow the individual to access and correct their personal information (subject to exceptions).

What steps can we take to ensure that we continue to comply with our privacy obligations?

Ongoing compliance with your privacy obligations is an essential part of considering your business' immediate and long-term response to COVID-19. Organisations should take the time to ensure that they are dealing with COVID-19 related health information in a way that is compliant with privacy obligations. For example, you should have clear procedures to address how you are handling COVID-19 related information and have suitable notices and consents where needed.

In addition, with many employees now working from home as a result of physical distancing measures, it is important to protect against data security threats and to have plans in place for dealing with any data breaches that may occur.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.



JULIAN LINCOLN

PARTNER,
MELBOURNE

+61 3 9288 1694
Julian.Lincoln@hsf.com



KAMAN TSOI

SPECIAL COUNSEL,
MELBOURNE

+61 3 9288 1336
kaman.tsoi@hsf.com

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.

© Herbert Smith Freehills 2021

SUBSCRIBE TO STAY UP-TO-DATE WITH LATEST THINKING, BLOGS, EVENTS, AND MORE

Close

© HERBERT SMITH FREEHILLS LLP 2021