Australian Government

Office of the Australian Information Commissioner

Coronavirus (COVID-19): Understanding your privacy obligations to your staff

The Office of the Australian Information Commissioner (OAIC) appreciates the unprecedented challenges Australian Government agencies and private sector employers are facing to address the spread of COVID-19. This guidance is intended to help entities regulated by the Privacy Act 1988 (Cth) (Privacy Act) to understand their privacy obligations in the context of the pandemic.

The Privacy Act will not stop critical information sharing. Agencies and private sector employers (including private health service providers)[1] have important obligations to maintain a safe workplace for staff and visitors and handle personal information appropriately, and already have practices in place to handle employee health information. For private sector employers, the employee records exemption will apply in many instances to permit the handling of employee health information.[2]

In order to manage the pandemic while respecting privacy, agencies and private sector employers should aim to limit the collection, use and disclosure of personal information to what is necessary to prevent and manage COVID-19, and take reasonable steps to keep personal information secure.

Regulated entities should also consider whether any changes to working arrangements will impact on the handling of personal information, assess any potential privacy risks and put in place appropriate mitigation strategies as part of Business Continuity Planning.

Key points

- Personal information should be used or disclosed on a 'need-to-know' basis
- Only the minimum amount of personal information reasonably necessary to prevent or manage COVID-19 should be collected, used or disclosed
- Consider taking steps now to notify staff of how their personal information will be handled in responding to any potential or confirmed case of COVID-19 in the workplace
- Ensure reasonable steps are in place to keep personal information secure, including where employees are working remotely.

[1] The OAIC's Guide to Health Privacy provides guidance for health service providers to help them comply with their obligations under the Privacy Act.

[2] For example, a record about a private sector employee's sick leave falls within this exemption where it is used or disclosed for a purpose directly related to a current or former employment relationship between the employer and individual.

Frequently asked questions

Can we collect information from employees or visitors in relation to COVID-19?

Yes, however you should collect as little information as is reasonably necessary for preventing or managing COVID-19. That includes information that the Department of Health says is needed to identify risk and implement appropriate controls to prevent or manage COVID-19, for example:

- whether the individual or a close contact has been exposed to a known case of COVID-19
- whether the individual has recently travelled overseas and to which countries.

Can we tell staff that a colleague or visitor has or may have contracted COVID-19?

Yes, you may inform staff that a colleague or visitor has or may have contracted COVID-19 but you should only use or disclose personal information that is reasonably necessary in order to prevent or manage COVID-19 in the workplace.

For example, depending on the circumstances, it may not be necessary to reveal the name of an individual in order to prevent or manage COVID-19, or the disclosure of the name of the individual may be restricted to a limited number of people on a 'need-to-know basis'. Whether disclosure is necessary should be informed by advice from the Department of Health.

Can staff work from home?

The Privacy Act does not prevent employees from working remotely as a response to COVID-19, however the Australian Privacy Principles (APPs) will continue to apply.

Agencies and employers will need to consider similar security measures for employees working remotely as those that apply in normal circumstances.

A Privacy Impact Assessment is a useful tool for evaluating and mitigating risks to personal information. Agencies are required to undertake a Privacy Impact Assessment for all high privacy risk projects or initiatives that involve new or changed ways of handling personal information.

How can we protect personal information when working remotely?

Some tips for making sure reasonable steps are in place to protect personal information include:

- Keep up to date with the latest advice from the Australian Cyber Security Centre
- Agencies should ensure continued compliance with Protective Security Policy Framework requirements
- Secure mobile phones, laptops, data storage devices and remote desktop clients
- Increase cyber security measures in anticipation of the higher demand on remote access technologies, and test them ahead of time
- Ensure all devices, Virtual Private Networks and firewalls have necessary updates and the most recent security patches (including to operating systems and antivirus software) and have strong passwords
- Make sure devices are stored in a safe location when not in use
- Use work email accounts not personal accounts for all work-related emails that contain personal information

- Implement multi-factor authentication for remote access systems and resources (including cloud services)
- Only access trusted networks or cloud services.

Background information

Protecting privacy while ensuring safety

Regulated entities need to ensure they meet their obligation to maintain a safe workplace for staff and visitors and handle personal information appropriately.

Agencies and private sector employers (including private health service providers) will likely need to collect, use and disclose personal information in order to prevent or manage COVID-19 in the workplace. This may include collecting information from visitors about risk factors or notifying staff members who may be at risk so necessary precautions can be taken.

Only personal information reasonably necessary in order to prevent or manage COVID-19 in the workplace should be collected, used or disclosed. For example, it may not be necessary to reveal an individual's name, or the disclosure of an individual's name may be restricted to a limited number of people on a 'need-to-know basis'. Whether disclosure is necessary should be informed by advice from the Department of Health.

Personal information and sensitive information

Personal information includes a broad range of information, or an opinion, that can identify an individual. It includes an individual's employee record information. It also includes 'sensitive information' which is afforded higher protection under the Privacy Act. Sensitive information includes information or an opinion about the health of an individual.

Information gathered about an individual that relates to infection and risk of exposure with COVID-19 will be sensitive information under the Privacy Act. Related information about the individual's symptoms, treatment or general health status will also be sensitive information.

Collecting sensitive information

Agencies and private sector employers can collect health information about individuals if:

- the individual gives consent (express or implied) to its collection, and
- the information is reasonably necessary, or directly related to, one or more of its functions or activities, such as to prevent or manage COVID-19 in the workplace.

Consent is not necessary if the collection is required or authorised under by or under an Australian law (APP 3.4(a)) or a 'permitted general situation' exists (APP 3.4(b)). This includes where the collection is undertaken to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

Using and disclosing sensitive information

Under APP 6, if a regulated entity (an APP entity) holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) another exception applies.

Primary purpose

The purpose for which an APP entity collects personal information is known as the 'primary purpose' of collection. This is the specific function or activity for which the entity collects the personal information. If an APP entity uses or discloses the personal information for another purpose, this is known as a 'secondary purpose.'

In relation to COVID-19, as a communicable disease, the purpose of collecting personal information from a staff member or visitor is to prevent or manage the risk and/or reality of COVID-19 to ensure that necessary precautions can be taken in relation to that individual and any other individuals that may be at risk. In these circumstances, personal information (including sensitive information) may be used or disclosed for this purpose as it falls within the primary purpose of collection.

Any other proposed use or disclosure of the information will be a secondary purpose and agencies and employers will need to consider whether it is permitted by an exception to APP 6. For example, APP 6.2(b) permits secondary uses where the use or disclosure is required or authorised under an Australian law or where a permitted general situation applies, such as where it is unreasonable or impracticable to obtain consent, and it is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.

Permitted general situations

The information handling requirements imposed by some APPs do not apply if a 'permitted general situation' exists. This exception applies in relation to the collection, use and disclosure of sensitive information.

The most relevant permitted general situation in the current circumstances is 'lessening or preventing a serious threat to the life, health or safety of any individual, or to public health or safety'.[3] This permitted general situation applies when an APP entity is collecting, using or disclosing personal information and:

- It is unreasonable or impracticable to obtain the individual's consent to the collection, use or disclosure, and
- The entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of an individual, or to public health or safety.

Employee records

For personal information relating to an individual held in a record by a private sector employer, an act or practice is also exempted where it is directly related to that record, and directly related to a current or former employment relationship between the employer and the individual.

[3] See APPs 3.4(b), 6.2(c), 8.2(d) and 9.2(d).