



Interpreting the legislation – *Information Privacy Act 2009*

All agencies - Use and disclosure to prevent harm (IPP 10(1)(b) and 11(1)(c) and NPP 2(1)(d))

- 1.0 Overview
- 2.0 The privacy principles
- 3.0 Is the threat serious?
- 4.0 Can use/disclosure prevent or lessen the threat?
- 5.0 Necessary
- 6.0 Prevent or lessen

1.0 Overview

Health Agencies¹ are required to comply with the National Privacy Principles (NPPs), and all other agencies² with the Information Privacy Principles (IPPs), in the *Information Privacy Act 2009* (Qld) (**IP Act**).

Note

In this guide, health agencies and other agencies are collectively referred to as *agencies*, unless their obligations differ. Where they have different obligations under their respective privacy principles they are referred to as health agencies and non-health agencies.

Under IPP 10 and NPP 2 an agency can only use personal information³ for the reason it was collected unless one of the exceptions applies. Under IPP 11 and NPP 2, an agency cannot disclose personal information outside the agency unless one of the exceptions applies.

The exceptions include that the use or disclosure is necessary to lessen or prevent a serious threat to an individual or to the public.

¹ In this guideline, health agency includes a bound contracted service provider to a health agency.

² In this guideline, agency includes Ministers and bound contracted service providers to the agency.

³ Any information or opinion about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.



Office of the Information Commissioner
Queensland

Note

It is important to note that the privacy principles do not *authorise* the disclosure of personal information. Rather, they mean that an agency legitimately disclosing personal information under IPP 11(1) or NPP 2(1) does not breach those privacy principles and can rely on them as a defence to a privacy complaint.

In addition, the privacy principles do not override provisions of other Acts that prohibit the disclosure of personal information, for example confidentiality provisions like those contained in the *Hospital and Health Boards Act 2012* or the *Child Protection Act 1999*.

2.0 The privacy principles

IPP 10

- (1) *An agency having control of a document containing personal information that was obtained for a particular purpose must not use the information for another purpose unless—*
- (b) *the agency is satisfied on reasonable grounds that the use of the information for the other purpose is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety, or welfare.*

IPP 11

- (1) *An agency having control of a document containing an individual's personal information must not disclose the personal information to an entity (the relevant entity), other than the individual the subject of the personal information unless—*
- (c) *the agency is satisfied on reasonable grounds that the disclosure is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety, or welfare.*

NPP 2

- (1) *A health agency must not use or disclose personal information about an individual for a purpose (the **secondary purpose**) other than the primary purpose of collection unless—*
- (d) *the health agency reasonably believes that the use or disclosure is necessary to lessen or prevent a serious*



threat to an individual's life, health, safety or welfare or a serious threat to public health, safety or welfare

3.0 Is the threat serious?

The threat the agency is trying to lessen or prevent by using or disclosing the personal information must be serious and it must be to an individual's life, health, safety or welfare or public health, safety or welfare.

- The individual whose personal information is being considered does not have to be the one facing the harm.
- The threat does not need to be to an identifiable person. It may be a threat of harm to be randomly inflicted, so that it is impossible to identify a specific person against whom the threat is directed.
- Health includes mental health—mere stress, aggravation, or inconvenience would not constitute serious harm, however the triggering of a serious stress-related disorder could.
- For public health, safety, or welfare—this must be a real and serious threat to the general public, or a portion of it, such as an outbreak of disease, or a bushfire threatening a locality.
- The threat does not have to occur in Queensland or even in Australia. It may happen anywhere in the world.

Sending information overseas

Under section 33(c), an agency can transfer personal information outside Australia if satisfied on reasonable grounds that the transfer is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare.

4.0 Can use/disclosure prevent or lessen the threat?

There must be a sufficient link between the use or disclosure of the personal information and the prevention or lessening of the threat. The information must be used only for that purpose, and not for any other. In the case of a disclosure, it would normally be to another agency or body with the capacity and authority to reduce or prevent the threat.

Generally, these exceptions should be used in emergency or extraordinary situations where time is of the essence and not to justify regular or ongoing uses or disclosures. However, in some circumstances this may be appropriate, depending on the nature of the threat and the sensitivity of the information. For example, a local council might regularly provide information to the Rural Bushfire Brigade so that the Brigade can prepare local landholders for bushfire season.

Where this exception is used to permit ongoing or regular disclosures, the agency should carefully consider their obligations under IPP 2 or



Office of the Information Commissioner
Queensland

NPP 1 to advise individuals from whom they are collecting personal information of any regular disclosures that will be made.

5.0 Necessary

Part of deciding if the use or disclosure is necessary involves making an assessment about whether the harm can be lessened or prevented using de-identified information. If so, then the use or disclosure is not necessary.

It is not sufficient that an agency simply believes the threat exists. It must believe that the use or disclosure of personal information is necessary to lessen or prevent that threat. The following questions will assist agencies in making that determination:

- Is the information being used or disclosed with the intention of lessening or preventing the threat?
- Is the personal information being used or disclosed to manage the threat?
- When disclosed, is the recipient in a position to act on the information to lessen or prevent the harm?
- Will the proposed use or disclosure reduce the threat?

Hint

An agency should consider whether there are alternative reasonable ways to reduce the threat (for example, by seeking consent to the use or disclosure) – this helps in working out whether the disclosure is necessary.

Agencies considering using or disclosing personal information to reduce threats to public health or public safety may find it useful to discuss the threat in general terms (and whether the proposed use or disclosure is likely to reduce the threat) with a relevant authority dealing with public health or safety, for example a health agency or the agency responsible for environmental health.

6.0 Prevent or lessen

For a threat to be prevented or lessened the use or disclosure of the personal information must allow the body using or receiving it to take steps they would not otherwise have been able to take to either remove the threat entirely, or to reduce it significantly. It must be more than a mere chance of reducing it, or a 'just in case' measure. For example, releasing a suspected offender's picture and details to the media would, in most circumstances, be unlikely to satisfy the requirements of these privacy principles.

If the attempt to prevent or lessen the threat is unsuccessful it will not invalidate a disclosure these privacy principles, as long as the belief that using or disclosing the personal information would do so was reasonable.



Office of the Information Commissioner
Queensland

For additional information and assistance please refer to the OIC's privacy guidelines, or contact the Enquiries Service on 07 3234 7373 or email enquiries@oic.qld.gov.au.

This guide is introductory only, and deals with issues in a general way. It is not legal advice. Additional factors may be relevant in specific circumstances. For detailed guidance, legal advice should be sought.

If you have any comments or suggestions on the content of this document, please submit them to feedback@oic.qld.gov.au.

Published 30 June 2009 and Last Updated 20 September 2019

Changes to legislation after the update date are not included in this document