Office of the Information Commissioner
Queensland

Applying the legislation

GUIDELINE *Information Privacy Act 2009*

Privacy and managing disaster events

In common with the rest of Australia, natural disaster events such as tropical cyclones, floods, bushfires and storms can occur in Queensland at any time. Natural disaster events exact a corresponding cost on individuals, communities and businesses, and also affect government functions and services. This is particularly likely during Queensland's storm season: between November and April.[1]

This guideline will help public service officers who need to use, disclose, or access personal information in a disaster or emergency event. It includes practical tips and examples to increase understanding and help simplify compliance with the *Information Privacy Act 2009* (Qld) (**IP Act**).

What is a disaster?

A disaster is defined as:

> *…a serious disruption in a community, caused by the impact of an event, that requires a significant coordinated response by the State and other entities to help the community recover from the disruption.* [2]

A critical component of this coordinated response is the timely exchange of accurate, complete, and up to date information, including the personal information of all individuals affected by a disaster event and those involved in its management.

Can agencies share personal information in a disaster or emergency situation?

There are privacy considerations whenever a Queensland government agency deals with personal information. While it is a common misconception that the privacy principles in the IP Act work against the sharing of personal information between agencies, the reality is that they not only provide generous flexibility for information exchange in disaster event circumstances, they do so without compromising the privacy of that information once the disaster event has been dealt with.

Personal information

The privacy obligations in the IP Act apply only to personal information, which is any information about an individual whose identity is apparent, or can reasonably be ascertained, from that information.[3]

[1] http://www.bom.gov.au/cyclone/about/eastern.shtml
[2] Section 13(1) of the *Disaster Management Act 2003*.
[3] Section 12 of the IP Act.

> **Tip**
>
> The capacity to identify a person is a key component of personal information. Aggregated or de-identified data does not raise privacy issues and should be used where the identity of individuals is not necessary to achieve the intended purpose.
>
> For example, sharing information that "*currently there are two people with diabetes, four pregnant women, two elderly people and five children on board and en route to the evacuation centre*" would be sufficient for the evacuation centre to undertake support planning.

Information about an individual is distinct from information about things associated with an individual or even information of great interest to individuals. For example, a land map showing the extent of flooding in a particular area would generally not be personal information, even though there would be individuals whose properties fall within the area shown on the map.

Additionally, private sector businesses and community sector organisations do not of themselves have personal information, however the individuals working for these entities do.

What flexibilities does the IP Act provide?

Collection

When an agency[4] collects personal information from the individual themselves, all reasonable steps must be taken to make the individual generally aware of why their information is being collected, any legislative authority for the collection, and the identity of third parties to which their personal information would usually be provided.[5] This 'collection notice' is not required in the context of the delivery of an emergency service where the agency reasonably believes there is no practical benefit in giving it and the individual would not reasonably expect this to occur.[6]

While the extent to which personal information is collected from an individual and the way it is collected should not intrude into an individual's domestic life, there is a reasonableness component to this obligation which can be applied to disaster events.

Reasonably necessary for health, safety or welfare reasons

Information Privacy Principle (**IPP**) 10[7], Information Privacy Principle 11[8] and section 33[9] all allow dealings with personal information where:

[4] This flexibility does not apply to health agencies. Health agencies have a different set of privacy obligations – the National Privacy Principles (**NPPs**) - which have slightly different obligations and permissions.
[5] This information is required by Information Privacy Principle 2 (3) and is often provided in a formal notice, commonly referred to as a 'collection notice'. It can be provided informally or verbally.
[6] Information Privacy Principle 2(5).
[7] Limits on use of personal information
[8] Limits on disclosure of personal information; see also NPP 2 for health agencies
[9] Transfer of personal information outside Australia

> *…the agency is satisfied on reasonable grounds that the [dealing] 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.*

This is the single most relevant privacy exemption in disaster events. While it could appear limiting that the threat must be serious, Queensland's experience has shown that disaster events often have tragic consequences, meaning they will generally represent a serious threat. It is not necessary for the threat to be immediate or imminent, which allows this exemption to cover prevention; it can encompass steps taken to ensure that the threat does not eventuate.

The 'reasonable necessity' test for the secondary use or disclosure requires a judgement about whether the threat to life or safety can be avoided or lessened without using or disclosing the personal information. Again, given the seriousness of the circumstances under which this exemption would be invoked, it would not be difficult for an agency to justify why the secondary use or disclosure would be necessary.

Required or authorised under a law

The privacy obligations are subject to all other Acts dealing with the collection, storage, handling, accessing, amendment, management, transfer, use and disclosure of personal information.[10] This means that if another law requires that personal information be dealt with in a certain way, the other law must be applied first. Some examples include agency authority to compel the provision of personal information and authorising provisions in emergency management laws. When a disclosure of personal information is made in accordance with another law, there can be no privacy breach.

The reverse is not the case. It is a common misconception that the privacy obligations are an authorising provision to disclose personal information, particularly when it comes to satisfying legislative confidentiality obligations. This is not correct. The IP Act does not override other legislation. Compliance with the privacy obligations applies to the IP Act only; it does not override confidentiality obligations in other Acts and cannot be used as a defence for being non-compliant with other legislation.

Consent

Consent is a strong permission. An individual can expressly or impliedly agree to a secondary use or disclosure of their personal information by an agency, or to the sharing of their personal information between agencies. An individual can also give express agreement to their personal information being transferred overseas, such as where it will posted on a website or social media site.

While it may commonly occur to an agency to ask for consent at the time of the secondary use or disclosure, there is nothing in the privacy principles that would prevent consent being obtained in advance of a disaster event, with the agreement then being relied upon should a disaster occur.

[10] Section 7(2) of the IP Act.

What protections are offered by the IP Act in the event of a disaster?

While there are generous flexibilities available to an agency in the secondary use and disclosure obligations in the event of a disaster, there are also provisions that ensure that the agency's dealings with personal information remain fair, particularly after the disaster event. The following protections remain, regardless of the fact that the initial information sharing occurred in the context of managing a disaster event.

Collection

Regardless of whether an agency sources the personal information from the individual themselves, another government agency or a third party, the agency must only collect/obtain information that is necessary for a purpose directly related to one or more of the agency's functions or activities.[11] The collected information must also be relevant to that purpose, and complete and up-to-date.[12]

Storage and security

Once an agency receives personal information from another source, it becomes responsible for protecting that information from loss, unauthorised dealings and any other misuse.[13] Individuals also have a right to seek access to and, as necessary, amendment of, this information from the agency that holds the information.[14]

Secondary use and disclosure.

An agency that has obtained personal information for the specific purpose of managing a disaster event is limited to other uses to which it could put the information. The agency is similarly limited in being able to itself provide personal information it has sourced from one agency to someone else.[15]

For additional information and assistance please refer to the OIC's 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 18 December 2015 and Last Updated 18 December 2015

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

[11] IPP 1 or NPP 1.
[12] IPP 3
[13] IPP 4 or NPP 4.
[14] IPPs 6 and 7 or NPPs 6 and 7, and Chapters 3 of the *Right to Information Act 2009* and the IP Act.
[15] IPP 10 and NPP 2.