FACT SHEET Personal Information Disclosure in an Emergency



When can you share personal information in an emergency?

Know your responsibilities.

We are all at the mercy of Mother Nature, especially during a Queensland summer. Get Ready Queensland reported that Queensland is the most disaster impacted state in the country, so it makes sense to be prepared and plan ahead before an emergency happens.

Bushfires, floods, cyclones, and disease outbreaks can occur without notice. As a member of the Queensland public service, it is important to know your privacy obligations and when it is appropriate to share personal information held by your agency (for example, with other departments or emergency services).

Understanding the basics of what should and should not be done with information sharing is critical, especially during emergencies, as it strengthens your agency's response effort.

Timely exchange of accurate, complete, and up-to-date information can protect the vulnerable and help save lives in emergencies.

That is why the OIC is encouraging Queensland public sector agencies and staff to understand their privacy responsibilities this disaster season:

- Know about the flexibilities in the *Information Privacy Act 2009 (IP)*
- Know how to apply them in an emergency event.
- Know your agency's information sharing strategy.

The IP Act contains protections and provisions for personal information held by Queensland public sector agencies. There are also flexibilities built in for emergencies, for example, when it comes to secondary use and disclosure, where the health and safety of individuals may be at risk.

Agencies can prepare for privacy and sharing information in an emergency by developing an information sharing strategy. This helps agencies by:

- anticipating the situations that may result in requests for personal information.
- establishing policies before an emergency occurs
- supporting staff to respond confidently and quickly to emergencies
- reducing the risk of personal information being handled inappropriately during an emergency
- ensuring agencies are mindful of other legislative provisions that may impact information sharing (i.e. confidentiality provisions).
- Being part of the Queensland public sector, there is a responsibility to be prepared and ready to respond in emergency situations. Understanding privacy obligations and flexibilities within the IP Act and understanding your agency's information sharing strategy can help everyone to respond confidently, accurately, and quickly in an emergency.
- It also means agencies are in a better position to reduce privacy risks and potential breaches, while also building greater trust with Queenslanders.

Follow the link below to find out more about Privacy and Information sharing during an emergency event from the Office of the Information Commissioner Queensland.

https://youtu.be/3KeAJfZmoJE

What is personal information?

Section 12 of the *Information Privacy Act 2009*

Personal information can be almost any information that is associated with an identifiable living individual. It can include correspondence, audio recordings, images, alpha-numerical identifiers, and combinations of these.

For information to be personal information two criteria must be satisfied.

- It must be about an individual.
- The individual's identity must be reasonably ascertainable from the information or opinion.

Information does not have to be true in order to be personal information and it does not need to be written down or recorded in another material form, such as a photograph or audio

recording. It can be spoken or communicated in another way, for example, by sign language.

Visit the Office of the Information commissioner Queensland website to read more on "What is personal information checklist."

what-is-personal-information-checklist

Examples of personal information

The definition of personal information is very broad and it captures a large amount of information. Examples of personal information are:

- a person's name, address, phone number or email address
- a photograph of a person
- a video recording of a person, whether CCTV or otherwise, for example, a recording of events in a classroom, at a train station, or at a family barbecue
- a person's salary, bank account or financial details
- allegations of wrongdoing against a person or details of wrongdoing or offences they may have committed.
- details about a person's land ownership or disputes to do with their land.
- details about a person's education or education activities, such as what degree they possess or their candidature for a PhD.
- the fact that a person is a member, or leader, of an association and their attendance at meetings.
- a person's medical details or health information
- a person's fingerprints or blood type
- details about a person's religious or sexual preferences
- details about a person's membership of a trade union or professional body.

Personal information includes some information that people may not normally consider to be private. For example:

- a work email address or phone number
- opinions given as part of a person's employment.
- the fact that a person is the author of a report.
- a person's name appearing in work documents.
- a letter written in a person's official capacity, such as a letter from the president of a club.

However, this does not necessarily mean that the routine personal work information of public servants is not appropriate to be released. See the Guideline: Routine personal work information of public sector employees for more information on this issue.

Privacy and managing disaster events.

In common with the rest of Australia, disaster events such as tropical cyclones, floods, bushfires, and storms can occur in Queensland at any time. A disaster event can include the serious disruption in a community caused by the impact of a pandemic.

A pandemic is a critical health issue which will directly affect many people's health, safety, and well-being. 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 and a flu season which may see, for example, an increased risk of an outbreak of human influenza.

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, which requires a significant coordinated response by the State and other entities to help the community recover from the disruption.

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.

Tip

The capacity to identify a person is a key component of personal information. Aggregated or de-identified data does contain personal information 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 enroute 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 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.

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.

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, Information Privacy Principle 11, and section 33 all allow dealings with personal information where:

…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. 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 be 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.

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. The collected information must also be relevant to that purpose, and complete and up to date.

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. 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.