Applying the legislation

GUIDELINE Information Privacy Act 2009

Privacy flexibilities in disaster management: information sharing scenarios

The privacy principles in the Information Privacy Act 2009 (IP Act) provide generous flexibility for disaster event managers and other Queensland public sector entities to deal with personal information in a range of circumstances as indicated below.

Key points to note include:

- privacy obligations only apply where there is personal Information (information about a living person who can be identified directly, or reasonably indirectly, from the information)¹
- personal information can be used or disclosed where it is reasonably necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare²
- aggregated or de-identified data is less likely to raise privacy issues and could be used where the identity of individuals is not needed (e.g. “two people with diabetes, four pregnant people, two elderly people and five children are currently in the evacuation centre”)
- the IP Act applies to Queensland public sector agencies including the Department of Communities, Disability Services and Seniors, Queensland Fire and Emergency Services, Queensland Police Service (QPS), local governments, and State, district and local disaster management groups³
- Consent is a strong privacy ‘permission’ – always ask where practicable⁴; and
- other legislated restrictions about confidentiality may apply and will override privacy obligations⁵.

Information sharing scenarios

Scenario 1: Healthcare workers and providers need access to timely, accurate and comprehensive clinical information and advice in order to effectively manage patients in a pandemic situation.

In the event that a public health or general emergency is declared, orders issued under public health legislation could require the collection, use and disclosure of certain personal information relating to employees and customers. In this event if it is necessary to collect, use or disclose these individuals’ personal information,

¹ Section 12 of the IP Act; see What is Personal Information for more information.
² Information Privacy Principle (IPP) 10(1)(b) and IPP 11(1)(c); see Use or Disclosure to Prevent Harm for more information.
³ Sections 18 and 21 of the IP Act
⁴ IPP 10(1)(a) and IPP 11(1)(b); see Key Privacy Concepts: agreement and consent.
⁵ Section 7(2) of the IP Act. See for example, sections 186-188 of the Child Protection Act 1999.
the specific legislative authority that is relied upon can be communicated to the subject individuals.

Otherwise, if the general exceptions to the privacy obligations in the IP Act are sought to be relied on, agencies must be able to demonstrate that their dealings with the personal information are necessary to lessen or prevent a serious threat to life, health, safety or well-being.

Scenario 2: In the event of a declared pandemic, agencies may need to collect, use and share the personal information – including medical information – of their employees in order to manage health and safety considerations, ensure continuity of service delivery, and to report on the impact.

Agency dealings with the personal information of their employees is necessary for the effective management of the workforce and is routinely collected, used and shared for this purpose. However, this event may require dealings with novel personal information such as medical information and information about domestic arrangements such as travel plans and history, and personal relationships including children and living arrangements.

The flexibilities in the privacy principles for the lessening or prevention of a serious threat to life, health, safety or well-being are broad enough to cover off most dealings with this information. However, given the sensitivities of the information involved, agencies should consider minimising what they collect, who has access to the information, what it is used for and who outside of the agency it is disclosed to.

It is recommended that in any dealings with this information, the process is both transparent and clearly communicated to the employees.

Scenario 3: The Queensland Government wants to release geo-coded information about damage to a large number of individual properties to ensure the community better understands the danger to the community in accessing the area.

Even where such information included personal information, it is likely that it could be released as the agency could reasonably be satisfied it was necessary to prevent or lessen a serious threat to public safety.

Scenario 4: Managers of evacuation centres may wish to release specific information about registered occupants to recovery agencies so that their individual needs can be serviced better.

Consent should be obtained where possible, particularly if sensitive information such as health information is involved. In some cases, it will be appropriate to rely on implied consent where it is impracticable to obtain consent and had consent been obtained, the individual would have consented. For example, an agency could usually assume that it could imply consent where the individual would benefit from the use of the information. However, if a person does not give or
subsequently retracts their consent the agency will need to factor this into their management of the individual.

Scenario 5: Managers of evacuation centres may want agencies with a knowledge of those who pose a risk to other members of the community to share that information about people on the registered list of occupants so that mitigation strategies can be put in place.

Other Queensland public sector agencies such as QPS, the Department of Child Safety, Youth and Women, and the Department of Communities, Disability Services and Seniors also have obligations under the IP Act. The IP Act permits an agency to share personal information where it is to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare. However often agencies also have strict confidentiality requirements they must comply with under other specific legislation about certain information and may therefore be restricted from sharing information. Information obtained must be stored securely.

Scenario 6: A disaster management group needs to use a range of media, including social media such as Twitter and Facebook, to communicate critical information for the community.

Where possible use de-identified information, aggregated information or information that is about property that would not identify individuals when publishing online. Alternatively, obtain the person’s agreement to use the personal information where practicable. In some cases, legislation authorises certain information to be posted on an agency’s web-site (only). Where there is a serious threat to health or safety the IP Act permits agencies to publish information online, however once the threat passes the information must be removed from the internet.

Scenario 7: Information collected during post-disaster interviews may be useful to a variety of organisations to assist with response and recovery activities, but may have been collected without the necessary privacy release declaration.

De-identified and aggregated data may able to be provided without revealing personal information, following appropriate risk assessment and treatment of data. If more specific information that would identify an individual is required, consider whether consent can be obtained or whether consent would be implied in the circumstances. More sophisticated deidentification techniques such as homomorphic encryption, synthetic data or use of closed data sets can be invoked. For research release and use might be strictly controlled as closed data with limits on use and publication and subject to strong confidentiality obligations. The information can also be shared where it is to prevent or lessen a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare.
Accessing information from Australian Government agencies

Entities responsible for disaster management at State, District and Local level may require personal information from Australian Government agencies to assist in providing appropriate services. Australian Government agencies are required to comply with similar Commonwealth privacy legislation when disclosing information. Such legislation has equivalent flexibility for sharing personal information for health and safety and law enforcement purposes.

For example, local governments may want to know information about individuals who may be vulnerable during a disaster, such as people with disabilities living independently, who may receive assistance from the Australian Government. When requesting information it will be important to explain the purpose for collecting the information and how it will be used. It is important that the information is kept up to date and accurate, and stored securely.

For additional information and assistance please refer to Privacy and managing Disaster Events or contact the Enquiries Service on 1 800 642 753 or by email on 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 21 January 2015 and Last Updated 30 March 2020

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