Information Privacy and Contracted Providers of Seniors Support Services

The Office for Seniors is part of the Department of Communities, Disability Services and Seniors (the department).

The department engages contracted service providers to deliver support and services on its behalf to older Queenslanders. In the course of providing support and services to older Queenslanders, many contracted service providers will handle personal information on behalf of the department.

Personal information is defined by section 12 of the *Information Privacy Act 2009* (the Act) as *information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent or can reasonably be ascertained, from the information or opinion.*

Individual means a natural person rather than a company or corporation.

Binding Contracted Service Providers

Contracted service providers handle personal information on behalf of the department, so the standard terms of the department's contracts and agreements will almost always bind contracted service providers to comply with the relevant provisions of the Act.

General guidance on the Act may be found on the website of the Office of the Information Commissioner (OIC) at http://www.oic.qld.gov.au. If a contracted service provider remains unsure of its obligations, it should obtain independent legal advice.

The Queensland Council of the Ageing may also be in a position to support service providers. Further information is available at www.cotaqld.org.au.

The purpose of this fact sheet is to explain the nature of the obligations that contracted service providers have when contracting with the Department to provide services. This fact sheet does not include specific guidance as to how the obligations under the Act should be performed because this is a matter for each provider having regard to how they operate their business, their size and resources.

Obligations

A bound contracted service provider is required to comply with the Queensland Information Privacy Principles (IPP) in Schedule 3 of the Information Privacy Act 2009. Health agencies are required to comply with the National Privacy Principles in Schedule 4 of the Queensland IP Act. Contracted service providers are also required to comply with section 33 of the IP Act. This provision prohibits the transfer of personal information outside Australia except in limited circumstances. It is important to note that a transfer of personal information outside Australia may occur if a contracted service provider's computer systems involve personal information being transferred to service provider based overseas.

Complaints

If a person alleges that a bound contracted service provider has breached an IPP in respect of their personal information, it is the contracted service provider's responsibility to deal with the complaint.

If a complainant is dissatisfied with the bound contracted service provider's response, the complainant may take the complaint to the OIC. The OIC will attempt to resolve the matter through mediation. If that process fails, the matter may be referred to the Queensland Civil and Administrative Tribunal (QCAT) for a hearing. QCAT may make a variety of orders, including an award of compensation of up to $100,000 per breach against the contracted service provider.

Breaches

Aside from requiring bound contracted service providers to comply with the IPPs and section 33 of the Act, the standard terms of the department's contracts require bound contracted service providers to notify the department of any breach of the privacy obligations under the IP Act or the contract or agreement.

A breach of privacy may involve the privacy of a single individual or it may involve the general loss of data. For example, a bound contracted service provider's computer system could be hacked or a laptop may be lost or stolen. In circumstances such as these, the department will want to ensure that any potential harm is avoided or minimised. For this reason, the department must be advised of any privacy data breaches where they concern the personal information under the service agreement.

Once a breach is notified to the department, it is expected that a bound contracted service provider will continue to manage the breach responsibly and in accordance with its legal and contractual obligations.

Other legislation

The IP Act is subject to other legislation that may specifically restrict the disclosure of information. e.g. the *Disability Services Act 2006.* The department expects that each bound contracted service provider will be aware of any relevant legislation.

In addition to its obligations under the Queensland Act, contracted service providers may also have obligations under the Commonwealth *Privacy Act 1998* which arise from funding or service agreements with entities other than the Queensland government. It is important to note that the Commonwealth Act will not override the Queensland IP Act, or any of the terms in its contract with the department (see sections 3 and 7B of the Privacy Act).

The IPPs summarised below govern the collection, use and disclosure of all personal information, and require that it be kept secure. Whenever a bound contracted service provider proposes to collect or deal with personal information in any way, the service provider must consider whether what they propose complies with the IP Act.

The Information Privacy Principles

The IPPs set out how personal information is to be collected, handled and accessed. Consult the Act for the full requirements, but in summary, the 11 IPPs provide the following:

IPP1 – Collection of personal information must be lawful, fair and necessary for the agency's functions.

IPP2 – Where an individual is requested to provide personal information, the agency or bound contracted service provider must advise the individual of the purpose of the collection, any laws which give the agency/service provider authority to collect the information, and to whom the agency/service provider usually discloses or gives the information.

IPP3 – Personal information that is collected must be relevant, up-to-date and complete. The collection must not be an unreasonable intrusion into the personal affairs of the individual.

IPP4 – The agency/service provider must ensure that personal information is protected against loss, unauthorised access or other misuse. The safeguards must be *'adequate to provide the level of protections that can reasonably be expected to be provided.'*

IPP5 – The agency/service provider must ensure individuals can find out what personal information is held about themselves.

IPP6 – The agency/service provider must give the individual access to their personal information unless the law allows for a refusal. For example, the Act allows the exemption from disclosure of information that is either conditionally or unconditionally exempt under Schedules 1-4 of the *Right to Information Act 2009*.

IPP7 – An individual has the right to require correction or amendment of their personal information, or alternatively the agency must attach a statement of correction.

IPP8 – Before using personal information, an agency must take reasonable steps to check the information is accurate, complete and up to date.

IPP9 – An agency must only use personal information for its original intended purpose. For the definition of 'use', see section 23 of the Act.

IPP10 – An agency may only use personal information for its original intended purpose subject to the listed exceptions.

IPP11 – An agency may only disclose personal information in the listed circumstances. For the definition of 'disclose', see section 23 of the Act.

Policy and Practice

The department recommends each contracted service provider have a privacy policy that outlines how they will meet the requirements of the IP Act.

Common issues

Information Privacy issues that commonly arise include:

- The nature and amount of personal information that is collected to fulfil functions; IPP1 prohibits the collection of excess information.
- Collection or privacy notices – IPP2.
- Systems required to keep personal information secure – the more sensitive the information the greater the care that needs to be taken to secure the information - IPP4. Policies and practices are likely to be required for:
    - Physical security of files and computers within offices
    - Prevention of unauthorised access or inspection (e.g. keeping desks clear of personal information, ensuring that access to electronic personal information is password protected
    - Rules about the removal of files, laptops etc. from the office and keeping them safe from loss or theft
    - Quiet spaces for sensitive conversations with service users
- Decisions whether particular personal information may be lawfully disclosed to, or shared with a family member, another service provider or agency (IPPs 8-11)

The OIC www.oic.qld.gov.au provides information, advice and training on meeting privacy obligations and can be contacted for advice on telephone: (07) 3234 7373 or free call 1800 642 753.