13 November 2013

UnitingCare Community

State Office
117 Gipps Street Fortitude Valley Q 4006
PO Box 491 Fortitude Valley Q 4006

Phone 07 3250 1900
Fax 07 3250 1810

ABN 28 728 322 186

www.uccommunity.org.au

RTI and Privacy Review
Department of Justice and Attorney-General
GO Box 149
BRISBANE Qld 4001

Submit via email to: FeedbackRTIandprivacy@justice.qld.gov.au

This submission is made on behalf of UnitingCare Community and Blue Care which are community service providers within the UnitingCare Queensland group. We are pleased to have the opportunity to make a submission on the operation of the *Information Privacy Act 2009* which is enclosed as a separate document.

I would also like to draw your attention to the Chapter 6 Protections and Offences provisions of the *Information Privacy (*IP) Act, which is not one of the questions posed in the discussion paper. It is arguable that a bound contracted service provider comes within the operation of subsection 183(1) because of the operation of paragraph 183(3)(d). However by contrast, a bound contracted service provider does not appear to be included among those protected by subsection 179(1) from an action for defamation or breach of confidence which appears to protect only "the State, an agency or officer of an agency because of the authorising or giving of the access". I ask that these provisions be also given attention in this review, and amended so that their application to bound contracted service providers is put beyond doubt and made clear and unambiguous.

Although the *Right to Information* (RTI) Act does not apply to UnitingCare Community, there is one very relevant question listed in the Discussion Paper of the Review of the RTI legislation that we wish to comment on in the remainder of this cover letter, namely:

> **Documents of contracted service providers, p14.**
>
> **4.6 Should the RTI Act and Chapter 3 of the IP Act apply to the documents of the contracted service providers where they are performing functions on behalf of government?**

Our view is that documents of bound contracted service providers which are not for profit (NFP) community service providers should not be subject to either the RTI Act or Chapter 3 of the IP Act for two reasons.

Firstly, from our experience there is no demand from our service users for access to our documents, other than those containing personal information. As a bound contracted service provider UnitingCare Community is required to comply with the Information Privacy Principles. UnitingCare Community complies with IPP6 in providing a person with access to their personal information if they ask for it. Therefore, application of access provisions under the RTI Act would only complicate the application of an existing provision already available to clients of the not for profit sector under the IPPs.

Secondly, if the RTI Act or Chapter 3 of the IP Act is amended to apply to bound contracted service providers, the effect, if taken up, would be to place the organisation under an excessive compliance burden. Currently if people wish to access UnitingCare Community documents not available through the application of the IPP 6, under our contractual obligations we must cooperate with any application made to the contracting agency concerning documents relating to service provision for which the organisation is funded. This satisfies transparency and accountability purposes. There are no public considerations to be met in making available to the general public the documents of a private not for profit organisation which do not relate to accountability for government funding.

If you have any queries or require further information please contact [redacted], Coordinator Legal Matters and Contracts on [redacted] or at [redacted]

Yours sincerely

[redacted]

Acting Executive Director

Encl

Confusion and complexity in privacy across Australia

This submission addresses the questions asked in the discussion paper from the perspective of a community services sector not for profit (NFP) organisation. Increasingly government at all levels is contracting out the provision of community services to the NFP sector. NFPs collect a lot of personal information in the course of the delivery of community services.

The primary purpose of privacy legislation is to protect the privacy of citizens as they access services. NFPs with a turnover of more than $3M are required to comply with the Commonwealth legislation, the *Privacy Act 1988*, and privacy principles. This legislation has been amended with the new Australian Privacy Principles (APP) to come into operation in March 2014.

NFPs which receive funds under service agreements with the Queensland government are also required to comply with the Queensland legislation, the *Information Privacy Act 2009*, (IP Act) and either the Information Privacy Principles (IPP) or the National Privacy Principles (NPP) or both. Understanding two separate privacy regimes is an excessive administrative burden for service providers and is too difficult to understand for service users and providers alike. Service providers are confused about what they need to do to achieve compliance with limited resources. Consumers are unlikely to know what their rights are or how to take advantage of the protections the legislation is supposed to provide for them. A single privacy system which is not overly prescriptive can meet both service user and provider interests and reduce compliance costs for the provider. This would of course be of interest to governments that desire efficient outcomes from community sector organisations, from which the government purchases services through grant funding.

When the National Disability Insurance Scheme (NDIS) comes into operation NFPs will need to comply with the Commonwealth APPs if their turnover exceeds $3M. Some will continue to have to comply with the Queensland regime. Compliance will need to be efficiently managed to minimise the cost being passed on to service users in a competitive market.

Accordingly, the general proposition of this submission is that there should be only one statute and one set of privacy principles applicable to NFPs. NFPs have already committed resources to become compliant with the APPs when they come into operation in March 2014. Queensland should align the IPPs with the APPs, or adopt the APPs in Queensland so that NFPs which are also Queensland government funded, do not have to comply with two privacy regimes.

Considering the Australian Privacy Principles (APPs) in Queensland

1.0 What would be the advantages and disadvantages of aligning the IPPs with the APPs, or adopting the APPs in Queensland?

(a) The advantages from a service user perspective:

Having only the APPs instead of the APPs and the IPPs or the NPPs (or both) will be less confusing and easier for service users to understand. Service users will be better able to exercise their rights and to interact more meaningfully with service providers about privacy issues. Clients should better understand what they are agreeing to when they give consent. There will be only one complaints and enforcement system.

Service users may better understand when it is desirable or necessary for personal information to be exchanged between entities for planning, research and service delivery purposes and to actively communicate with service providers in considering these issues. This should contribute to consumers developing a better understanding of service delivery issues, improved communication and engagement with service providers and an increased sense of trust. This will be particularly relevant when the NDIS system comes into operation.

(b) Advantages from the service provider perspective:

Unquestionably Queensland adopting the APPs or aligning the IPPs and the NPPs with the APPs would be the most cost efficient and effective way for NFP bound contracted service providers to implement privacy protection processes and systems and train staff.

Service providers will not have to expend excessive resources in trying to understand whether they are required to comply with either or both Commonwealth and Queensland regimes. Establishing and maintaining a single privacy compliance system and processes based on only the one set of principles will be easier and cheaper for NFPs.

Those resources of the Office of the Information Commissioner Queensland's (OICQ) which are devoted to managing bound contracted service providers are directed towards agency compliance, rather than assisting service providers to meet their obligations. The OICQ does not provide privacy training for NFPs although it does for government departments even though they have more resources than NFPs have at their disposal. This responsibility is placed on government departments:

> *Agencies should be aware that a bound contracted service provider may have little experience in managing applications for access or amendment. Agencies should make themselves available to their bound contracted service providers to offer the necessary support and guidance.*
>
> *Hint*
>
> *Building a process into the contract so that agency handles application for access to and amendment of personal information under the relevant privacy principles on behalf of the bound contracted service provider would ensure that these applications are dealt with in a way that best serves the public interest.*[1]
>
> ***Compliance with the privacy principles***
>
> *Once a service provider becomes a bound contracted service provider, it is required to comply with the privacy principles while meeting its obligations under the service arrangement.*
>
> *Hint*

[1] OIC guidelines: "Interpreting the Legislation – Information Privacy Act 2009 Privacy Guideline Section 5 – Contracted service providers" and "Applying the legislation GUIDELINE – Information Privacy Act 2009 Contracted Service providers", 2.3 on page 5

> *Simply stating in the contract or other arrangement that the bound contracted service provider is to comply with the relevant sections may not be sufficient to satisfy section 35. An agency should consider setting out how the bound contracted service provider is to comply, particularly with regards to the access and amendment privacy principles.*[2]

The adequacy of clause 20 of the Service Agreement (Part A) – Standard Terms of Funding published by the Department of Communities, Child Safety and Disability Services and the terms contained within the new draft are arguable. The statutory and contractual regime is complex, unclear and confusing.

By contrast, the APPs provide reasonable guidance without being overly prescriptive. If there is only one set of principles with which to comply, then there is only a single authority and set of terminology and definitions. The Commonwealth requirements are contained in the legislation and principles and do not require additional terms to be added to a contract to achieve effectiveness.

No disadvantages from either service user or provider perspectives are evident.

(c) Perceived advantages from the government perspective:

From a state government perspective, it would seem desirable that all reasonable options be adopted to minimise the administrative costs of managing the regulation of grant funding. This was noted in the recent Queensland Commission of Audit as most costly (grant administration cost per $100 funding) in the community services sector. It stands to reason then, that there is a natural incentive for the state government to seek to decrease its costs by removing the duplication of applying legislation adequately addressed by Commonwealth legislation. Adoption of the federal regime would automatically release the state from administration of the legislation over community organisations, thus effecting significant public sector savings, which would be welcomed by service users and provided, in addition to the state government.

Sharing Information

2.0 Does the IP Act inappropriately restrict the sharing of information? If so, in what ways? Do the exceptions need to be modified?

It is arguable that the IPPs do not inappropriately restrict sharing of information. However it is unclear. There are at least two broad circumstances which need to be considered. The first is for transfer of information about a client where an organisation is providing a service to the person and the person does not want to have to repeat the same information a number of times to one or more services to which the person is referred. It should not be material whether any of the organisations is a government department or not, because the purpose is to provide a service to the client. This kind of information sharing should be permitted and should be clearly stated (and not in a roundabout way). The client's consent would be actual or implied because the organisation making the referral would discuss the referral with the person being referred.

The second is where two or more organisations whether or not one or more is a government department need to share information about services provided to people. In this setting, the sharing is not related to the provision of a service to a particular person, but is about the service provision

[2] OIC guideline "Interpreting the legislation" page 3 at point 2.0

which might include the characteristics of the people to whom the service/s is/are provided. The information is needed for planning or budgeting or research or service improvement or one of the kinds of activities modern service providers, be they government departments or government funded NFPs, engage in for the purposes of providing quality, responsive services effectively and efficiently. This kind of information sharing should be permitted and should be clearly stated and not in a roundabout way. If the transfer is not for actual service provision the information can be 'de-identified', and consent should not be needed. If it is for service delivery the person would need to be identified.

If privacy principles do not clearly and unambiguously permit these kinds of information sharing, amendment needs to enable it.

When a NFP considers the issue of sharing information about a client (or a staff member or volunteer) the very real difficulty they confront is which legislation and privacy principles apply and then to what extent is that affected by contractual terms and conditions.

Again having to comply with only the APPs would decrease the administrative burden. It is preferable to have one set of legislative requirements in the form of the APPs, which are not tied to contractual terms other than (if necessary) that the service provider is required to comply with the APPs or however the Queensland legislation aligns with or adopts them.

Definition of 'personal information'

3.0 Should the definition of personal information in the IP Act be amended to bring it into line with the definition in the Commonwealth Privacy Amendment Act 2012?

If the preferred position of adopting the APPs or aligning Queensland and Commonwealth legislation accordingly is not adopted, it would be crucial to bring the definition of 'personal information' in the IP Act into line with the Commonwealth definition. Understanding the definition is fundamental to managing privacy compliance. It would be just chaotic to have two definitions. Furthermore, the new Commonwealth definition is simpler and does not significantly change the scope.

Definition of 'agency' – Government Owned Corporations

4.0 Should government owned corporations in Queensland be subject to the Queensland's IP Act, or should they continue to be bound by the Commonwealth Privacy Act?

These entities should remain within the operation of the Commonwealth Privacy Act which provides a comprehensive regime. They will be expending resources to achieve compliance with the amendments to commence in March 2014.

Transfer of personal information outside Australia

Technology issues

5.0 Should section 33 be revised to ensure it accommodates the realities of working with personal information in the online environment?

Any changes to section 33 which would provide more certainty as to its application to common business arrangements and technology uses are supported. This could be done by amendment to section 33 to clarify its application, or by the release of more detailed guidance and the provision of

more support by the OICQ in terms of education and advice. The resources made available online by the OICQ are of only limited help. More assistance in determining the application of provisions such as section 33 to our particular circumstances would be appreciated.

Cloud computing
Personal information published on agency websites
An alternative approach to transferring personal information

6.0 Does section 33 present problems for agencies in placing personal information online?

7.0 Should an 'accountability' approach be considered for Queensland?

The approach taken in the APPs should be adopted for the simple reason that, as is acknowledged in the discussion paper, this is an exceedingly complex and rapidly changing area. NFPs within the scope of the Commonwealth legislation will be required to comply with APP 8 from March 2014. This is another reason NFP organisations should have to comply with only one set of legislative requirements. If the APPs are adopted for Queensland, the Commonwealth and Queensland governments can work together and consult with NFPs about the issues concerning electronic information technology systems for business and service delivery purposes and transactions.

Although section 33 does not currently provide problems for our organisation by itself, its application and lack of consistency with APP 8 which applies to the delivery of services by us pursuant to Commonwealth government contracts does cause us issues. The lack of consistency imposes a significant compliance burden on our organisation in having to meet the requirements of different regimes. As a service provider for both Queensland and Commonwealth government agencies, as well as being an entity carrying on business in Australia, our organisation must comply with the Commonwealth Privacy Act as it applies to private sector entities and as it applies to agencies in the context of delivery of Commonwealth funded services (there are still distinctions in the new APP 8) as well as with the Queensland IP Act where required by our contracts with Queensland Government agencies. Consequently we would support a consistent approach to cross-border data flows. Although we do not regard APP 8 as providing the best possible alternative to section 33, we must comply with it from March 2014 and we seek to have to comply with only one regime.

The adoption of an accountability approach which would be more acceptable to our clients and other stakeholders is supported, recognising that it is important for regulation to reflect the community's expectations. However the APP 8 accountability model could be improved because provisions of APP 8, particularly the exceptions, are difficult to understand and apply and are likely to give rise to uncertainty. Nevertheless one regime is better than two. (Adoption of a framework similar to that proposed by the Australian Law Reform Commission, which is more consistent with international frameworks (such as the APEC Framework and the OECD Privacy Guidelines) would have been preferable.)

Our organisation will continue to bear a significant compliance burden unless the Queensland and the Commonwealth Governments can agree on a satisfactory consistent approach to regulating cross-border data flows. It would significantly reduce our compliance burden if it could be recognised that bound contracted service providers to the Queensland Government were compliant with their section 33 obligations if they meet the requirements of APP 8. That would mean that we

could determine in the context of different service obligations whether it would be more appropriate for us to comply with the Queensland or the Commonwealth government cross-border data flow regime.

Clause 20 in Department of Communities, Child Safety and Disability Services Service Agreement (Part A) – Standard Terms of Funding, and any other similar government terms and conditions may need to be amended to enable the simplification of these privacy requirements.

Privacy Complaints – a standard approach

8.0 Should the IP Act provide more detail about how complaints should be dealt with?

The discussion paper raises the lack of procedures for handling complaints to agencies when compared with the "very detailed processes specified for applications for access to and amendment of personal information held by an agency". In this regard, service users of NFP bound contracted service providers are doubly disadvantaged in that they do not have the benefit of a process for getting access to personal information much less for making a complaint to the organisation about access or any other privacy matter.

Chapter 5 of the IP Act deals with complaints to the Information Commissioner. It expressly provides for a person to make a complaint about a NFP which is a bound contracted service provider (see sections 164 – 166). A number of provisions of the IP Act require a bound contracted service provider to comply "as if it were the agency" (see subsection 35(1)) or "as if it were the entity that is the contracting agency" (see subsection 36(1)) or "as if it were an agency" (see subsection 36(3)). This is hardly precise and is very unsatisfactory as it provides no real guidance for the service provider and is of little assistance to the service user in trying to obtain compliance. Clause 20 of the Standard terms and conditions (part A) is of little assistance.

By contrast APP 12 provides a process for giving access and provides more assistance to the organisation for when it may refuse to give access because it provides a more detailed articulation of the relevant circumstances (see APP 12.3). APP 12 recognises the limited administrative resources of a NFP bound contracted service provider while at the same time providing guidance to the service provider. This also better informs the service user what they can expect from the service provider.

APP 12 is not overly prescriptive as to the timeframe for giving access requiring only that it be "within a reasonable period after the request is made" and that access to the information is given "in the manner requested by the individual if it is reasonable and practicable to do so" (see APP 12.4.(a)(ii) and (b)). APP 12.5 provides that access may be given "in a way that meets the needs of the entity and the individual". An organisation may charge for giving access "which must not be excessive" (APP 12.8) and must give reasons for refusal and information about the complaints mechanisms (APP 12.9 and 10). As indicated above, such provisions have the potential to improve service user and provider communication and engagement.

It is considered that a process for making complaints about a breach of the privacy principles over and above the organisation's general complaints procedure would be unnecessary if the APPs are adopted. APP 1 requires the publication of a privacy policy about the management of personal information by the entity (APP 1.3) which must include how an individual may complain about a breach (APP 1.4(e)), which in turn could be the general complaints procedure.

Privacy complaints – timeframe for resolving

9.0 Should the IP Act provide more flexibility about the timeframe for complaints to the OIC to be lodged?

The APP system should apply. But failing this, if this has been causing significant problems then amend the statute accordingly – otherwise leave it alone.

Powers of the Privacy Commissioner

10.0 Are additional powers for the Information Commissioner to investigate matters potentially subject to a compliance notice necessary?

The Information Commissioner's powers need to be sufficient to investigate alleged breaches. The Commonwealth provision as set out in the discussion paper adequately addresses the issue and should be adopted for Queensland.

Person acting as an agent for a child

11.0 Should a parent's ability to do things on behalf of a child be limited to Chapter 3 access and amendment applications?

According to the OICQ and the Department of Communities, Child Safety and Disability Services Chapter 3 does not apply to NFPs which are bound contracted service providers which, on this view, are not subject to any procedural requirements for access and amendment. The question itself is troublesome because "a parent's ability to do things on behalf of a child" – if this means making decisions for a child (i.e. a person under 18 years of age) – is the responsibility of a parent unless the child is assessed as Gillick competent. Where a child is assessed as Gillick competent, the young person is able to make his or her own decision. This should be applicable to the operation of the IP Act.

Generally available publication

12.0 Should the definition of 'generally available publication' be clarified? Is the Commonwealth provision a useful model?

Adopting the Commonwealth definition to include a document available for a fee as set out in the discussion paper would remove any lack of clarity in this respect.

IPPs specific to documents

13.0 Should the reference to 'documents' in the IPPs be removed; and if so how would this be regulated?

Unlike the IPPs, the APP's do not make reference to a document or record containing the relevant information or in a repository which it is held. It would seem that for the APPs it must be implied that the principles mean the relevant information contained in a document or record.

It is difficult to imagine how an entity might hold or control information if it is not in a document or record of some sort other than if it is held in a person's mind which presents its own different problems. It this is what this issue is driving at, then perhaps this aspect of the issue is best left to

mechanisms for managing human conduct such as for maintaining confidentiality or more generally in a code of conduct.

IPP4 - element of reasonableness

14.0 Should IPP 4 be amended to provide, in line with other IPPs, that an agency must take reasonable steps to ensure information is protected against loss and misuse?

This is a sensible approach. Compliance with this principle ultimately rests on appropriate risk assessment and control mechanisms being implemented within available resources and budget constraints. IPP 4 as currently worded requires actions as if the risk assessment was uniformly at a very high level across an entity's operations instead of proportionate to the actual circumstance. This may require a disproportionate allocation of resources away for other activities considered by the organisation to be of equal or higher priority to meet service user need.

For comparison, APP 11.1 provides:

> *11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:*
> *(a) from misuse, interference and loss; and*
> *(b) from unauthorised access, modification or disclosure.*

IPP 2 and 3 – 'Collect' information? Or 'ask for information?

15.0 Should the words 'ask for' be replaced with 'collect' for the purposes of IPPs 2 and 3?

This would be a sensible amendment. It would be consistent with the APPs and picked up by their adoption for Queensland.