Fact Sheet June 2019

Consent and Bundled Consent

Privacy laws in NSW sometimes require that an individual's consent is needed for an activity to occur. This fact sheet has been designed to provide guidance to NSW public sector agencies and Health Care Providers in understanding the issue of consent in relation to Privacy laws in NSW.

This Fact Sheet refers to the Information Protection Principles (IPPs) in the *Privacy and Personal Information Protection Act 1998* (NSW), and the Health Privacy Principles (HPPs) in the *Health Records and Information Privacy Act* 2002 (NSW).

NOTE: This Guidance is not intended to be legal advice for specific cases or a complete explanation of how privacy protection principles that raise consent issues need to be interpreted. It will assist organisations to refer directly to the text of particular statutory provisions that specific circumstances raise for consideration. Any reference to personal information in this fact sheet should be read to include health information.

The principle of an individual being able to not identify themself (unless necessary for some public interest purpose) is a cornerstone of privacy and data protection regimes. The relevant regimes contemplate the collection of limited information for a specific purpose (or identified purposes). The NSW Privacy laws provide for consent, necessity, limitations, security, and other protections for personal information. Where society decides that there are competing interests that should override those protections, then those societies approve exemptions, or other methods of obviating the requirements of privacy statutes. In summary:

- In the absence of another rule or exemption, secondary uses or disclosures of personal information will require the consent of the individual.
- To be valid, consent must be: voluntary, informed, specific, current, and given by a person with capacity.
- Unless otherwise indicated, consent can be express or implied, written or verbal.
- 'Bundled' authorisations may not meet the criteria for valid consent[1]

What is the difference between a privacy notice and a consent form?

What is a privacy notice?

A privacy notice is a one-way communication; it does not ask for a response from the individual. It simply states: 'this is what is going to happen with your personal information'. Notifying a person of what you intend to do with their information is not the same as seeking their consent to do those things. It is important to not confuse a privacy notice with consent.

What is the purpose of a privacy notice?

The purpose of a privacy notice is to provide accessible information to individuals about the use of personal information by the regulated entity.

It notifies individuals of the terms under which a regulated entity will provide a service or some other type of engagement with the public.

However, it is not a mechanism by which regulated entities may deal with personal information that deviate from their responsibilities under privacy legislation.

When is a privacy notice required?

There are routine primary and secondary uses or disclosures over which you offer the individual little or no choice. These are authorised on grounds other than consent, for example, when use or disclosure:

- is 'for a directly related secondary purpose'; or
- is required or permitted by another law; or
- is required or permitted under a different public interest exemption (for example s27A, Band C of the PPIP Act).

In such cases, you should notify the individual by way of a privacy notice under IPP 3 and HPP 4.

[1] *KJ v Wentworth Area Health Service [2004] NSWADT 84* at [55], [61]

What should a privacy notice contain?

It is recommended that a good privacy notice contain the following:

- be written in clear language the individual will understand
- be truthful and in no way misleading
- contain the following sections:
  - the categories of data collected / processed
  - why the data is collected (purpose)
  - how the data is used (processed)
  - the lawful basis for processing the data (where applicable)
  - how the data is stored and how long for, and how security is ensured
  - who / which organisations data is shared with and why
  - what those organisations will do with the data
  - individuals rights over their data (including right of access)
  - contact details (for queries)
- highlight any changes made to the way the personal data is processed.

This list is not exhaustive and regulated entities are expected to tailor the notice to meet their own requirements – covering any elements that are specific to them operating context.

What is consent?

Consent is a two-way communication. It asks the individual for their permission to use or disclose their personal information in a certain way, and the individual can respond with either 'yes' or 'no' to their personal information being use or disclosed in that way.

When is consent required?

Consent is relevant to the operation of a number of IPPs and HPPs. In some, consent is an exception to a general prohibition against personal information being handled in a particular way (for example, IPP 10 and HPPs 10 and 11). In others, consent provides authority to handle personal information in a particular way (for example HPP 12).

If a law governing a public sector organisation's operations includes prohibitions regarding a particular use or disclosure of personal information, a privacy notice may not be an appropriate way for the organisation to justify disclosures of personal information that the law prohibits. In such cases, consent will be required.

The five key elements of consent are:

- The individual gives consent voluntarily
- The individual is adequately informed before giving consent
- The consent is specific
- The consent is current
- The individual has the capacity to understand and communicate their consent.

When is consent voluntary?

Consent is voluntary if given without coercion or threat, and with sufficient time to understand the request and, if appropriate, take advice.

For consent to be voluntary the person must be free to exercise genuine choice to provide or withhold consent. They must be free to say 'no,' and still receive the primary service being sought. They must also be free to say 'yes,' but be able to at some time later change their mind and revoke their consent for future disclosure or use.

If a person has no practical alternative but to agree to the use or disclosure of their personal information in a particular way, an organisation should not suggest that they are seeking the person's consent for that use or disclosure. As such, acquiescence to a set of standard Terms and Conditions does not constitute valid consent. In other words, unless you actually give the person the choice of agreeing or disagreeing to what you propose, you are not seeking their consent. To be voluntary, consent must not be a pre-condition for receiving a government service, when the law governing the transaction does not otherwise permit the action the request for consent contemplates.

For example, an organisation may provide health, welfare or housing services to the public. If a member of the public exercises their right to request services from the organisation, it will not be appropriate for the organisation to request consent to disclose the applicant's personal information as a condition of the provision of services where laws that apply to the organisation prohibit or do not permit the particular disclosure.

When is consent informed?

A person must have reasonable knowledge of all the relevant facts including the implications of providing or withholding consent. Providing incorrect or misleading information may mean that a person's consent is invalid.

An organisation should ensure that an individual is properly and clearly informed about how their personal information will be handled, so they can decide whether to give consent.

How specific should consent be?

Consent should be as specific as possible. The level of specificity required will depend on the circumstances, including the sensitivity of the personal or health information. In particular, if the standard required is 'express' consent, the Tribunal expects the terms of a consent to be "precise as to the kind and, possibly, the exact contents of the information to which the consent relates."[2]

For example when designing a consent form, each request for a secondary use or disclosure should have its own box to tick.

What is 'bundled consent'?

Bundled consent refers to the practice of an organisation 'bundling' together multiple requests for an individual's consent to a wide range of collections, uses and disclosures of personal information, without giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not.

An example of a bundled consent is seeking consent to 'all legitimate uses or disclosures'. If a bundled consent is contemplated, an organisation should ensure that it sufficiently informs the individual about each of the proposed collections, uses and/or disclosures that it intends with the personal information that is collected.

Digital platforms routinely collect information of individuals that is not necessary to provide the service requested. They do this by obtaining their bundled consent for a large variety of user data collection and use for a range of different purposes. Although the practice is gaining popularity, this practice also has the potential to undermine the voluntary and specific nature of any consent.

By bundling consents in these different ways, digital platforms are not giving the individual the opportunity to choose which collections, uses and disclosures they agree to and which they do not.

Hence the reliance on general, blanket or bundled consent terms can be problematic and open to challenge and not encouraged as best practice. An organisation should not seek a broader consent than is necessary for its specific purposes and needs, for example, consent for undefined future uses.

The NSW Civil and Administrative Tribunal has expressed the view that a 'bundled' approach to gaining permission for the sharing of personal information, such as a patient registration form covering all circumstances for the patient's life, will not provide the specificity required for a valid consent[3].

When is consent current?

An organisation should generally seek consent from an individual for collection and proposed uses and disclosures of personal information at the time the information is collected. If consent was not sought at the time of collection, or that consent did not cover a proposed use or disclosure, an entity should seek the individual's consent before the proposed use or disclosure that is now intended and that was not captured by the consent that was given.

Consent given in particular circumstances cannot be assumed to endure indefinitely. Good practice is to inform the person of a specific period for relying on their consent, in the absence of any material change.

You should also make it clear that a person is entitled to change their mind and revoke their consent later on.

Once an individual has withdrawn consent, you can no longer rely on their past consent for any future use or disclosure of the individual's personal information. The individual should be made aware of the potential implications of withdrawing consent, such as no longer being able to access a service.

What happens when a person withdraws consent?

A regulated entity should tell the individual that their agreement can be withdrawn, and the practical effect of that withdrawal. Where an individual has agreed to the regulated entity disclosing their personal information to a third party, withdrawal after the disclosure has taken place will not have any effect on the action already taken but will have effect on any future action.

Withdrawal of agreement does not require the regulated entity to retrieve the information, as its disclosure was lawful at the time it occurred.

However, where goods and services are dependent on the individual agreeing to the future and ongoing disclosure and/or use of their personal information, the regulated entity may no longer be able to provide such goods and services to the individual because the consent has been withdrawn. These implications should be communicated to the individual clearly prior to finalising the withdrawal of consent and the options available should be discussed with the individual.

When is consent given by a person with capacity?

Consent is only genuine if the person giving consent has capacity to give or withhold consent. A person has capacity if they are able to understand the general nature and effect of a particular proposed use or disclosure of their personal information, and can communicate their consent.

A person's capacity to make a particular decision should only be doubted if there is a factual basis to doubt it.

---

[2] *Vice-Chancellor, Macquarie University v FM* (GD) [2003] NSWADTAP 43 at [97]

[3] *KJ v Wentworth Area Health Service [2004] NSWADT 84* at [55], [61]

Issues that could affect an individual's capacity to consent include:

- age
- physical or mental disability
- temporary incapacity, for example during a psychotic episode, a temporary psychiatric illness, or because the individual is unconscious, in severe distress or suffering dementia
- limited understanding of English.

An organisation should consider whether any such issue could be addressed by providing the individual with appropriate support to enable them to have capacity to consent. For example, it may be appropriate for a parent or guardian to consent on behalf of a young person.

The Best Practice Guide: Privacy and people with decision-making disabilities should be referred to for specific and detailed guidance on how to deal with a person with limited or no capacity to give or withhold their consent to a use or disclosure of their personal information'.

Written or verbal consent

Consent (and refusal of consent) "may be given in writing, orally or in any other form where the consent is clearly communicated[4]. However, documented consent is of greater value in the event of a later dispute about whether an individual actually gave consent for a particular use or disclosure[5].

Express or implied consent

Express consent means "consent that is clearly and unmistakably communicated". The organisation "must have gone to the individual concerned and obtained an express consent that is precise as to the kind and, possibly, the exact contents of the information to which the consent relates"[6]. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.

Implied consent is "consent that can reasonably be inferred from an individual's actions"[7]. An example is when a person lodges an official complaint with an organisation, their consent can be inferred to have their personal information used and disclosed, as reasonably necessary in order to investigate their complaint[8].

An organisation should not assume that an individual has consented to a collection, use or disclosure that appears to be advantageous to that person. Nor can an entity establish implied consent by asserting that if the individual knew about the benefits of the collection, use or disclosure, they would probably consent to it.

Some privacy principles require 'express consent.' Others simply require 'consent,' which could therefore be either express or implied[9]. The following table shows which NSW privacy principles require express consent:

Type of personal information	Use (IPP/HPP10)	Disclosure (IPP/HPP11)	Transborder disclosure (IPP12, HPP14)
Health information	Consent	Consent	Consent
Sensitive information	Consent	Express consent	Express consent
All other Types	Consent	Express consent	Express consent

Even for those actions which would allow for implied consent, it is generally preferable to seek a person's express consent. This is because it may be difficult to demonstrate that an individual has genuinely consented if consent is merely inferred by an organisation.

Even if a person has not stated their objection to the proposed use or disclosure, their consent cannot necessarily be inferred, because they may not have heard, may not have understood or may have had insufficient information to make an informed decision[10]. Consent may not be inferred if an individual's intent is ambiguous or there is reasonable doubt about the individual's intention. An organisation also cannot infer consent simply because it provided an individual with notice of a proposed collection, use or disclosure of personal information.

Consent should not be inferred just because:

- the person's capacity to provide or refuse consent is impaired
- the proposed conduct is disclosure of personal information to a spouse or family member
- the benefits of consenting, as the agency sees them, suggest that the person would 'probably' consent if asked
- most other people have consented to the same use or disclosure of the information
- the person has consented in the past
- the person has given general consent only – for example the agency has requested broad

[4] Privacy NSW, *Best Practice Guide: Privacy and people with decision-making disabilities,* 2004, p.10.
[5] Privacy NSW, Best *Practice Guide: Privacy and people with decision-making disabilities,* 2004, p.10.
[6] *Vice-Chancellor, Macquarie University v FM* (GD) [2003] NSWADTAP 43 at [97].
[7] Privacy NSW, *Best Practice Guide: Privacy and people with decision-making disabilities,* 2004, p.10; see also Privacy *NSW,Handbook to Health Privacy,* 2004, part 1.3.
[8] See for example *VZ v University of Newcastle* [2009] NSWADT 18 at [19], LN v *Sydney South West Area Health Service (No (2) [201OJ NSWADT at [74], AQB v St Vincent's Hospital Sydney Limited [2013] NSWADT 210, and BFP v NSW Ambulance Service [2015] NSWCATAD 39*
[9] *LN v Sydney South West Area Health Service* [2011] NSWADTAP 3
[10] Privacy NSW, Best Practice Guide: Privacy and people with decision-making disabilities, 2004, p.10; see also Privacy NSW, Handbook to Health Privacy, 2004, part 1.3.

authorisation for a range of conduct in a 'bundled consent' (as sometimes happens when a person first comes into contact with an agency)

- the person does not have sufficient English language proficiency to communicate their wishes without an interpreter.

Opt-out mechanisms

Use of an opt-out mechanism to infer an individual's consent will only be appropriate in limited circumstances, as the individual's intention in failing to opt-out may be ambiguous. An organisation will be in a better position to establish the individual's implied consent the more that the following factors, where relevant, are met[11]:

- the opt out option was clearly and prominently presented
- it is likely that the individual received and read the information about the proposed collection, use or disclosure, and the option to opt out
- the individual was given information on the implications of not opting out
- the opt out option was freely available and not bundled with other purposes
- it was easy for the individual to exercise the option to opt out, for example, there was little or no financial cost or effort required by the individual
- the consequences of failing to opt out are not serious
- an individual who opts out at a later time will, as far as practicable, be placed in the position as if they had opted out earlier.

An organisation should as far as practicable implement procedures and systems to obtain and record consent. This may resolve any doubt about whether consent was given (either on the basis of express or implied consent).

Conclusion

The five elements required for a valid consent set a high standard for organisations seeking to rely on 'consent' to authorise their activities. The Tribunal has noted that these elements should be strictly applied, in order to protect one's freedom from interference with privacy[12].

This high standard is deliberate. This is because routine uses and disclosures which are for directly related secondary purposes do not require consent in the first place. Consent as a legal mechanism is best applied to special cases: non-routine uses and disclosures, for purposes that are not directly related to the primary purpose of collection and in circumstances where no other exemption applies.

Not all activities will be capable of meeting these five elements. For example, 'Big Data' analytics, which often seeks to re-use data for purposes quite unrelated to the original purpose of collection, and potentially even unanticipated at the time of collection, cannot rely on vague terms in a privacy notice given some time ago. To rely on 'consent' to authorise new forms of data analytics would generally require a fresh process of communication with the subject individuals. Where such a process is not practical, other ways of authorising the secondary use or disclosure may be preferable, such as a research exemption.

For more information

Contact the Information and Privacy Commission NSW (IPC):

Freecall: 1800 472 679
Email: ipcinfo@ipc.nsw.gov.au
Website: www.ipc.nsw.gov.au

NOTE: The information in this fact sheet is to be used as a guide only. Legal advice should be sought in relation to individual circumstances

[11] Federal Privacy Commissioner Guidance 2015, B.40. https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts

[12] *Vice-Chancellor, Macquarie University v FM* (GD) [2003] NSWADTAP43