



Checksheet: Consent

Am I intending to use or disclose personal or health information?

No



No consent required.

Yes



Uses or disclosures of personal information may require the consent of the individual.



Question	Things to consider in making decision
What is the difference between notice and consent?	<p>Consent</p> <ul style="list-style-type: none"> Seeking a person's permission to use or disclose their information by giving them the choice of agreeing or disagreeing to what is proposed. <p>Notice</p> <ul style="list-style-type: none"> Advising a person of what you intend to do with their information by way of privacy notice under IPP 3 and HPP 4. Routine primary and secondary uses or disclosure that does not require consent should still be notified to the individual.
When is consent required for disclosure or use of a person's information?	<p>The consent is required when:</p> <ul style="list-style-type: none"> The use or disclosure is not directly related to the primary purpose of collection, in circumstances where no other exemption applies. <p>The consent is not required when:</p> <ul style="list-style-type: none"> The use or disclosure is for the primary purpose for which the personal information was collected in the first place. The use or disclosure is for a directly related secondary purpose (which is within the person's reasonable expectations, or to which you have no reason to believe they would object). The use or disclosure is authorised or required under another law.
When is consent valid?	<p>For consent to be valid it must be voluntary, informed, specific, current and given by a person who has capacity to give it.</p> <p>Is the consent voluntary?</p> <ul style="list-style-type: none"> Was a person free to exercise genuine choice about whether to give or withhold consent? Was consent given without coercion or threat? Was sufficient time allowed to understand the request and, if appropriate, take advice? <p>Is the consent informed?</p> <ul style="list-style-type: none"> Does the person have reasonable knowledge of all the relevant facts before they give or refuse consent? The relevant facts will include: <ul style="list-style-type: none"> the purpose of collecting the information who will have access to information the intended use for the information the recipients of the information whether disclosure of information is voluntary or required by law the consequences of giving or refusing consent <p>Is the consent specific?</p> <ul style="list-style-type: none"> Is the consent reasonably specific as opposed to general, blanket or bundled? <p>Is the consent current?</p> <ul style="list-style-type: none"> Was the person advised of a specified period for reliance on their consent? Was the person advised that they are entitled to revoke consent later on? <p>Is the consent given by a person with capacity?</p> <ul style="list-style-type: none"> Is the person giving consent able to understand the general nature and effect of a particular proposed use or disclosure of their personal information and able to communicate their consent? Does the person have a disability? <ul style="list-style-type: none"> Refer to our <i>Best Practice Guide: Privacy and people with decision-making disabilities</i>
Should consent be written or verbal?	<ul style="list-style-type: none"> Consent and refusal of consent can be indicated in writing, verbally, or through behaviour. Wherever practicable, consent should be sought in writing.
Is consent express or implied?	<p>Is there <u>express consent</u>?</p> <ul style="list-style-type: none"> Has the consent been clearly and unmistakably communicated by the person? <u>Express consent</u> is required in the following circumstances: <ul style="list-style-type: none"> Disclosure of personal information (excluding health information) Transborder disclosure of personal information (excluding health information) <p>Is there <u>implied consent</u>?</p> <ul style="list-style-type: none"> Can the consent be reasonably inferred from a person's actions? (examples of when consent can be inferred have been provided in the main body of this Fact Sheet). Consent cannot be inferred through exercise of 'opt out' mechanisms.

Guidance: Consent

Privacy and Personal Information Protection Act 1998 Health Records and Information Privacy Act 2002

Privacy laws in NSW sometimes require that an individual's consent is needed for an activity to occur. This Fact Sheet offers interpretation and guidance on the meaning of 'consent'.

This Fact Sheet makes reference 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)*. Please note any reference to personal information in this fact sheet should be read to include health information.

Key points

- 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.

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

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.

By contrast, a consent form 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.'

For example, 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 the law prohibits.

On the other hand, there are routine primary and secondary uses or disclosures, over which you offer the individual no or little choice. They 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, B and C of the PPIP Act).

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

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).

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; and
- the individual has the capacity to understand and communicate their consent.

1. 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 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 not permit the particular disclosure.

2. 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.

3. Specific

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."

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

Reliance on general, blanket or bundled consent terms can be problematic and open to challenge. An organisation should not seek a broader consent than is necessary for its purposes, for example, consent for undefined future uses.

The 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. 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 sufficiently inform the individual about each of the proposed collections, uses and/or disclosures.

4. 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 at the time of the use or disclosure.

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.

5. 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.

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; and
- 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”.¹ 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.²

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.”³ 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”.⁴ 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.⁵ 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.

¹ Privacy NSW, *Best Practice Guide: Privacy and people with decision-making disabilities*, 2004, p.10.

² Privacy NSW, *Best Practice Guide: Privacy and people with decision-making disabilities*, 2004, p.10.

³ *Vice-Chancellor, Macquarie University v FM (GD)* [2003] NSWADTAP 43 at [97].

⁴ 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.

⁵ See for example *VZ v University of Newcastle* [2009] NSWADT 18 at [19], *LN v Sydney South West Area Health Service (No 2)* [2010] NSWADT at [74], *AQB v St Vincent's Hospital Sydney Limited* [2013] NSWADT 210, and *BFP v NSW Ambulance Service* [2015] NSWCATAD 39

Some privacy principles require 'express consent.' Others simply require 'consent,' which could therefore be either express or implied.⁶ The following table illustrates which of the NSW privacy principles require *express* consent:

Type of personal information	Use (IPP 10, HPP 10)	Disclosure (IPP 11, HPP 11)	Transborder disclosure (IPP 12, HPP 14)
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, 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.⁷ 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.

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 met⁸:

- 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; and
- 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.

⁶ *LN v Sydney South West Area Health Service* [2011] NSWADTAP 3

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 Federal Privacy Commissioner Guidance 2015, B.40.

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.⁹

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.

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.

⁹ *Vice-Chancellor, Macquarie University v FM (GD)* [2003] NSWADTAP 43