Fact Sheet

September 2026

# Consent

**Who is this information for?**

NSW public sector agencies and Health Care providers

**Why is this information important?**

This guidance is provided to assist NSW public sector agencies and Health Care providers understanding the issue of consent under the *Privacy and Personal Information Protection Act (PPIP) 1998* (NSW), and *Health Records and Information Privacy Act (HRIP) 2002 (NSW).*

NOTE: Any reference to personal information in this fact sheet should be read to include health information.

Privacy laws in NSW provide that, in certain circumstances, before an agency can use or disclose an individual's personal information, their consent must be obtained. 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 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 not to 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 any proposed use or disclosure of their personal information.

It notifies individuals of the terms under which a regulated entity will provide a service or otherwise engage with members of the public.

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

## When is a privacy notice required?

There are routine primary and secondary uses or disclosures over which the individual is offered 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 specific public interest exemption (for example sections 27A, 27B and 27C of the PPIP Act).

In such cases, you should notify the individual by way of a privacy notice which complies with the requirements of section 10 of the PPIP Act[2] and HPP 4[3].

## What should a privacy notice contain?

A good privacy notice should:

- be written in clear language that the individual will understand
- be truthful and in no way misleading
- contain the following sections:
    - the categories of data collected
    - why the data is collected (purpose)

[1] *KJ v Wentworth Area Health Service [2004] NSWADT 84* at [55], [61]
[2] s 10 *Privacy and Personal Information Protection Act 1998* (NSW).
[3] sch 1, s 4 *Health Records and Information Privacy Act 2002* (NSW)

- how the data is to be used
- 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)

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

## What is consent?

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

## When is consent required?

Consent is relevant to the operation of several IPPs and HPPs. For some principles, the giving of consent operates as an exception to a general prohibition against personal information being handled in a particular way (for example, IPPs 10,[4] 11[5] and 12[6] and HPPs 10 and 11).[7]

The giving of a privacy notice will often be insufficient to establish that consent has been given to a particular use or disclosure.

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 it is given:

- without coercion or threat,
- with sufficient time to understand the request and,
- if appropriate, with sufficient time to 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, at some later time, to 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.

Consent will not be voluntary if it is made a pre-condition for receiving a government service. The only exception is where the law governing the transaction requires consent as a precondition for delivery of the service.

For example, an organisation may provide health, welfare or housing services to the public. If a person exercises their right to request services from the organisation, it will not be appropriate for the organisation to impose a condition that the provision of services will occur on the receipt of a person's consent to disclose their personal information if the laws that apply to the organisation prohibit or do not expressly 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 invalidate a person's consent.

So that an individual can decide whether or not to give consent, an organisation should ensure that the individual is properly and clearly informed about how their personal information will be handled.

[4] s 10 *Privacy and Personal Information Protection Act 1998* (NSW).
[5] s 18 *Privacy and Personal Information Protection Act 1998* (NSW).
[6] s 19 *Privacy and Personal Information Protection Act 1998* (NSW).
[7] See s 26 *Privacy and Personal Information Protection Act 1998* (NSW).

## How specific should consent be?

Consent should be as specific as possible and to an identified purpose. An organisation should not seek a broader consent that is necessary for its purpose.

The level of specificity required will depend on the circumstances, including the sensitivity of the personal or health information involved.

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."[8]

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 '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 an individual is informed about each of the proposed uses and/or disclosures of the information collected.

Digital platforms routinely collect personal information that may not be needed to provide the services requested. They do this by obtaining bundled consents for the collection and use of a large volume of user data and for a range of different purposes. Although the practice is widespread, it is questionable whether such consents would be considered voluntary or sufficiently specific to be considered valid.

By bundling consents in this way, digital platforms are not giving individuals the opportunity to choose which collections, uses and disclosures they agree to and which they do not.

Nominal consents obtained via the use of general, blanket or bundled consent terms can be problematic, are open to challenge and are not encouraged as best practice. An organisation should not seek a consent that is broader than is necessary for its specific purposes and needs, such as a consent for undefined future uses.

The NSW Civil and Administrative Tribunal has expressed the view that a 'bundled' approach to gaining consent for the sharing of personal information, such as a patient registration form covering all circumstances for the patient's life, will be insufficiently specific for the purposes of the IPPs and HPPs.[9]

## When is consent current?

Consent to collection, proposed uses and disclosures of personal information should be sought from an individual 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.

Consent cannot be assumed to endure indefinitely. Whether consent that has been given in the past is still current depends on the circumstances in which the consent was given, and the amount of time that has passed. Good practice is to inform the person of a specific period that the organisation intends to rely on their consent.

It should also be made 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 collection, 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 consent 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 any action already taken but will have effect on any future action by the entity.

A withdrawal of consent does not require the regulated entity to retrieve any information that has been disclosed so long as its disclosure was lawful at the time it occurred.

However, where the provision of goods and services is 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.

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

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

Prior to finalising the withdrawal of consent, any such repercussions should be clearly communicated to the individual and a discussion, outlining the options available to them, should take place.

## What is the "capacity" to give consent?

A person's consent is only genuine if they have the capacity to give or withhold consent. A person has capacity if they can 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
- limited understanding of English.

An organisation should consider whether, in a particular circumstance, these issues can be addressed by providing an individual with appropriate support. For example, it may be appropriate for a parent or guardian to consent on behalf of a young person.

For 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 see Privacy and persons with reduced decision-making capacity: A guide for public sector agencies.

## 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. However, documented consent is of greater value in the event of a later dispute about whether an individual genuinely consented to a particular use or disclosure.

## 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.'[10] Consents can be recorded in a variety of ways including in the form of a hardcopy or digitally signed document, a file note of an oral statement or a voice signature.

Implied consent is consent that can reasonably be inferred from an individual's actions. Where, for example, a person lodges an official complaint with an organisation, it can be inferred that they have consented to the use and disclosure of their personal information as is reasonably necessary to investigate the complaint.[11]

Some privacy principles require 'express consent.' Others simply require 'consent,' which could therefore be either express or implied.[12] The following table shows which NSW privacy principles require express consent:

| Type of personal information | Use (IPP10[13]/ HPP10) | Disclosure (IPP11[14]/ HPP11) | Transborder disclosure (IPP12[15]/ HPP14) |
|---|---|---|---|
| **Health information** | Consent | Consent | Consent |
| **Restricted information** | Consent | Express consent | Express consent |
| **All other Types** | Consent | Express consent | Express consent |

Because of the difficulty in establishing a person's genuine implied consent, it is generally preferable to seek a person's express consent, even if not strictly required.

Silence or any other failure to state an objection to a proposed use or disclosure should not be relied on to infer consent. This is because a person may not have heard, may not have understood or may have had insufficient information to make an informed decision.

[10] *Vice-Chancellor, Macquarie University v FM* (GD) [2003] NSWADTAP 43 at [97].
[11] 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 38 at [74], *AQB v St Vincent's Hospital Sydney Limited* [2013] NSWADT 210, and *BFP v NSW Ambulance Service* [2015] NSWCATAD 39
[12] *LN v Sydney South West Area Health Service* [2011] NSWADTAP 3
[13] s 17 *Privacy and Personal Information Protection Act 1998* (NSW).
[14] s 18 *Privacy and Personal Information Protection Act 1998* (NSW).
[15] s 19(2) *Privacy and Personal Information Protection Act 1998* (NSW).

Consent may not be inferred if an individual's intent is ambiguous or there is reasonable doubt about the individual's intention.

The following factors cannot be relied on to infer that consent has been given:

- that the person's capacity to provide or refuse consent is impaired
- that the proposed conduct is disclosure of personal information to a spouse or family member
- that the benefits of consenting, as the agency sees them, suggest that the person would 'probably' consent if asked
- that the person has been provided with a Privacy Notice, a collection notice or terms and conditions policy
- that most other people have consented to the same use or disclosure of the information
- that the person has consented in the past
- the person has given general consent only – for example the agency has requested broad authorisation for a range of conduct in a 'bundled consent' (as sometimes happens when a person first comes into contact with an agency)
- that 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 the best position to establish an individual's implied consent where it can establish, where relevant, that:[16]

- 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 same position as if they had opted out at an earlier time.

An organisation should, as far as practicable, implement procedures and systems to obtain and record consents.

## Conclusion

Routine uses and disclosures for primary and directly related secondary purposes do not require consent. However, where it is required, the five elements of a valid consent set a high bar. As the Appeal Panel has remarked:

> *'[the] legislation protects an aspect of an important human right, that of freedom from interference with privacy. The express consent provision should be strictly applied so as to underpin that right.'*[17]

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

### 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.*

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

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