



## IPC Privacy Statement of Jurisdiction

<b>Who is this information for?</b>	NSW citizens seeking information on the jurisdiction of the IPC and Privacy Commissioner
<b>Why is this information important to them?</b>	This fact sheet will help citizens understand how their privacy is protected, what to do if they think their privacy has been breached and the jurisdiction of the NSW Privacy Commissioner and the IPC.

### What is the NSW Privacy Commissioner's jurisdiction?

The NSW Privacy Commissioner oversees two main privacy laws. They are:

- the *Privacy and Personal Information Protection Act 1998* (PPIP Act), and
- the *Health Records Information Privacy Act 2002* (HRIP Act)

The PPIP Act protects your personal information, whereas the HRIP Act protects your health information.

Both Acts aim to protect your privacy by imposing obligations on the people who handle your information and by enabling you to complain if you think your privacy has been breached.

Other federal and NSW laws may also be relevant to privacy issues, including but not limited to:

- [Workplace Surveillance Act 2005 \(NSW\)](#)
- [Surveillance Devices Act 2007 \(NSW\)](#)
- [Adoption Act 2000 \(NSW\)](#)
- [Assisted Reproductive Technology Act 2007 \(NSW\)](#)
- [Crimes \(Forensic Procedures\) Act 2000 \(NSW\)](#)
- [Criminal Records Act 1991 \(NSW\)](#)
- [Privacy Act 1988 \(Cth\)](#)
- [Telecommunications \(Interception and Access\) Act 1979 \(Cth\)](#)

However, the Privacy Commissioner does not have jurisdiction in relation to these laws and can only deal with privacy issues that arise under the PPIP and HRIP Acts.

### What is the difference between my personal information and my health information?

Personal information is any information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.

Personal information includes:

- information or an opinion which is part of a database,
- information or an opinion which may not be recorded in a material form,
- a written record which may include your name, address and other personal details about you,
- photographs, images, video or audio footage of individuals, and
- a person's fingerprints, blood or DNA samples.

Health information is a type of 'personal information' that is information or an opinion about:

- an individual's physical or mental health or disability,
- an individual's express wishes about the future provision of health services, or
- a health service provided or to be provided to a person.

Health information also means other personal information:

- collected to provide or in providing a health service,
- collected in connection with the donation, or intended donation, of body parts, organs or body substances,
- that is genetic information about an individual arising from a health service provided in a form that is or could be predictive of the health of the individual or of a genetic relative of the individual, or
- healthcare identifiers (i.e. usually a number assigned to individuals and healthcare providers).

## Who is bound by the NSW PPIP Act and HRIP Acts?

NSW public sector agencies are bound by both the PPIP Act and HRIP Act. This includes:

- state government agencies,
- local councils,
- universities, and
- Ministers and Minister's offices.

From 28 November 2023, some state owned corporations (SOC's) will also be required to comply with the PPIP Act. More information is available via the [IPC's fact sheet about SOC's](#).

Private sector persons (individuals, corporations, partnerships and trusts) are not bound by the PPIP Act, however they will be bound by the HRIP Act if they provide a health service or collect, hold or use health information.

## Are there limits to the NSW Privacy Commissioner's Jurisdiction?

The Privacy Commissioner does not have privacy jurisdiction over the conduct of private sector persons (individuals, corporations, partnerships and trusts) except where they are bound by the HRIP Act.

## How does this work in conjunction with federal legislation?

Organisations not covered by the PPIP and/or HRIP Acts (e.g. state owned corporations not otherwise captured under the PPIP Act, federal government departments, and some private sector organisations) may be covered by the Federal *Privacy Act 1988* (Privacy Act) which is dealt with by the Office of the Australian Information Commissioner (OAIC).

The Privacy Act also applies to all health service providers in the private sector throughout Australia. That is, a person or entity providing a health service and holding health or personal information. It does not apply to public sector health service providers such as public hospitals which are instead covered by the HRIP Act.

The OAIC is also the independent privacy regulator for the My Health Record system and Healthcare Identifier service and has functions and responsibilities under both the *My Health Records Act 2012* and the *Healthcare Identifiers Act 2010*. More information regarding this is available through the [OAIC's website](#).

## How is my privacy protected in NSW?

The PPIP Act and HRIP Act provide for the proper collection, holding, security, access to, amendment, disposal, use and disclosure of your personal and health information.

The PPIP Act provides this through 12 Information Protection Principles (IPPs). The IPPs are legal obligations that NSW public sector agencies must comply with when dealing with your personal information.

More information is available about the [IPPs and their exceptions and exemptions](#).

The HRIP Act similarly sets out 15 Health Privacy Principles (HPPs). These HPPs are legal obligations that NSW public sector agencies and private sector persons must comply with when dealing with your health information.

Part 4 of the HRIP Act imposes additional obligations on private sector persons, covering retention, access and amendment of health information.

More information is available [about the HPPs](#).

The Privacy Commissioner has a role in ensuring that those bound by the legislation meet the IPPs and HPPs when dealing with your personal and health information.

From 28 November 2023, public sector agencies are also required to comply with the Mandatory Notification of Data Breach (MNDB) Scheme.

The MNDB Scheme requires public sector agencies to notify the Privacy Commissioner and affected individuals of data breaches involving personal or health information that are likely to result in serious harm.

As part of the Scheme, agencies are required to publish a data breach policy, which outlines an agency's overall strategy for managing data breaches. Agencies must also maintain an internal register of eligible data breaches.

## What if I think my privacy has been breached?

If you have concerns that your privacy has been breached by a public sector agency, the following options may be available to you:

- ask the agency to conduct an internal review of the conduct that is alleged to have breached your privacy. This is a fact finding investigation undertaken by the agency into your privacy complaint, or
- make a complaint to the NSW Privacy Commissioner about the conduct.

If you think that your privacy has been breached by a federal government department or private sector organisation that is governed by the Privacy Act, further information is available through the [OAIC's website](#).

You have 6 months from when you first become aware of the conduct to ask for an internal review or make a complaint to the Privacy Commissioner.

If you are seeking an internal review by the agency, you must be aggrieved by the conduct or complaining on behalf of someone else who is aggrieved.

If you are a member of a class of people whose privacy may have been breached, you can only make a complaint about the conduct in so far as you are personally aggrieved. Other members of that class are also able to make complaints about the conduct as it relates to them.

If you make a complaint to the Privacy Commissioner that could also be dealt with as an internal review by the agency, the Privacy Commissioner may decide not to deal with your complaint because it would be more appropriate to make an application for internal review. Internal review provides you with rights of review which can then be exercised in the NSW Civil and Administrative Tribunal (NCAT).

The Privacy Commissioner has an oversight role in the internal review process, and can make submissions to the agency about its draft findings. Therefore when you choose to have your concerns dealt with as an internal review by the agency, the Privacy Commissioner still has a role in that process.

If you request an internal review by an agency, then at the completion of that review you will be informed of:

- the findings of the review,
- the action (if any) proposed by the agency in response to your complaint, and
- your further review rights.

More information is available about the [internal review process](#).

The Privacy Commissioner is notified of all NCAT administrative reviews under the PPIP Act and has a right to appear and be heard in any such proceedings before the Tribunal.

Generally, the Privacy Commissioner will appear or file submissions in proceedings that involve novel or complex questions of law where the Tribunal would benefit from submissions by the Commissioner.

The Privacy Commissioner is independent and does not represent or advocate for either applicants or agencies in privacy internal reviews or NCAT administrative reviews.

More information is available about [NCAT's review process](#).

## Complaints about a private sector person under the HRIP Act

If you are concerned that a private sector person has not met their privacy obligations under the HRIP Act, your first action should always be to contact the person or organisation directly and communicate your concerns.

If you are not able to resolve your complaint directly with the private sector person you can make a complaint to the NSW Privacy Commissioner.

A complaint must be made within 6 months (or such later time as the Privacy Commissioner may allow) from the

time you first became aware of the conduct or matter the subject of the complaint.

If there is overlapping jurisdiction, you should carefully consider whether you wish to have your complaint dealt with under the HRIP Act or the Privacy Act. The complaint processes, possible outcomes and rights of review are different under each of these Acts and once you have your complaint dealt with under one Act, you may not be able to later choose to have it dealt with under the other. Information about your rights under the Privacy Act is available from the [OAIC's website](#).

If you choose to make your complaint to the NSW Privacy Commissioner you can do so by writing to the IPC or filling in the online webform here. You should also provide a copy of all your correspondence with the private sector person.

The NSW Privacy Commissioner will then:

- assess your complaint,
- determine whether the private sector person appears to have breached a HPP, provision of Part 4 of the HRIP Act, or a health privacy code of practice, and
- how to deal with your complaint.

The Privacy Commissioner will generally endeavor to resolve your complaint through a conciliation processes.

If the NSW Privacy Commissioner is not able to resolve the complaint via conciliation, the NSW Privacy Commissioner can investigate and provide a report. This report will enable you to apply to NCAT for a review of the conduct though the application must be made within 28 calendar days after you receive the report.

If the NSW Privacy Commissioner deals with your complaint in any other way (including by determining that the matter has been resolved) and you do not receive a report from the NSW Privacy Commissioner in response to your complaint, NCAT will have no power to consider your matter.

## What can the NSW Privacy Commissioner do?

The functions of the Privacy Commissioner are set out in both the HRIP and PPIP Acts.

In an internal review conducted by an agency, the Privacy Commissioner exercises an oversight role. This means that the Privacy Commissioner is notified of applications for internal reviews made to agencies, kept informed of the progress of those reviews and informed of their findings and any action proposed to be taken by the agency in relation to the matter.

The Privacy Commissioner can also make submissions about the subject matter of any internal review, including, but not limited to whether:

- the agency's conduct did or did not constitute a breach of the IPPs/HPPs,

- an apology should be made to the applicant,
- changes should be considered to the agency's practices or procedures, or
- further or refresher training about the agency's privacy obligations should be given to its staff.

Any submissions made by the Privacy Commissioner are required to be considered by agencies when conducting the internal review.

However, the Privacy Commissioner does not have jurisdiction to award or direct that compensation be paid in relation to either an internal review or a complaint.

The Privacy Commissioner may also, without having received a complaint, conduct inquiries and make such investigations into privacy related matters as the Privacy Commissioner thinks appropriate.

The Privacy Commissioner also plays a role in the operation of the Mandatory Notification of Data Breach Scheme.

Under the MNDB scheme, the Privacy Commissioner is empowered to work with agencies to facilitate legal compliance, develop and promote privacy best practice and investigate instances of agency non-compliance.

The Privacy Commissioner's role under the scheme also involves:

- monitoring, auditing and reporting on the functions of individual agencies and on the operation of the scheme as a whole; and
- receiving notifications from agencies of eligible data breaches.

The Privacy Commissioner also has the power to access an agency's premises to observe its systems, policies and procedures.

## What other privacy legislation can apply?

If you are concerned about the conduct of a private sector person breaching your privacy, it is likely that your concerns also allege a possible breach of one or more of the [Australian Privacy Principles \(APPs\)](#) under the Privacy Act.

The underlying principles and privacy protections of the HRIP Act and Privacy Act are similar.

You may therefore be able to have your complaint dealt with by the OAIC instead if the private sector person is covered by the Privacy Act. For more information, contact the OAIC on 1300 363 992 or via its website – <http://www.oaic.gov.au/>

If you are complaining about a business that offers goods or services to European Union citizens, then they may also be subject to the General Data Protection Regulation (GDPR). This is a European privacy law.

You can find more information about the effect of the GDPR on Australian businesses on the [OAIC website](#).

## For more information

Contact the Information and Privacy Commission NSW (IPC):

**Freecall:** 1800 472 679

**Email:** [ipcinfo@ipc.nsw.gov.au](mailto:ipcinfo@ipc.nsw.gov.au)

**Website:** [www.ipc.nsw.gov.au](http://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.*