

COMPARATIVE TABLE OF ORGANISATIONS' RESPONSIBILITIES UNDER AUSTRALIAN PRIVACY LEGISLATION

This Info Sheet has been developed to help organisations sort out the four sets of privacy principles under Victoria's Information Privacy Act 2000 (IPA) and Health Records Act 2001(HRA) and the Commonwealth Privacy Act 1988 (PA). It is a more detailed companion to Info Sheet 04.02 which discusses generally the coverage of the three Acts.

This Info Sheet is a series of tables which briefly summarise the:

1. Information Privacy Principles (IPPs) contained in the IPA;
2. Health Information Privacy Principles (HPPs) contained in the HRA;
3. National Privacy Principles (NPPs) contained in the Privacy Act 1988 (as amended); and
4. Information Privacy Principles for the Commonwealth public sector (FIPPs) in the PA.

Tables have also been included which compare the:

5. key similarities of the HPPs, NPPs, and FIPPs, against the IPPs; and
6. key differences of the HPPs, NPPs and FIPPs against the IPPs.

This Info Sheet is not a general comparison of the coverage of the three Acts. Rather, its focus is their privacy principles.

Contents of this Info Sheet should not be used as a substitute for the full privacy principles or be interpreted as legal advice. Organisations should seek independent legal advice in determining whether their policies and practices comply with relevant legislation.

INFORMATION PRIVACY ACT 2000 (IPA)

INFORMATION PRIVACY PRINCIPLES (IPPs) IN SUMMARY

Also refer to Guidelines May 2002 and August 2002; IPPs in everyday language; and Info Sheet 03.02 which covers Frequently Asked Questions

NO.	SUBJECT	BRIEF SUMMARY
IPP1	Collection	<p>Collect the personal information by lawful, fair and reasonable means necessary for an organisation's functions or activities and preferably collect it from the individual concerned.</p> <p>Before, at or near the time of collection notify the individual of:</p> <ul style="list-style-type: none">• the organisation's contact details;• the purpose of collection;• an individual's right to access personal information;• usual disclosures;• where the collection is required by law; and• the main consequences of not providing personal information. <p>Where collect personal information from third parties tell the individual whose personal information is collected of the six points listed above.</p>
IPP2	Use & Disclosure	<p>Use or disclose personal information:</p> <ul style="list-style-type: none">• for the primary purpose collected;• for a related secondary purpose an individual would reasonably expect;• where individual consents;• for law enforcement; or• for other prescribed exceptions. <p>Where disclosure is for law enforcement make a written note of the disclosure.</p>
IPP3	Data Quality	<p>Take reasonable steps to ensure personal information is accurate, complete, up to date and relevant.</p>
IPP4	Data Security	<p>Take reasonable steps to protect personal information held from misuse, loss, unauthorised access, modification or disclosure.</p> <p>Destroy or permanently de-identify information no longer required. Provisions dealing with retention in other Acts, such as the Public Records Act, apply to the public sector.</p>
IPP5	Openness	<p>Document clearly expressed policies on the management of personal information and steps individuals have to take to access personal information. Make policies available to anyone who asks. On request, take reasonable steps to let the enquirer know, generally, what sort of personal information is held, for what purposes, and how the organisation collects and manages that information.</p>
IPP6	Access & Correction	<p>Administrative or formal procedures for access to personal information under the Freedom of Information Act will apply in the public sector. Provide the individual with access to personal information on request by the individual, except to the extent that prescribed exceptions apply. If an individual establishes that the information is not accurate, complete and up to date, take reasonable steps to correct the information.</p>
IPP7	Unique Identifiers	<p>May only assign unique identifiers to individuals if it is necessary to carry out functions efficiently. Must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless prescribed exceptions apply.</p>
IPP8	Anonymity	<p>Wherever it is lawful and practicable individuals must have the option of not identifying themselves when entering transactions with an organisation.</p>
IPP9	Transborder Data Flows	<p>May transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if prescribed conditions apply.</p>
IPP10	Sensitive Information	<p>Must not collect sensitive information about an individual, such as ethnicity or criminal record, unless prescribed exceptions apply.</p>

HEALTH RECORDS ACT 2001 (HRA)

HEALTH INFORMATION PRIVACY PRINCIPLES (HPPs) IN SUMMARY

Refer statutory guidelines issued by HSC for HPP 10

NO.	SUBJECT	BRIEF SUMMARY
HPP1	Collection	<p>Collect health information about an individual by lawful, fair and reasonable means necessary for an organisation's functions or activities and preferably from the individual concerned. Added requirement of also having the individual's consent or one of the other prescribed matters in HPP1.1 present. Before, at or near, the time of collection, notify the individual of:</p> <ul style="list-style-type: none">• the organisation's contact details;• the purpose of collection;• an individual's right to access health information;• usual disclosures;• where the collection is required by law; and• the main consequences of not providing health information. <p>Where collect health information from third parties, tell individual whose personal information is collected of the six points listed above. Information communicated in confidence from third parties can be collected.</p>
HPP2	Use & Disclosure	<p>Use or disclose health information:</p> <ul style="list-style-type: none">• for the primary purpose for which the information was collected; or• for a directly related secondary purpose an individual would reasonably expect;• where individual consents;• law enforcement; or• other prescribed exceptions. <p>Where disclosure for law enforcement make a written note of the disclosure.</p>
HPP3	Data Quality	<p>Take reasonable steps to ensure that health information is accurate, complete, up to date and relevant to an organisation's functions.</p>
HPP4	Data Security & Data Retention	<p>Take reasonable steps to protect health information held from misuse, loss, unauthorised access, modification or disclosure. Health service provider must retain health information for prescribed periods. A non health service provider must retain for as long as lawful purpose. Provisions dealing with retention in other Acts, such as Public Records Act, apply to the public sector. For 30 years after death health information is protected by HPPs.</p>
HPP5	Openness	<p>Document clearly expressed policies on the management of health information and steps individuals have to take to access health information. Make the policies available to anyone who asks.</p> <p>On request take reasonable steps to let the enquirer know generally, what sort of health information the organisation holds, for what purposes, and how it collects and manages that information.</p>
HPP6	Access & Correction	<p>Administrative or formal procedures for access to health information under the Freedom of Information Act will apply in the public sector. FOI procedures for access to health information will apply where health information is held in the public sector. Where health information is held in the private sector, HRA procedures will apply. Information collected after 1 July 2002 accessed in full. If collected prior to 1 July 2002 at a minimum the individual is entitled only to a summary.</p> <p>If an individual is able to establish that their health information held by an organisation is not accurate, complete, and up to date, must take reasonable steps to correct the information.</p>
HPP7	Identifiers	<p>May only assign identifiers to individuals if is necessary for an organisation to carry out any of its functions efficiently.</p> <p>A private sector organisation may not adopt as its own identifier of an individual an identifier that has been assigned to that person by a public sector organisation unless prescribed exceptions apply.</p>
HPP8	Anonymity	<p>Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.</p>
HPP9	Transborder Data Flows	<p>May transfer health information about an individual to someone (other than the organisation or the individual) who is outside Victoria only if prescribed conditions apply.</p>
HPP10	Transfer or Closure of Practice of Health Service Provider	<p>If the practice or business of a health service provider is to be transferred or closed, the provider must comply with a prescribed set of procedures and statutory guidelines, centering on notification to former clients and the public.</p>
HPP11	Making Information Available to Another Health Service Provider	<p>If an individual requests a health service provider make their health information available to another provider, the former must comply with the request as soon as practicable.</p>

PRIVACY ACT 1988 (PA) NATIONAL PRIVACY PRINCIPLES (NPPs) PRIVATE SECTOR (including private health service providers) IN SUMMARY

Refer to Federal Privacy Commissioners Guidelines to the National Privacy Principles (NPPs) September 2001; Guidelines on Privacy in the Private Health Sector October 2001

NO.	SUBJECT	BRIEF SUMMARY
NPP1	Collection	<p>Collect personal information by lawful, fair and reasonable means necessary for an organisation's functions or activities and preferably from the individual concerned.</p> <p>Before, at or near the time of collection notify the individual of:</p> <ul style="list-style-type: none"> • the organisation's contact details; • the purpose of collection; • an individual's right to access personal information; • usual disclosures; • whether collection is required by law; and • the main consequences of not providing personal information. <p>Where personal information is collected from third parties tell the individual whose personal information is collected of the six points listed above.</p>
NPP2	Use & Disclosure	<p>Use or disclose personal information:</p> <ul style="list-style-type: none"> • for the primary purpose for which information was collected; or • for a directly related secondary purpose an individual would reasonably expect; • where individual consents; • for law enforcement; • for direct marketing if information is not "sensitive", it is impracticable to obtain consent and individual can opt out; or • for other prescribed exceptions. <p>If disclosing health information prescribed exceptions may apply. Where disclosure for law enforcement, make a written note of the disclosure.</p>
NPP3	Data Quality	<p>Take reasonable steps to ensure that the personal information it collects and manages is accurate, complete and up to date.</p>
NPP4	Data Security	<p>Take reasonable steps to protect personal information from misuse and loss and from unauthorised access, modification or disclosure. Destroy or permanently de-identify personal information no longer required. Provisions dealing with retention in other Acts may apply.</p>
NPP5	Openness	<p>Document clearly expressed policies on the management of personal information and steps individuals have to take to access health information. Make the policies available to anyone who asks.</p> <p>On request, take reasonable steps to let the enquirer know, generally, what sort of personal information is held, for what purposes, and how the organisation collects and manages that information.</p>
NPP6	Access & Correction	<p>Provide the individual with access to information on request by the individual, except to the extent that prescribed exceptions apply.</p> <p>If an individual establishes that the information is not accurate, complete and up to date, take reasonable steps to correct the information.</p>
NPP7	Identifiers	<p>May only assign an identifier to an individual where it is necessary to enable the organisation to carry out any of its functions efficiently.</p> <p>Must not adopt as its own identifier of an individual an identifier that has been assigned by another organisation unless prescribed exceptions apply.</p>
NPP8	Anonymity	<p>Wherever it is lawful and practicable individuals must have the option of not identifying themselves when entering transactions with an organisation.</p>
NPP9	Transborder Data Flows	<p>May transfer personal information about an individual to someone (other than the organisation or the individual) who is outside Australia only if prescribed conditions apply.</p>
NPP10	Sensitive Information	<p>Must not collect sensitive information about an individual unless prescribed exceptions apply.</p>

PRIVACY ACT 1988 (PA) FEDERAL PUBLIC SECTOR INFORMATION PRIVACY PRINCIPLES (FIPPs)* IN SUMMARY

*FIPPs have been used in order to differentiate the federal public sector privacy principles from the other principles. Refer to Guidelines issued by Federal Privacy Commissioner Guidelines for Information Privacy Principles (FIPPs) October 1994.

NO.	SUBJECT	KEY CONCEPTS
FIPP1	Collection	Collect personal information about an individual by lawful, fair and reasonable means necessary for one or more of its functions or activities.
FIPP2	Solicitation from Individual Concerned	At or near the time of collection notify the individual of: <ul style="list-style-type: none"> • the purpose of collection; • if the collection is required by law; and • usual disclosures.
FIPP3	Solicitation of personal information generally	Take reasonable steps to make sure that the personal information it collects and manages is relevant, up to date, complete, and does not intrude to an unreasonable extent on the personal affairs of an individual.
FIPP4	Storage and security of personal information	Take reasonable steps to protect the personal information it holds from loss and from unauthorised access, use, modification or disclosure and other misuse. Information destroyed or permanently de-identified if no longer required. Provisions dealing with retention of personal information in other Acts, such as the Archives Act may apply.
FIPP5	Information relating to records	Maintain a general record of what sort of personal information is held, for what purposes, classes of individuals who have access to information, and how individual can gain access. Must make this record available to general public and the Privacy Commissioner (Federal). Take steps to advise an individual of records containing personal information, the nature of the information, purposes for which that information is used and steps to obtain a record.
FIPP6	Access	Provide the individual with access to the information unless required or authorised to refuse under Commonwealth law.
FIPP7	Alteration of records	Take steps to make corrections, deletions and additions to ensure personal information is accurate, relevant, up to date, complete and not misleading, subject to limitations in Commonwealth law. Where unwilling to correct by deletion or addition must, if requested by individual, attach a statement of correction provided by individual.
FIPP8	Accuracy	Prior to use take steps to ensure personal information is accurate, up to date and complete.
FIPP9	Use for a relevant purpose	Personal information to be used only for a relevant purpose.
FIPP10	Limits on use	Use personal information; <ul style="list-style-type: none"> • for the particular purpose collected; • for a directly related purpose; • where an individual consents; • for law enforcement; or • where authorised and required by law. Where use is for law enforcement make a written note of the use. Information under Commonwealth contract not to be used for direct marketing unless prescribed exceptions at 16F of the PA apply.
FIPP11	Disclosure	Disclose personal information; <ul style="list-style-type: none"> • if the individual is likely to have been aware of the disclosure under FIPP2; • where an individual consents; • for law enforcement; or • where authorised or required by law. Where disclosure is for law enforcement, make a written note of the disclosure.

WHAT'S DIFFERENT - A COMPARISON OF THE HEALTH PRIVACY PRINCIPLES (HPPs), THE NATIONAL PRIVACY PRINCIPLES (NPPS) AND THE FEDERAL PUBLIC SECTOR INFORMATION PRIVACY PRINCIPLES (FIPPs) WITH THE IPPs

This table compares only the privacy principles. There are other differences between the legislation. Some codes of practice for particular industries operate, which replace the privacy principles. Check these differences too.

Information Privacy Principle	Key Differences Compared to IPPs
IPP 1 Collection	<p>HPP1 – At time of collection must have at least one of the prescribed requirements set out in HPP 1.1(a) – (i) present. Separate section on health information communicated to health service provider in confidence by third party.</p> <p>FIPP – No specific mention of collection from an individual or third parties.</p>
IPP2 Use & Disclosure	<p>HPP – Added exceptions listed at HPP 2.2(d), ((e) – use only (f), (g), 2.4, and 2.5).</p> <p>NPP - Has a limited exception for direct marketing.</p> <p>FIPP - Separate principles for use. One concerns purpose and the other refers to limits on use. Section 16F of the PA limits the use and disclosure of information under Commonwealth contract for direct marketing unless prescribed exception applies.</p>
IPP3 Data Quality	<p>FIPP – Separate principles for accuracy. One concerns accuracy at time of collection the other refers to accuracy prior to use.</p>
IPP4 Data Security	<p>HPP – Health service provider must retain health information for prescribed minimum period. The destruction or transfer of health information must be in accordance with prescribed requirements. Health information is protected by privacy laws for 30 years after death.</p>
IPP5 Openness	<p>FIPP – Policy has to contain different matters. A copy is to be available for general public inspection and the Federal Privacy Commissioner holds a copy.</p>
IPP6 Access & Correction	<p>HPP – Specifically prevents access where there is a threat to the life or health of individual, where information communicated in confidence by third party to health service provider. Access and correction under HPP6 has sections which cover: proof of identity, evidence of authority to act for another, an ability to access information by viewing health information and being provided with an explanation of what the health information means by a health service provider.</p> <p>NPP - Provides and exception for limiting access to health information where there is a threat to the life or health of individual.</p> <p>FIPP – Must give access and can only refuse if permissible under Commonwealth law. Correction is a separate principle.</p>
IPP7 Unique Identifiers	<p>FIPP - No separate principle. Discussed elsewhere in the Act under TFN information section, section 17 of the Privacy Act,</p>
IPP8 Anonymity	<p>FIPP – No separate principle.</p>
IPP9 Transborder Data Flows	<p>FIPP – No separate principle.</p>
IPP10 Sensitive Information	<p>HPP – No separate principle.</p> <p>FIPP – No separate principle.</p>
Additional	<p>HPP – Separate principle Transfer or closure of the practice of a health service provider. *Only applies to health service provider</p>
Additional	<p>HPP – Separate principle Health service provider making information available to another health service provider (only applies to a health service provider).</p>

WHAT'S SIMILAR - A COMPARISON OF THE HEALTH PRIVACY PRINCIPLES (HPPs), THE NATIONAL PRIVACY PRINCIPLES (NPPs) AND THE PUBLIC SECTOR PRIVACY PRINCIPLES (FIPPs) WITH THE IPPs

Information Privacy Principle

Key Similarities Compared to IPPs

IPP1 Collection

HPP, NPP, FIPP – Collect lawfully fairly, and by reasonable means where necessary for functions.

Tell the individual the purpose of collection, whether the collection is required by law and who the organisation usually discloses personal information to.

IPP2 Use & Disclosure

HPP, NPP, FIPP – Disclose or use for a primary purpose. Secondary use and disclosures are permitted where:

- the individual has consented; or
- for a law enforcement purpose; or,
- where authorised or required by law.

Make a note of any disclosures or uses for law enforcement.

IPP3 Data Quality

HPP, NPP, FIPP – Take reasonable steps to ensure information is accurate, up to date and complete.

IPP4 Data Security

HPP, NPP, FIPP – Take reasonable steps to prevent information against loss, unauthorised access, use, modification and disclosure.

IPP5 Openness

HPP, NPP, FIPP – Organisations to have a policy on the management of information.

IPP6 Access & Correction

HPP, NPP, FIPP – Individuals have a right of access to their personal or health information subject to certain exceptions, and they can also seek to correct it.

IPP7 Unique Identifiers

HPP, NPP – Assign unique identifiers only necessary to functions. Do not adopt other organisations' unique identifiers unless exceptions apply.

IPP8 Anonymity

HPP, NPP – Where lawful and practicable give individuals the choice of transacting anonymously.

IPP9 Transborder data Flows

HPP, NPP – Where personal or health information is transferred out of one privacy protection regime it should be protected by another privacy regime unless exceptions apply.

IPP10 Sensitive Information

NPP – Do not collect sensitive information unless a prescribed exception applies.