# Quick reference guide: comparison of the IPPs, HPPs and APPs

This quick reference guide has been developed to provide users with a side-by-side comparison of the privacy obligations under the *Privacy and Data Protection Act 2014* (Vic), *Health Records Act 2014* (Vic) and *Privacy Act 1988* (Cth).

You will notice that the three pieces of legislation cover similar principles and the obligations under each are similar. However, there are also important differences between them, we therefore advise you to refer to the relevant Act when applying the principles. The language in this guide has been summarised to be used as a quick reference tool.

|  |  |  |
| --- | --- | --- |
| **Information Privacy Principles (IPPs)** | **Health Privacy Principles (HPPs)** | **Australian Privacy Principles (APPs)** |
| **Legislation** |
| *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) | *Health Records Act 2014* (Vic) (**HR Act**) | Privacy Act 1988 (Cth) (**Privacy Act**) |
| **Regulator** |
| Office of the Victorian Information Commissioner (**OVIC**) | Health Complaints Commissioner (**HCC**) | Office of the Australian Information Commissioner (**OAIC**) |
| **What types of entities are covered?** |
| * Victorian public sector organisations; or
* Contracted service providers to a VPS organisation with a State contract including specific clause binding them to comply with IPPs.

(See section 13 of the PDP Act) | * Health service providers providing a health service in Victoria; or
* Non-health service providers handling health information in Victoria.

(See sections 10, 11 and 12 of the HR Act) | * Australian government agencies; or
* Private organisations with an annual turnover of $3 million or more.

(See sections 15 and 6 of the Privacy Act).  |
| **What types of information are covered?** |
| **Personal information** defined as information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies.(See section 3 of the PDP Act) | **Health information** includes:* Information or an opinion about a person’s disability; physical, mental or psychological health; the health services they have had or plan to receive; or their expressed wishes about the future provision of health services.
* Other personal information collected in providing a health service or in connection with the donation of their body parts.
* Other personal information that is genetic information about that individual that could predict the health of that individual or their descendants.

(See section 3 of the HR Act)  | **Personal information** defined as any information or an opinion about an identified individual or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether the information or opinion is recorded in a material form or not.(See section 6 of the Privacy Act) |
| **Duty to take proactive privacy measures** |
| **Not applicable.**  | **Not applicable.**  | **APP 1.1** – You must take reasonable steps to implement practices and systems that will ensure your organisation’s compliance with the APPs. |

|  |
| --- |
| **Collection** |
| **IPP 1.1 -** You can only collect personal information that is necessary for the performance of one or more of your organisation’s functions. | **HPP 1.1 -** You can only collect health information if:* it is necessary for the performance of one or more of your organisation’s functions **and**
* either the individual has consented, or the collection meets another condition set out at HPP 1.1(b) - (i).
 | **APP 3-** You can only collect personal information that you request if it is reasonably necessary for one or more of your organisation’s functions.**APP 4 -** If you receive personal information which you did not request (**unsolicited**), you must determine whether your collection of this information would have been authorised by applying the test from APP 3. If you determine that the collection would not have been authorised, then you must, as soon as practicable and only if it is lawful, destroy the information or ensure it is de-identified.  |
| **IPP 1.2** – You can only collect personal information by lawful and fair means and not in an unreasonable intrusive way. | **HPP 1.2** – You can only collect health information by lawful and fair means and not in an unreasonable intrusive way. | **APP 3.5 –** You can only collect personal information by lawful and fair means.  |
| **IPP 1. 4 –** Where reasonable and practicable, you should collect personal information about an individual directly from that individual.  | **HPP 1.3 -** Where reasonable and practicable, you should collect health information about an individual directly from that individual. | **APP 3.6 –** You can only collect personal information about an individual directly from that individual unless it is unreasonable or impracticable to do so or otherwise authorised by APP 3.6. |

|  |  |  |
| --- | --- | --- |
| **IPP 1.3 and 1.5** – When collecting personal information, either directly from the individual or indirectly from a third party, you should make the individual aware of:* how they are able to contact your organisation;
* that the individual is able to gain access to their personal information;
* the purposes you are collecting the personal information for;
* the types of individuals or organisations you usually disclose personal information to;
* any law that requires the particular information to be collected; and
* the main consequences for the individual if any of the personal information is not collected.
 | **HPP 1.4 and 1.5 -** When collecting health information, either directly from the individual or indirectly from a third party, you should make the individual aware of:* how they are able to contact your organisation;
* that the individual is able to gain access to their health information;
* the purposes you are collecting the health information for;
* the types of individuals or organisations you usually disclose health information to;
* any law that requires the particular information to be collected; and
* the main consequences for the individual if any of their health information is not collected.
 | **APP 5.1** – When collecting personal information, either directly from the individual or indirectly from a third party, you should make the individual aware of:* how they are able to contact your organisation;
* if you have collected personal information from someone other than the individual, that you have done so;
* the purposes you are collecting the personal information for;
* the types of individuals or organisations you usually disclose personal information to;
* any law that requires the particular information to be collected;
* the main consequences for the individual if any of their personal information is not collected; and
* that your privacy policy contains further information.
 |

|  |  |  |
| --- | --- | --- |
| **Not applicable.**  | **HPP 1.7 –** You must take reasonable steps to ensure that the health information you hold remains confidential where:* you receive health information from a recipient who is not the individual that the health information is about; or
* you receive health information from a health service provider that provided a health service to the individual; and
* in either case, the provider of the health information requests that you do not communicate that information to the individual that the information is about.
 | **Not applicable.**  |

|  |
| --- |
| **Use and disclosure** |
| **IPP 2 –** You should only use or disclose personal information: * for the primary purpose for which it was collected; **or**
* for a secondary purpose **if** one of the exceptions to the primary purpose rule (set out at IPP 2.1(a) – (h)) applies, such as:
	+ the secondary purpose is related to the primary purpose of collection and the individual would reasonably expect your organisation to use or disclose the information for this secondary purpose;
	+ the individual has consented;
	+ the use or disclosure is reasonably necessary to lessen or prevent a serious threat to the individual’s life or the public’s health or safety;
	+ you have reason to suspect that lawful activity has been engaged in and the use or disclosure is necessary as part of your organisation’s investigation or in reporting the matter to the relevant authorities;
	+ the use or disclosure is authorised by law;
	+ the use or disclosure is reasonably necessary to assist a law enforcement agency perform its function or to protect the public revenue.
 | **HPP 2** – You should only use or disclose health information:* for the primary purpose for which it was collected; **or**
* for a secondary purpose **if** one of the exceptions to the primary purpose rule (set out at HPP 2.2) applies, such as:
	+ the secondary purpose is directly related to the primary purpose and the individual would reasonably expect your organisation to use or disclose the information for this secondary purpose;
	+ the individual has consented;
	+ the use or disclosure is authorised by law;
	+ you are a health service provider providing a health service to the individual **and** the use or disclosure is reasonably necessary for the provision of the health service **and** the individual is incapable of giving consent **and** it is not practicable to obtain consent from their authorised representative;
	+ the use or disclosure does not identify the individual and is for the purposes of managing a health service or training your employees in providing a health service;
	+ the use or disclosure is reasonably necessary to lessen or prevent a serious threat to the individual’s life or the public’s health and safety;
	+ you have reason to suspect that lawful activity has been engaged in and the use or disclosure is necessary as part of your organisation’s investigation or in reporting the matter to the relevant authorities;
	+ the use or disclosure is reasonably necessary to assist a law enforcement agency to perform its function;
	+ the use or disclosure is necessary to establish a legal claim.

. | **APP 6** – You should only use or disclose personal information:* for the primary purpose for which it was collected; **or**
* if the individual has consented; **or**
* for a secondary purpose **if** one of the exceptions to the primary purpose rule (set out at APP 6.2) applies, such as:
	+ the secondary purpose is related to the primary purpose and the individual would reasonably expect your organisation to use or disclose the information for this secondary purpose;
	+ the use or disclosure is authorised by law;
	+ a permitted general satiation exists (see s 16A and s 16B);
	+ the use or disclosure is reasonably necessary to assist a law enforcement body to perform its function.
 |

|  |
| --- |
| **Marketing** |
| **Not applicable.**  | **Not applicable.**  | **APP 7** – You must not use or disclose personal information for the purposes of direct marketing unless otherwise authorised by APP 7.  |
| **Data quality** |
| **IPP 3** – You must take reasonable steps to ensure that the personal information you collect, use or disclose is accurate, complete and up to date. | **HPP 3** – You must take reasonable steps, to ensure that the health information you collect, use or disclose is accurate, complete, up to date and relevant to your organisation’s function. | **APP 10** – You must take reasonable steps to ensure that the person you collect is accurate, up to date and complete. You must also take reasonable steps to ensure that the personal information you use or disclose is accurate, up to date, complete and relevant to your organisation’s functions. |
| **Data security** |
| **IPP 4.1** – You must take reasonable steps to protect the personal information your organisation holds from misuse, loss and from unauthorised access, modification or disclosure. | **HPP 4.1** – You must take reasonable steps to protect the health information your organisation holds from misuse, loss and from unauthorised access, modification or disclosure. | **APP 11.1** – You must take reasonable steps to protect personal information your organisation holds from misuse, interference, loss and from unauthorised access, modification or disclosure. |

|  |
| --- |
| **Destruction or de-identification** |
| **IPP 4.2 –** If you no longer need personal information for any purpose, you must take reasonable steps to destroy or permanently de-identify it. | **HPP 4.2 and 4.5** – If you no longer need health information for the purpose for which it was collected or any other authorised purpose then you must take reasonable steps to destroy or permanently de-identify it. You must hold the health information for 7 years after the health information was collected or, in the case of a child, until the individual turns 25. | **APP 11.2** – If you no longer need personal information for any purpose, the information is not contained in a Commonwealth record and you are not required to retain the information under any law or court order, then you must take reasonable steps to destroy the information or de-identify it. |
| **Not applicable.**  | **HPP 4.3 and 4.4** – If you delete health information or transfer it to another organisation and cease to hold it, you must make a written note of the transfer or destruction.  | **Not applicable.**  |
| **Openness** |
| **IPP 5.1 –** You must set out, in a clearly expressed document, your organisation’s policy on the handling of personal information. You must make this document available to anyone who asks for it. | **HPP 5.1 –** You must set out, in a clearly expressed document, your organisation’s policy on the handling of health information and the steps that an individual can take in order to obtain access to their health information. You must make this information available to anyone who asks for it. | **APP 1.3** – You must set out, in a clearly expressed and up to date document, your organisation’s policy on the handling of personal information. The document must contain the information in APP 1.4 and you must make this document available to anyone who asks for it. |

|  |  |  |
| --- | --- | --- |
| **IPP 5.2** – If you are requested by an individual, you must take reasonable steps to let them know:* the general nature of what sort of personal information you hold;
* for what purposes you collect the information; and
* how you collect, hold, use and disclose that information.
 | **HPP 5.2 –** If you are requested by an individual, you must take reasonable steps to let them know:* whether you hold health information about them;
* the steps that the individual can take if they wish to obtain access to their health information;
* the nature of the health information;
* the purposes for which the health information is used; and
* how you collect, hold, use and disclose health information.
 | **Not applicable.**  |
| **Access** |
| **IPP 6** – You must provide an individual, upon their request, with access to their personal information unless one of the exceptions in IPP 6 applies.IPP 6 only applies where an individual cannot access their personal information under the *Freedom of Information Act 1982* (Vic.).  | **HPP 6 –** You must provide an individual, upon their request, with access to their health information in accordance with Part 5 of the Act unless one of the exceptions in HPP 6 applies.HPP 6 only applies where an individual cannot access their health information under the *Freedom of Information Act 1982* (Vic.). | **APP 12** – You must provide an individual, upon their request, with access to their personal information unless one of the exceptions in APP 12 applies.APP 12 operates alongside and does not replace other legal procedures by which an individual can access their information, including the *Freedom of Information Act 1982* (Cth.).  |

|  |
| --- |
| **Correction** |
| **IPP 6.5** – Where an individual informs you that the personal information you hold about them is not accurate, complete or up to date, you must take reasonable steps to correct that information. \* See above note regarding IPP 6. | **HPP 6.5** – Where an individual informs you that the health information you hold about them is inaccurate, incomplete, misleading or not up to date, you must take reasonable steps to correct that information. \* See above note regarding HPP 6. | **APP 13** – Where an individual informs you or you are not yourself satisfied that the personal information you hold about them is accurate, up to date, complete, relevant and not misleading, then you must take reasonable steps to correct the information. Special considerations apply to Commonwealth records, which can only be altered in accordance with the *Archives Act 1983* (Cth.). |
| **Unique and government identifiers** |
| **IPP 7** – You must not assign, adopt, use or disclose a unique identifier unless doing so is necessary for your organisation to carry out its functions or otherwise authorised by IPP 7.  | **HPP 7** – You must not assign, adopt, use or disclose a unique identifier unless doing so is reasonably necessary for your organisation to carry out its functions or otherwise authorised by HPP 7.  | **APP 9** – You must not adopt a government related identifier as your own unless doing so is authorised by APP 9. You must not use or disclose a government related identifier unless the use or disclosure is reasonably necessary for you to verify the identity of the individual or is otherwise authorised by APP 9. |

|  |
| --- |
| **Anonymity** |
| **IPP 8** – When entering into transactions with your organisation, you must provide individuals with the option of not having to identify themselves, unless such an option is not lawful or practicable.  | **HPP 8** – When entering into transactions with your organisation, you must provide individuals with the option of not having to identify themselves, unless such an option is not lawful or practicable.  | **APP 2** – When dealing with your organisation, you must provide individuals with the option of not having to identify themselves or of using a pseudonym. The exception is where your organisation is required to deal with only individuals who identify themselves or it is impracticable for you to do so. |
| **Transborder data flows** |
| **IPP 9 –** You must not transfer personal information to a third-party recipient outside of Victoria unless: * that recipient is subject to similar obligations as the IPPs when handling that information; **or**
* the individual, who the information is about, has consented; **or**
* the transfer is otherwise authorised by IPP 9.
 | **HPP 9** – You must not transfer health information to a third-party recipient outside of Victoria unless: * that recipient is subject to similar obligations as the HPPs when handling that information; **or**
* the individual, who the information is about, has consented; **or**
* the transfer is otherwise authorised by HPP 9.
 | **APP 8** – Before you disclose personal information to a third-party recipient located overseas, you must take reasonable steps to ensure that the recipient does not breach the APPs when handling that information. If you fail to do so, you may be accountable for the actions of the recipient. However, you will not be held accountable if one of the exceptions from APP 8 applies. |

|  |
| --- |
| **Sensitive information** |
| ‘**Sensitive information**’ includes information about an individual’s: ethnic origin; political opinions; membership of political or professional trade association; religious beliefs; philosophical beliefs; sexual preferences; or criminal record. | **Not applicable.**  | ‘**Sensitive information**’ includes information about an individual’s: ethnic origin; political opinions; membership of political or professional trade association; religious beliefs; philosophical beliefs; sexual preferences; criminal record; health information; genetic information that is not otherwise health information; or biometric information. |
| **IPP 10** – You must not collect sensitive information unless: * the individual, who the information is about, has consented; **or**
* the collection is otherwise authorised by IPP 10.
 | **Not applicable.**  | **APP 3.3 –** You must not collect sensitive information unless: * the individual, who the information is about, has consented and the information is reasonably necessary for one or more of your organisation’s functions; **or**
* the collection is otherwise authorised by APP 3.3.
 |

|  |  |  |
| --- | --- | --- |
| There are some modifications to the way sensitive information can be used or disclosed; such as the requirement that, if being disclosed for a secondary reasonably expected purpose, the secondary purpose is directly related to the primary purpose of collection (not merely related).  | **Not applicable.**  | There are some modifications to the way sensitive information can be used or disclosed; such as the requirement that, if being disclosed for a secondary purpose that the individual would expect, the secondary purpose is directly related to the primary purpose of collection (not merely related).  |
| **Transfer or closure of practice** |
| **Not applicable.**  | **HPP 10** – If you are a health service provider and your practice is to be sold or closed, you must:* publish a notice in a local newspaper stating that your practice is about to be sold or closed down and the manner in which you propose to deal with the health information held by your practice; **and**
* provide individuals with the option of having their health information transferred to the health service provider taking over your practice or any other health service provider nominated by the individual.
 | **Not applicable.**  |

|  |
| --- |
| **Making information available to another health service provider** |
| **Not applicable.**  | **HPP 11 –** If you are a health service provider and an individual requests that you transfer their health information to another health service provider, you must provide a copy or summary of the health information you hold about the individual to the health service provider that the individual has nominated.  | **Not applicable.**  |