

## The Information Privacy Principles and the Health Privacy Principles

The Information Privacy Principles (IPPs) under the *Privacy and Data Protection Act 2014* (PDPA) and the Health Privacy Principles (HPPs) under the *Health Records Act 2001* (HRA) are strongly aligned. There is a significant amount of overlap in the first 9 principles with only a few key differences as outlined below. IPP 10 and HPP 10 and 11 are unique to their own legislation and so are addressed separately on the following page. This information sheet provides a basic overview only. Organisations seeking further information should refer to the PDPA, the HRA, relevant guidance material, or obtain legal advice.

The IPPs apply to *personal information* under the PDPA, while the HPPs apply to *health information* under the HRA. It is important for organisations to know the type of information they are handling, and if they have obligations under the PDPA or HRA (or both). Generally, personal information is information or opinion in any form, true or false, which can identify an individual but does *not include* health information under the HRA. Health information includes any information or opinion about an individual's physical, mental, or psychological health, health services, disabilities, organ donation, and genetic information, as well as any personal information supplied for the purpose of obtaining a health service. The HRA continues to apply to deceased individuals for up to 30 years, while the PDPA does not. Please refer to the full text of either act for complete definitions.

### Similar principles

### Key differences

#### 1. Collection

An organisation must not collect personal or health information about an individual unless it is necessary for one or more of its functions.

Collection must be lawful, by fair means, and not unreasonably intrusive. Organisations should endeavour to collect directly from individuals, and whether information is collected directly or indirectly (i.e. from another person or organisation), organisations must take reasonable steps to provide notice that their information has been collected.

*As well as being necessary, the HPPs require at least one of nine conditions to be met. Generally this is **consent**, however there are eight other instances listed under HPP1.1.*

#### 2. Use and Disclosure

An organisation must not use or disclose personal or health information for a purpose other than the primary purpose.

IPP and HPP 2 have 8 and 12 exceptions respectively, which allow for use and disclosure of personal or health information for a secondary purpose under certain circumstances including where there is individual consent, if required by law, or to prevent serious and imminent harm.

*In addition to the shared exceptions, the HPPs include health-specific exceptions for use and disclosure for a secondary purpose. These include (but are not limited to) disclosure for evaluation of a health service.*

#### 3. Data Quality

Organisations must take reasonable steps to ensure that the personal or health information it collects, uses or discloses is accurate, complete and up to date.

*HPP 3.1 also requires health information to be **relevant** to its functions or activities as a data quality issue.*

#### 4. Data Security

Organisations must take reasonable steps to protect the information it holds from misuse, loss, unauthorised access, modification or disclosure.

*Under IPP 4.2, information no longer required for any purpose must be **deleted or de-identified**. HPP 4 refers to security **and retention**, prohibiting the deletion of health information relating to an individual (even if inaccurate) by health service providers unless permitted under certain circumstances.*

## 5. Openness

Organisations must set out in a document clearly expressed policies on its management of personal or health information, which should be available to anyone who asks for it.

*No key difference.*

## 6. Access and Correction

An organisation that holds personal or health information must provide individuals with access to their information except in certain circumstances (e.g. providing access would pose a serious threat to life or health, or it would have an unreasonable impact on privacy).

If the individual is able to establish that the information held about them is not accurate, complete or up to date, the organisation must take reasonable steps to correct the information.

Note: in certain circumstances individuals will need to make a request under the *Freedom of Information Act 1982* to access information, rather than the PDPA or HRA.

*A health service provider may correct health information about an individual so that it is accurate, however it must not delete the information in accordance with HPP 4.2, even if it is inaccurate.*

## 7. Unique Identifiers

Unique identifiers should not be assigned to individuals unless it is reasonably necessary to enable the organisation to carry out any of its functions efficiently.

*HPP 7.4 includes circumstances pertaining to using and disclosing unique identifiers between public and private organisations.*

## 8. Anonymity

Wherever lawful and practicable, individuals must have the option of not identifying themselves.

*No key difference.*

## 9. Transborder data flows

Organisations may only transfer information (health or personal) to someone outside of Victoria under certain circumstances.

*No key difference.*

## Principles unique to the PDPA or HRA

### **IPP 10. Sensitive information**

Organisations must not collect sensitive information (as defined in the PDPA) unless under certain circumstances, for example: consent, required by law, to prevent harm.

### **HPP 10. Transfer or closure of the practice of a health service provider**

Health service providers must comply with certain requirements.

### **HPP 11. Making information available to another health service provider**

If an individual requests their health information to be made available to another health services provider they must do so.

Please note that the contents above are for general information purposes only, and should not be relied upon as legal advice. This office does not guarantee or accept legal liability whatsoever arising from, or connected to the accuracy and reliability of the contents of this information.