

# HEALTH PRIVACY PRINCIPLES

## Background

There are 11 Health Privacy Principles listed in [Schedule 1 of the Health Records Act 2001 \(Vic\)](#) (“the Act”).

## Application of the Health Privacy Principles

The Health Privacy Principles applies to the University of Melbourne (“the University”) to the extent that it collects, holds or uses health information.

## Definition of health information

Under [section 3 of the Act](#), “health information” may include the following:

- An individual’s physical, mental or psychological health;
- Any disability that an individual may have, or may have had;
- Any health services that have been, or are to be, provided to an individual;
- The individual’s wishes about what health services are to be provided to them;
- Any personal collected in relation to:
  - Providing a health service
  - Donating body parts, organs or substances;
- Genetic information which could be used to predict the health of an individual or their descendants.

## Relevant terminology

- **Consent** means permission. Consent is only valid if:
  - The individual has capacity to give consent;
  - It is voluntary;
  - It is informed;
  - It is specific to the circumstances; and
  - It is current.
- **Identifier** means an identifier (e.g. a number) that is used to uniquely identify an individual.
- **Primary Purpose** means the purpose for which information is collected, or the intended use for the information.
- **Secondary Purpose** means any purpose other than the Primary Purpose.

# SUMMARY OF HEALTH PRIVACY PRINCIPLES

## 1 Collection

- As a general rule, health information may only be collected if it is necessary for the University's functions and the individual has provided consent. In limited circumstances, health information may be collected without consent (e.g. if it is necessary to prevent serious harm to a person's life or safety).
- Health information must be collected lawfully, fairly, reasonably and preferably directly from the individual.
- Prior to, or at the time of, collecting health information, the University must notify the individual of:
  - Why the information is being collected;
  - Who has access to the information; and
  - How they can access or amend their health information.

## 2 Use and Disclosure

- The University may use or disclose health information for the Primary Purpose in which it was collected.
- The University may not use or disclose health information for a Secondary Purpose unless:
  - It is directly related to the Primary Purpose and reasonably expected by the individual; or
  - The individual has provided consent; or
  - It is permitted by law (e.g. to prevent serious harm to a person's life or safety).

## 3 Data Quality

- The University must take reasonable steps to ensure that the health information held is accurate, complete, up-to-date and relevant to its functions or activities.

## 4 Data Security and Retention

- The University must protect health information from unauthorised access, modification or disclosure.
- Health service providers must retain health information for a prescribed period of time.
- All other areas of the University must destroy or permanently de-identify health information if it is no longer needed.

## **5 Openness**

- The University must ensure that its [Privacy Policy](#) is easily accessible.
- If the University holds health information about an individual, it must let the individual know:
  - What the information is;
  - Why the information is held; and
  - How the information is collected, held, used and disclosed.

## **6 Access and Correction**

- As a general rule, individuals have a right to access and correct any health information they have provided.
- The University may, in some circumstances, refuse to provide access to health information. If so, the University must provide written reasons for the refusal.

## **7 Identifiers**

- The University may only assign identifiers to individuals if it is reasonably necessary to carry out its functions efficiently.

## **8 Anonymity**

- As far as it is lawful and practicable, individuals should have the opportunity to transact anonymously with the University.

## **9 Transborder Data Flows**

- When health information travels outside Victoria, the University has a responsibility to ensure that the privacy of the information is safeguarded.

## **10 Transfer/closure of health service provider**

- If a health service provider is to be sold, transferred or closed down, it must notify its current or former clients.

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

- Upon request from an individual, a health service provider must make information about that individual available to another health service provider.

