

PRIVACY – KEY DEFINITIONS

Access

The ability to view, obtain or retrieve information in any form to any other person.

Direct Identifier

A direct identifier is any information that directly identifies a single individual. Direct identifiers may consist of one or more variables that can be used to identify an individual, either by themselves or in combination with other readily available sources of information. Examples include name, address, email address, telephone number, health card number, staff or student number, device identifier, internet protocol (IP) address number and web universal locator (URL).

Disclosure

Making the information accessible or visible to others outside the organisation holding the information.

Health Information

Health information is defined in the Health Records Act (Vic) 2001 to include:

- information or opinion about the physical or mental health, or disability, of an individual
- an individual's expressed preferences about the future provision of health, disability or aged care services to the individual
- the nature of health, disability or aged care services that have been, or are to be, provided to an individual
- information originally collected in the course of providing a health, disability or aged care service to an individual
- personal information collected in connection with the donation of human tissue
- genetic information that is or could be predictive of the health of an individual or their descendants

Hold

The information is contained in a document that is in the possession or under the control of the University. This can be solely in the possession or control of the university or jointly with another organisation. The location of the document is irrelevant – i.e. it may be within Victoria or outside Victoria.

Modification

Changing, removing or adding components to the original information.

Personal Information

Personal information is defined in the Privacy and Data Protection Act 2014 (Vic) and includes any 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 be reasonably ascertained from the information or opinion but does not include information of a kind to which the Health Records Act 2001 applies. Examples include:

- name, address, birth date, telephone number, email address
- age, sex, marital status
- finger prints and other biometrics
- employment, educational, financial or criminal history
- an image in a photograph or voice in a recording
- location data, device details, online identifier (in some circumstances)

Personal information may include unique identifiers, direct identifiers and quasi identifiers – these are explained below. Context and/or linking of information may result in seemingly unidentified information becoming personal information.

Quasi Identifier

Quasi identifiers do not of themselves enable the identification of an individual but can be aggregated and linked with other information to identify an individual. Examples include date of birth, age, gender, postcode and other demographic information.

Context is also a factor in determining if seemingly non personal information is in fact classified as personal information.

Sensitive Information

Sensitive information is defined in the Privacy and Data Protection Act 2014 (Vic) to mean information or an opinion about an individual's

- racial or ethnic origin, or
- political opinions, or
- membership of political associations, or
- religious beliefs or associations, or
- philosophical beliefs, or
- membership of a professional or trade association, or
- membership of a trade union, or
- sexual orientation or practices, or
- criminal record,

that is also personal information.

Unique Identifier – Health Information

A unique identifier, as defined by the Health Records Act 2001 (Vic), means an [identifier](#) which is usually, but need not be, a number, and does not include an [identifier](#) that consists only of the [individual](#)'s name, that is:

- assigned to an [individual](#) in relation to the [individual](#)'s [health information](#) by an [organisation](#) for the purpose of uniquely identifying that [individual](#), whether or not it is subsequently used otherwise than in relation to [health information](#); or
- adopted, used or disclosed in relation to the individual's health information by an organisation for the purpose of uniquely identifying that individual.

Unique Identifier – Personal Information

A unique identifier, as defined by the Privacy and Data Protection Act 2014 (Vic), means an identifier (usually a number) assigned by an organisation to an individual to uniquely identify that individual for the purposes of the operations of the organisation. It does not include an identifier that consists only of the individual's name and does not include an identifier within the meaning of the Health Records Act.

Examples include:

- student id number
- staff id number
- statistical linkage key comprised of a person's initials and date of birth (e.g. JHS 21051915)
- driver's license number
- passport number
- tax file number
- vehicle registration number
- IP address
- online identifier – in some circumstances
- device details – in some circumstances.

Misuse

Personal or health information is misused if it is used in a way that contravenes any of the Information or Health Privacy Principles – particularly IPP 2 and HPP 2, which deal with use and disclosure.

Loss

The physical whereabouts of information that is unknown (including both hard and/or soft copies), and involves the failure to preserve or maintain the information in a known place. Loss does not include the intentional destruction or de-identification of information.

Unauthorised access, modification or disclosure

Access, modification or disclosure of information will be unauthorised where an individual:

- has no proper authority to access, modify or disclose the information; or
- exceeds their authority by acting beyond their power; or
- misuses their authority to access, modify or disclose the information.

Confidentiality

For the purposes of data security, confidentiality refers to the limiting of official information to authorised persons for approved purposes, commonly understood as the 'need to know'.

Integrity

For the purposes of data security, integrity refers to the assurance that information is only created, modified or deleted only by intended and authorised means and it is correct and valid.

Availability

For the purposes of data security, availability allows authorised persons to access particular information for authorised purposes, at the time they need to do so.