



Understanding Privacy

An overview of the Information Privacy Act 2000

Steve Halliwell

Deputy University Secretary

hals@unimelb.edu.au

privacy-officer@unimelb.edu.au

8344 6398

<http://www.unimelb.edu.au/unisec/privacy/>



- What is Information Privacy?
- The 10 Information Privacy Principles
- The Three Key Areas
 - Collection
 - Use and disclosure
 - Management





The Privacy Protection Landscape



Privacy Act 1988 (Cth)

- Personal information handled by Federal govt agencies, e.g. Centrelink
- Much of the private sector



Health Records Act 2001 (Vic)

- All health related personal information held in public and private sectors
- Most of the personal info handled by health service providers



Information Privacy Act 2000 (Vic)

- All recorded personal information handled by State government agencies and local government (other than health related info)



Charter of Human Rights & Responsibilities Act 2006 (Vic)

- Victorian government departments & agencies must act compatibly with human rights – including explicitly, the right to privacy



Recorded information or opinion
whether **true or not** about an
individual whose **identity** is apparent
or can be **reasonably ascertained**





Information Privacy Principles

1) Collection

6) Access and Correction

2) Use and Disclosure

7) Unique Identifiers

3) Data Quality

8) Anonymity

4) Data Security

9) Transborder Data Flows

5) Openness

10) Sensitive Information





- IPPs are connected and set minimum standards for how personal information should be handled:
 - Collection (IPPs 1, 8, and 10)
 - Use and disclosure (IPPs 2 and 9)
 - Management (IPPs 3, 4, 5, 6 & 7)
 - Remember **COLLUDIMAN**
-



When collecting personal information, include a **Privacy Collection Notice** that says:

- **who** is collecting the information;
- **what** it will be used for;
- **how** the person can get access to the information;
- **who else** usually has access to the information;
- **whether** it is required by law; and
- **what** the main consequences are, if any, for the person if they do not provide the information.



Use and Disclose only:

- For the **Primary Purpose** for which it was collected **OR**
- For a **Secondary Purpose** that is related and a person would expect **OR**
- With **Consent** that is
 - Voluntary
 - Informed
 - Specific
 - Current





Have **policies and procedures** in place to ensure:

- personal information is
 - **accurate** and **up-to-date**
 - **physically secure**
 - **operationally secure**
 - individuals are provided with **access** to their personal information (**FOI** may apply)
-

- **Collection**
 - collect only the information you need
 - advise people why you need the information and how it will be used and disclosed
- **Use and Disclosure**
 - use and disclose only for the primary purpose of collection, a reasonable secondary purpose or
 - with consent
- **Management**
 - Make sure it's accurate and up-to-date
 - Make sure it's secure





Head of Department is Responsible for:

1. **Containing** the breach
 2. **Evaluating** the risks
 3. **Notifying** the relevant people
 4. **Preventing** future breaches
 5. **Reporting** the breach
-