UNDERSTANDING PRIVACY

An overview of the Information Privacy Act 2000 (Vic)

Louise Goh
Lawyer – Compliance & Trusts
l.goh@unimelb.edu.au
8344 7919
Session outline

• 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.
<table>
<thead>
<tr>
<th></th>
<th>Information Privacy Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Collection</td>
</tr>
<tr>
<td>2</td>
<td>Use and Disclosure</td>
</tr>
<tr>
<td>3</td>
<td>Data Quality</td>
</tr>
<tr>
<td>4</td>
<td>Data Security</td>
</tr>
<tr>
<td>5</td>
<td>Openness</td>
</tr>
<tr>
<td>6</td>
<td>Access and Correction</td>
</tr>
<tr>
<td>7</td>
<td>Unique Identifiers</td>
</tr>
<tr>
<td>8</td>
<td>Anonymity</td>
</tr>
<tr>
<td>9</td>
<td>Transborder Data Flows</td>
</tr>
<tr>
<td>10</td>
<td>Sensitive Information</td>
</tr>
</tbody>
</table>
Information Privacy Principles set minimum standards for how personal information should be handled and can be divided into Three Key Areas:

**Collection** (IPPs 1, 8 and 10)
**Use and Disclosure** (IPPs 2 and 9)
**Management** (IPPs 3, 4, 5, 6 and 7)
Collection of Personal Information

University should collect Personal Information:

a. only when it is necessary for one or more of the University’s functions or activities;

b. in lawful and fair means, and not in an unreasonably intrusive way;

c. from the individual him or herself if possible; and

d. must advise the individual of certain matters (commonly via a Privacy Collection Notice)
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.
Privacy Collection Notice

• should be used every time personal information is being collected by the University

• will impact on how personal information may be **Used and Disclosed** by the University

Sensitive information (IPP 10) is personal information about an individual’s
• racial or ethnic origin,
• political opinions,
• religious beliefs or affiliations,
• philosophical beliefs,
• membership of a professional or trade association or a trade union,
• sexual preferences or practices, or
• criminal record.

General Rule: sensitive information can only be collected with the individual’s consent (limited exceptions apply)
Use and Disclosure of Personal Information

General Rule

Personal Information may be **used and disclosed** only for:

1. **Primary Purpose** for which it was collected **OR**

2. A related **Secondary Purpose** that would be reasonably expected **OR**

3. With **Consent** that is
   - Voluntary
   - Informed
   - Specific
   - Current
Some **Limited Exceptions to the General Rule**, including where use and disclosure is necessary for:

- research, or the compilation or analysis of statistics
- serious or imminent threat to the individual’s life, health or safety
- serious threat to public health or safety
- law enforcement purposes
- otherwise required by law

**ALWAYS SEEK ADVICE IF UNSURE!**
Management of Personal Information

Have policies and procedures in place to ensure:

- personal information is
  - accurate and up-to-date
  - secure
  - de-identified or destroyed if no longer needed (of course in accordance with PROV disposal schedules!)

- individuals are provided with access to their personal information (FOI may apply)
Summary

• **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
See: http://www.unimelb.edu.au/unisec/privacy/ for the University Privacy Policy, Privacy Procedure and Privacy Guidelines, along with other useful resources including FAQs, Summary of Information Privacy Principles.

Queries: privacy-officer@unimelb.edu.au