Privacy Impact Assessments – the Organisation versus the Individual’s viewpoints
Information and Communication Technology (ICT) projects can fail
It’s hard to escape from the fact that ICT **Privacy and Security** are critical issues

- especially in healthcare where private and highly **sensitive** data prevail
- in the media – the emphasis is on involving the consumers .......
"The potential of health information exchange will be realized only if privacy is addressed."

Washington Post, 11 March 08
Leslie Harris, president and CEO, Center for Democracy & Technology.

The developers of a successor to the federal advisory panel on healthcare IT are being told by stakeholders that privacy should be a top concern, and that consumers should be well represented this second time around.

Stakeholders call for AHIC's (American Health Information Community) successor to focus on consumers.

Healthcare IT News by Diana Manos, Senior Editor, 03/11/08
BUT - is it a case of the ‘too hard box’?

• Many critical aspects are not adequately addressed. e.g. privacy, ethics, acceptance, appropriate security measures, data linking, secondary data use and user consent issues

• Too often these complex and often emotive issues are placed in the infamous ‘too hard box’

• This is particularly prevalent when it involves consultation with third parties and end users
Consider the UK £4.5 billion ID card

‘The survey found confidence in the Government's ability to handle sensitive data had fallen among two thirds of adults, following the loss of discs containing the details of 25 million child benefit claimants’.

Information should be treated as sensitively and carefully as hard cash.
“2) Research Appropriate Models that Address Perceived Privacy Risk and Undertake More Extensive Surveys on User’s Attitudes”.

Dr P.R. Croll’s submission to the Government office of the Access Card
BUT how well are we doing?

Royal Perth Hospital dump computers, patient details

EXCLUSIVE: Paul Lampathakis
April 04, 2008 10:00pm

CONFIDENTIAL patient details are being left on old computers dumped in an open skip bin in a busy laneway at Royal Perth Hospital.

Personal information, including patient names and addresses, dates of birth, medical conditions and patient numbers, was accessed with ease by The Sunday Times this week.

Sources say up to 500 computers have been dumped in the bin, pending collection, since November.

Sources also claimed computers had been sent to auction yards in the past without their hard drives wiped clean.

The hospital yesterday denied this, saying the computer hard drives were cleaned and the computers were collected every day by contractors to be crushed.

Health Minister Jim McGinty last night accused The Sunday Times of stealing the computers and hacking into their contents.

The Sunday Times editor Sam Weir rejected the allegations. He said The Sunday Times observed the computers in the bin for several days, easily available for anyone to pick them up.
We could (should) do better

'Hacker shuts down government computers'

BY PHOEBE STEWART  May 16, 2008 07:10am

AN EXPERT hacker allegedly shut down the Northern Territory Government computer system and deleted thousands of employees' identities, a Darwin court heard yesterday.

And the court heard the Government could still be at risk of another cyber attack.
SECURITY ≠ PRIVACY
Privacy Impact Assessment (Australia)

• “A PIA can be a valuable tool to help identify what needs to be done to ensure a project’s compliance with privacy legislation”

Key questions to be answered through analysis phase of the PIA:

Q#1 “Does the project comply with privacy legislation and agency-specific legislative requirements?”
A PIA is:

“...an assessment tool that describes the personal information flows in a project, and analyses the possible privacy impacts that those flows, and the project as a whole, may have on the privacy of individuals

– it ‘tells the story’ of the project from a privacy perspective.

The purpose of doing a PIA is to identify and recommend options for managing, minimising or eradicating privacy impacts.”

[PIA 2006]
## PIA - international

<table>
<thead>
<tr>
<th>Country</th>
<th>Title</th>
<th>Authority</th>
<th>Web reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>UK</td>
<td>Privacy Impact Assessment</td>
<td>Information Commissioners Office</td>
<td><a href="http://www.ico.gov.uk">www.ico.gov.uk</a></td>
</tr>
<tr>
<td>NZ</td>
<td>Privacy Impact Assessment</td>
<td>Privacy Commissioner</td>
<td><a href="http://www.ahrq.gov">www.ahrq.gov</a></td>
</tr>
</tbody>
</table>
Undertaking a Privacy Impact Analysis involves several stages requiring user involvement:

1. **Scoping**
2. **Document Mapping**
3. **Mapping Information Flows**
4. **Legal Compliance Check**
5. **Risk Analysis**
Handling complexity – Australian Health Privacy Map can help demystify the complex legislative framework

www.healthprivacy.com.au
Handling Complexity - Privacy Impact Analysis

PIA

Nature of the Project

Threshold Assessment

Mapping the Information Flows

IPPA Compliance Checklist

A) Information Privacy Principles (IPPs)

1) Manner and purpose of collection

2) Solicitation of personal information from the individual concerned

3) Nature and method of personal information solicited

4) Storage and security of personal information

5) Information related to records

6) Access

7) Alteration of records

8) Record-keeper's obligation to check accuracy etc.

9) Use only for relevant purposes

10) Limits on use for other purposes

11) Disclosure

B) Commonwealth Contracts

1) Identifiers

2) Anonymity

3) Transborder data flows

4) Sensitive information

Privacy Impact Analysis

Privacy Management

Better Life ICT © 2008
Detail of PIA

A) Information Privacy Principles (IPPs)

1) IPP 1 – Manner and purpose of collection
   
   1) Is the personal information to be solicited by the collector from the individual concerned

2) IPP 2 - Solicitation of personal information from the individual concerned
   
   2) Will “reasonable steps” be taken to inform the individual of the purpose of the collection

3) IPP 3 - Nature and method of personal information solicited
   
   3) If the collection is to be “authorised” or “required” by law, will the individual be so advised?

4) IPP 4 - Storage and security of personal information
   
   4) Will the individual be advised about the “usual disclosures”? 
What does a PIA in Healthcare protect?

- depends on the values of the organisation
- consider question 2 of IPP 1 on the PIA checklist: ‘Will the information collected be “necessary for” or “directly related to” that purpose?’
- OR question 2 of IPP 2: ‘Will “reasonable steps” be taken to inform the individual of the purpose of the collection?’

‘reasonable steps’ allows for interpretation
- ALRC propose that the Privacy Commissioner provides guidance about the meaning of ‘reasonable steps’.
ALRC Privacy Review Timetable

- 31 January 2006: Release of formal Terms of Reference
- January 2006-April 2007: community consultations and release of Issues Papers 31 and 32
- September 2007: Release of Discussion Paper 72
- Final report #108 (Dated May 08) released at Privacy Awareness week 24 Aug.
- ? New Federal Law ?
Health Informatics Society of Australia - Submission

Key Points of Concern

- 1) National Consistency
- 2) Capabilities of Human Research Ethics Committee (HREC)
- 3) Wider Stakeholder Involvement
- 4) Maintaining Technology Neutrality
- 5) Towards ‘User-Centric’ Health Provision
- 6) Pragmatic Approaches to Consent Issues
- 7) Recognition of National and Globalisation trends with Health Data
- 8) Support for Clinical Audit and Quality Assurance

http://www.hisa.org.au/hips
Conclusions

• Get **staff** that understand the **views of all the stakeholders**
• Minimise your **risks** with **comprehensive tools and guides**
• Don’t show **fear** of complex yet fundamental problems by assigning them to the ‘too hard box’
• **Educate** everyone to **talk the same language**
• Have a **vision** that incorporates both current and future policies, legislation and community expectations
• Complex problems need breaking down, i.e. apply Occam’s Razor = ‘don’t make things more complicated than they need to be’

…. then you are ready to engage ‘the person in the centre’
Want to find out more?

• Come and see me on exhibition Stand #8
  - ‘Better Life ICT’

Peter Croll