



Dr. Peter R. Croll

Director: Health Informatics
Society of Australia (HISA Ltd)

Director: International
Association of Privacy
Professions (iappANZ)

Owner: Better Life ICT

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.

Healthcare IT News
THE NEWS SOURCE FOR HEALTHCARE INFORMATION TECHNOLOGY

CDT launches new project to tackle PHR privacy issues
By Andy Merri, Associate Editor | 03/11/08

WASHINGTON - The Center for Democracy & Technology has launched a project on health policy and information technology in collaboration with the Health Privacy Project.

CDT's Health Privacy Project will take on key privacy questions, including the proper role of notice and consent, the right of patients to access their own health records in electronic format, identification and authentication, secondary uses and enforcement mechanisms.

STORY CONTINUES BELOW

CDW Healthcare.
Better technology for better patient care.

HHS.gov
Improving the health, safety and well-being of America

Health Information Technology

American Health Information Community

The American Health Information Community (AHIC) is a federal advisory body, chartered in 2005 to make recommendations to the Secretary of the U.S. Department of Health and Human Services on how to accelerate the development and adoption of health information technology. AHIC was formed by the Secretary to help advance efforts to achieve President Bush's goal for most Americans to have access to secure electronic health records by 2014.

Plans are now underway to establish a successor to the AHIC as a public-private partnership based in the private sector by Fall 2008. The AHIC successor will be independent and sustainable and will bring together the best attributes and resources of public and private entities. This new public-private partnership will develop a unified approach to realize an effective, interoperable nationwide health information system that supports the health and well-being of the people of this country. For more information, please visit the [AHIC Successor](#) page.

Since its formation, the AHIC identified four initial areas with potential for early breakthroughs in the advancement of standards that will lead to interoperability. The AHIC organized four workgroups to pursue recommendations in these areas, and delivered their first set of recommendations to the Secretary in May of 2006. Three additional workgroups have since been formed to address a wider range of issues, and these workgroups are expected to deliver recommendations to the Secretary in 2007.

Learn more about:

- [Breakthrough areas](#)
- [Workgroups](#)
- [Revised AHIC Charter - February 2006 \(PDF - 341K\)](#)

NHIN Opportunity
Accepting Proposals from
Proposals due March 17, 2008

Section 3.2.1 of the Notice entitled "Submission Date and Times" has been changed as follows:

The receipt of applications is extended to 5:00PM EDT on March 24, 2008.

Review of applications will begin on March 24, 2008.

Target date for award is on or about March 31, 2008.

[Full Notice of Funding Availability Here](#)

National Health IT Summit: A Washington - Texas Dialogue
April 15 & 16, 2008
Houston, Texas
Registration Here:
<http://www.nhst.org>

Upcoming Events
ATA 2008

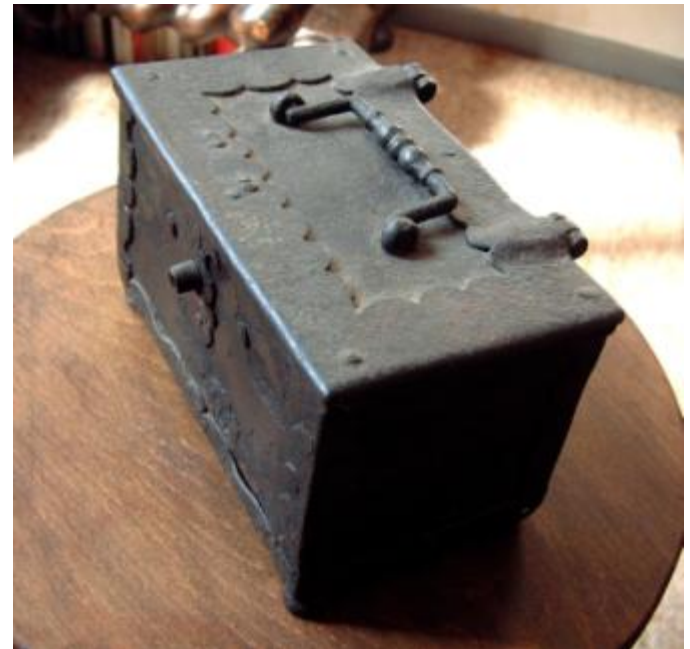
"The developers of a successor to the federal advisory panel on healthcare IT are being told by stakeholders that privacy should be a top concern,"

"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

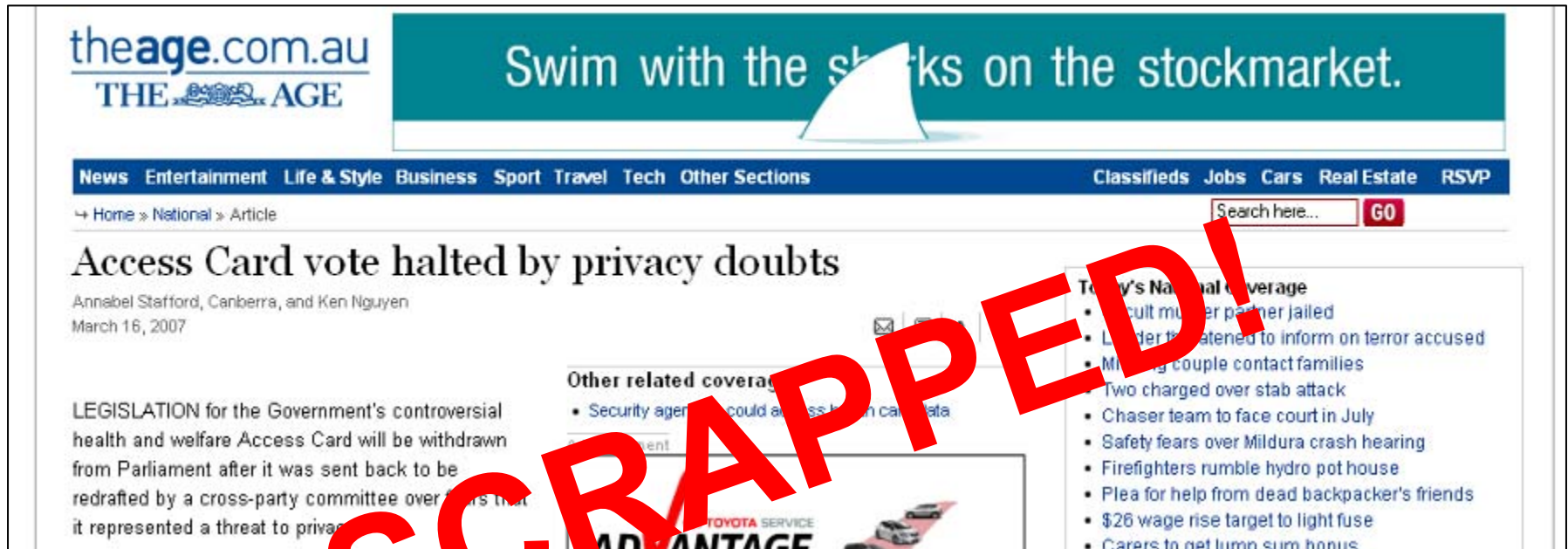


The screenshot shows the Daily Mail website interface. At the top, the masthead reads "Daily Mail" with "24 HOURS A DAY" underneath. To the right, there's a small banner for "MADONNA IS AT IT AGAIN" with a link to "The Material Girl po but a wrestling belt leotard ...more". Below the masthead, navigation links include "« Back to home", "Login »", and "Register »". The date "17 March 2008" is displayed in the top right corner. A sidebar on the left lists "Main sections" with a dropdown menu, and a list of links: "News", "News headlines", "World news", "City news", "Mail comment", "Benedict Brogan", "Peter Hitchens", "Photos & video", "Mac cartoons", "Joe Martin", "News alerts", "E-editions", and "Message boards". The main content area features a headline "Dodgy data: Millions put at risk from faulty Government ID records" by James Slack, dated 13th March 2008. The article text states: "Millions of Britons face having their lives made a 'miser' by mistakes on Government databases, it was claimed last night. Experts warned these errors could even put lives at risk by leading to inappropriate medical treatment. Research by IT specialists found 4 per cent of the population - almost two million people - had discovered incorrect information stored under their name by Whitehall or local authorities. The total climbs even higher when partial or incomplete information is included. The British Computer Society said this left". To the right of the article is a photograph of a man working at a computer. Below the article, there's a "TODAY'S POLL" section with a small image and the text "Was David Cameron right to let TV cameras film his family at".

‘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.

... then the Australia's \$1 Billion+ Health & Social Services Access 'Smart' Card







“(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

Article from: PerthNow

Font size:  Email article:  Print article:  Submit comment: 

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.



PRIVACY BREACH: Confidential patient details are being left on computers dumped by Royal Perth Hospital.


We could (should) do better


NEWS


Article from: **ABC NEWS**

'Hacker shuts down government computers'


BY PHOEBE STEWART May 16, 2008 07:10am

Email article 

Share article 

Printer friendly 

Text size A⁻ A⁺



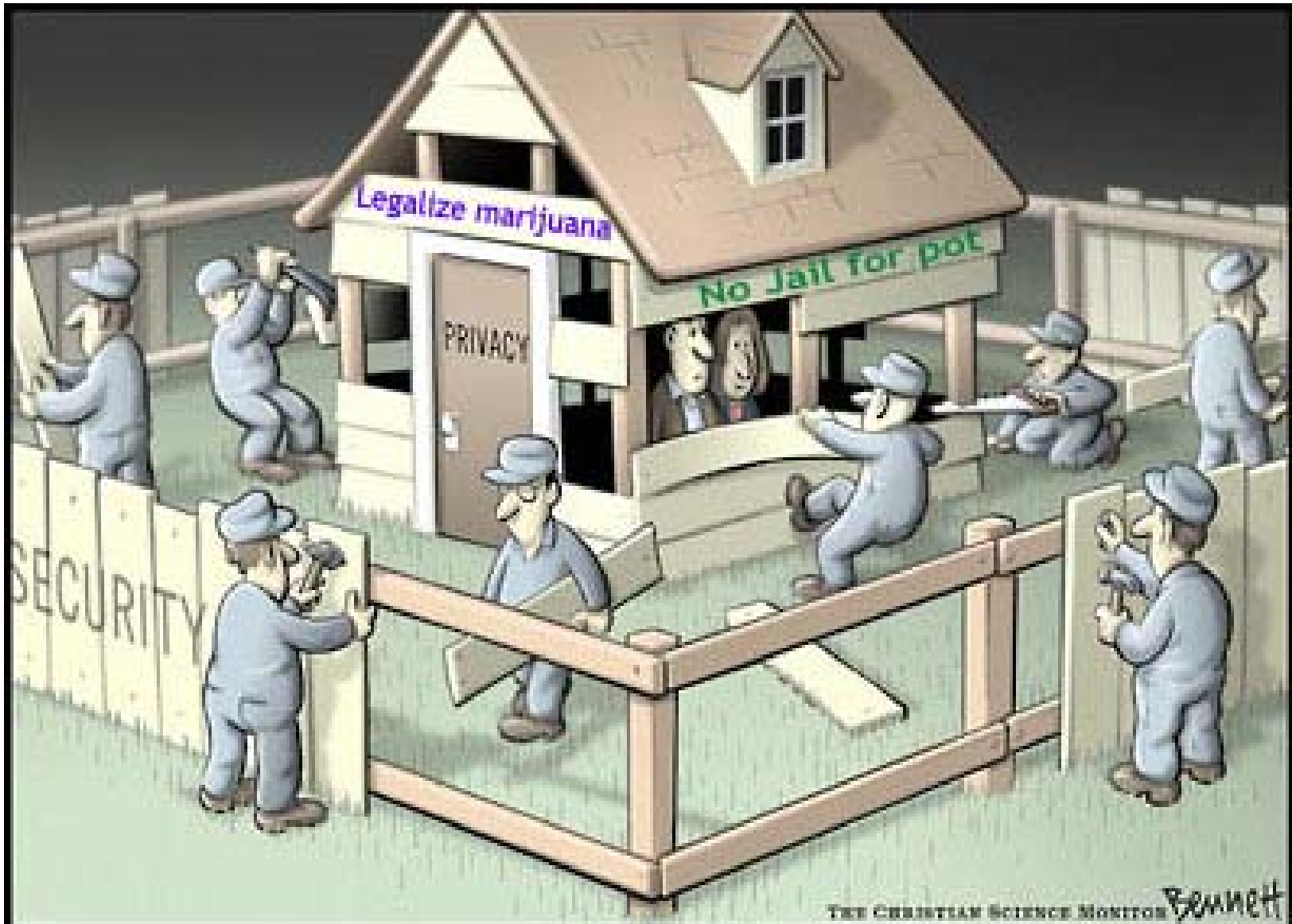
▲ Royal Darwin Hospital ... a hacker allegedly took down servers for hospitals, a prison and a supreme court / Amy Brabin

- ▣ Hacker allegedly shut down hospital and prison computers
- ▣ Northern Territory Government still working to restore data
- ▣ [Technology: Read more news and reviews in our tech section »](#)

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

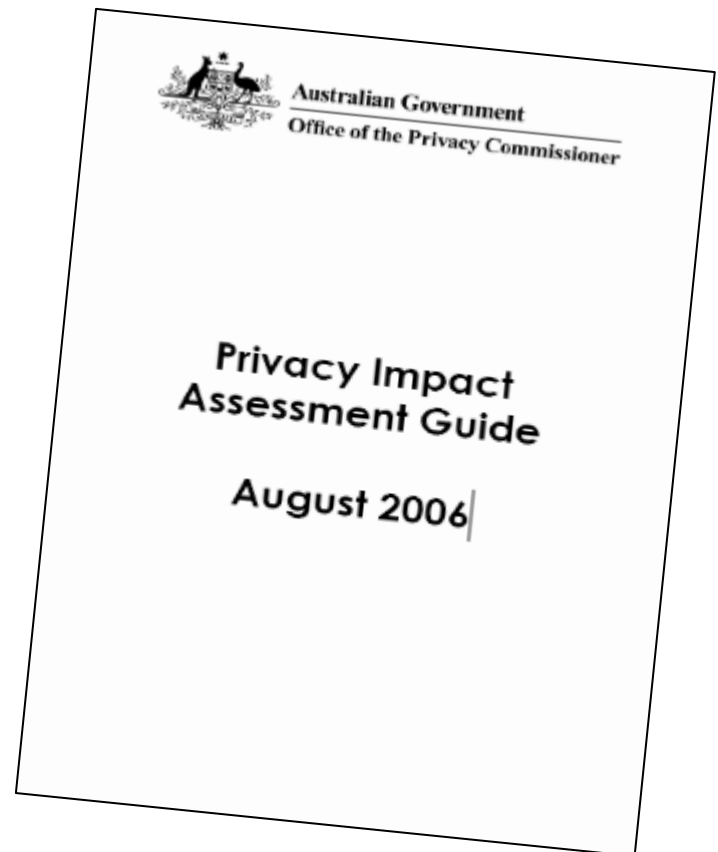


Privacy Impact Assessment (Australia)

- “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.

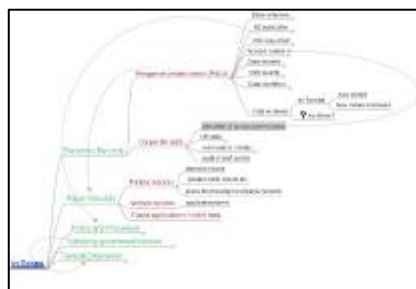
The purpose of doing a PIA is to identify and recommend options for managing, minimising or eradicating privacy impacts.”

[PIA 2006]

PIA - international

Country	Title	Authority	Web reference
UK	Privacy Impact Assessment	Information Commissioners Office	www.ico.gov.uk
NZ	Privacy Impact Assessment	Privacy Commissioner	www.ahrq.gov
US	Privacy Impact Assessments Official Guidance	Department of Homeland Security	www.dhs.gov
US	Privacy and Security Solutions for Interoperable Health Information Exchange – Impact Analysis	Office of the National Coordinator	www.ahrq.gov
AU	Privacy Impact Assessment Guide	Office of the Privacy Commissioner	www.privacy.gov.au

Undertaking a Privacy Impact Analysis involves several stages requiring user involvement



Scoping



Document Mapping



Mapping Information Flows

Risk	Likelihood	Impact	Risk Level	Mitigation Strategy
Staff working on the project will be in a position to access the data for the project	Possible (2)	Minor (1)	Low	Strengthen internal security and ensure that data is only accessible to those who need it
Staff working on the project will be in a position to access the data for the project	Possible (2)	Minor (1)	Low	Strengthen internal security and ensure that data is only accessible to those who need it
Staff working on the project will be in a position to access the data for the project	Possible (2)	Minor (1)	Low	Strengthen internal security and ensure that data is only accessible to those who need it
Staff working on the project will be in a position to access the data for the project	Possible (2)	Minor (1)	Low	Strengthen internal security and ensure that data is only accessible to those who need it
Staff working on the project will be in a position to access the data for the project	Possible (2)	Minor (1)	Low	Strengthen internal security and ensure that data is only accessible to those who need it
Staff working on the project will be in a position to access the data for the project	Possible (2)	Minor (1)	Low	Strengthen internal security and ensure that data is only accessible to those who need it
Staff working on the project will be in a position to access the data for the project	Possible (2)	Minor (1)	Low	Strengthen internal security and ensure that data is only accessible to those who need it
Staff working on the project will be in a position to access the data for the project	Possible (2)	Minor (1)	Low	Strengthen internal security and ensure that data is only accessible to those who need it
Staff working on the project will be in a position to access the data for the project	Possible (2)	Minor (1)	Low	Strengthen internal security and ensure that data is only accessible to those who need it
Staff working on the project will be in a position to access the data for the project	Possible (2)	Minor (1)	Low	Strengthen internal security and ensure that data is only accessible to those who need it

Recommendations

Likelihood	Rare (1)	Unlikely (2)	Possible (3)	Likely (4)	Almost Certain (5)
Impact					
Catastrophic (5)	5	10	15	20	25
Major (4)	4	8	12	16	20
Moderate (3)	3	6	9	12	15
Minor (2)	2	4	6	8	10
Insignificant (1)	1	2	3	4	5

Risk	Required Actions
High Risk	Significant Risk— Immediate treatment required, i.e. should be addressed as soon as practicable
Medium Risk	Moderate Risk— Treatment required as medium priority, i.e. should be addressed within the next few months
Low Risk	Accepted Risk— May be by specific monitoring or response procedures, i.e. policies and procedures should be in place within a year
Negligible Risk	Rejected Risk— No special action is required, i.e. remains at this level

Legal Compliance Check

Article	Health Privacy Principles	Health Privacy Legislation	Regulation
1(1)	Health Privacy Principle 1: Access to Health Information	Health Privacy Act 2000 (HPIA)	Health Privacy Commission
2(1)	Health Privacy Principle 2: Accuracy of Health Information	Health Privacy Act 2000 (HPIA)	Health Privacy Commission
3(1)	Health Privacy Principle 3: Security of Health Information	Health Privacy Act 2000 (HPIA)	Health Privacy Commission
4(1)	Health Privacy Principle 4: Openness of Health Information	Health Privacy Act 2000 (HPIA)	Health Privacy Commission
5(1)	Health Privacy Principle 5: Control of Health Information	Health Privacy Act 2000 (HPIA)	Health Privacy Commission
6(1)	Health Privacy Principle 6: Access to Health Information	Health Privacy Act 2000 (HPIA)	Health Privacy Commission
7(1)	Health Privacy Principle 7: Accuracy of Health Information	Health Privacy Act 2000 (HPIA)	Health Privacy Commission
8(1)	Health Privacy Principle 8: Security of Health Information	Health Privacy Act 2000 (HPIA)	Health Privacy Commission
9(1)	Health Privacy Principle 9: Openness of Health Information	Health Privacy Act 2000 (HPIA)	Health Privacy Commission
10(1)	Health Privacy Principle 10: Control of Health Information	Health Privacy Act 2000 (HPIA)	Health Privacy Commission

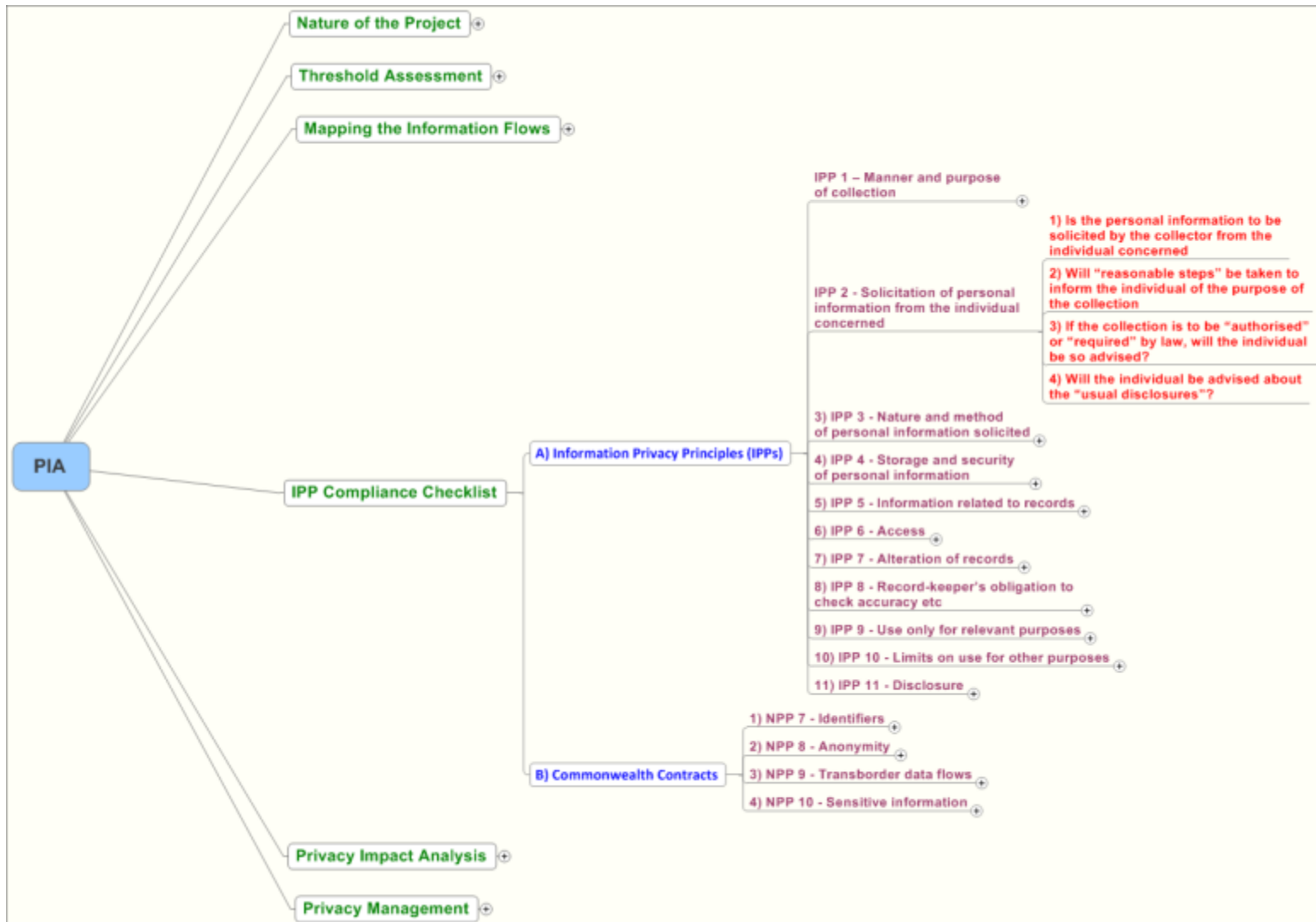
Risk Analysis

Handling complexity – Australian Health Privacy Map can help demystify the complex legislative framework

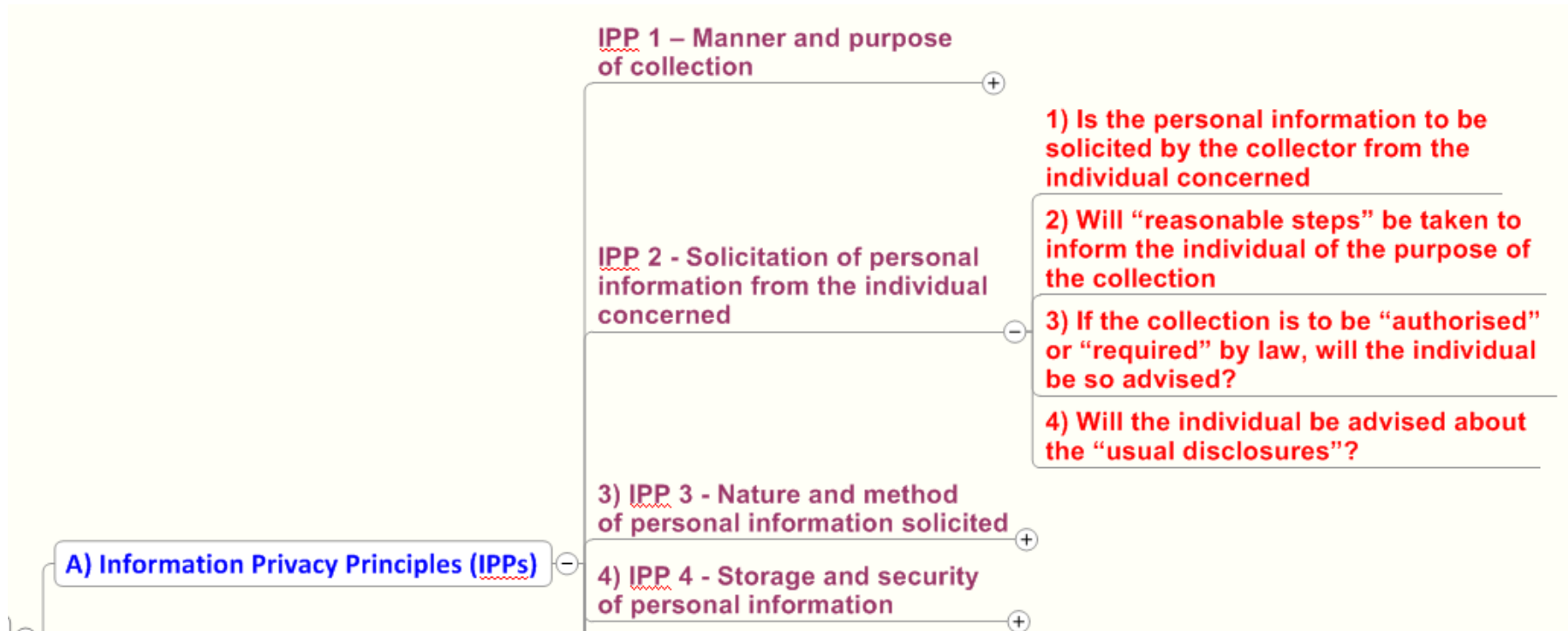


www.healthprivacy.com.au

Handling Complexity - Privacy Impact Analysis



Detail of PIA



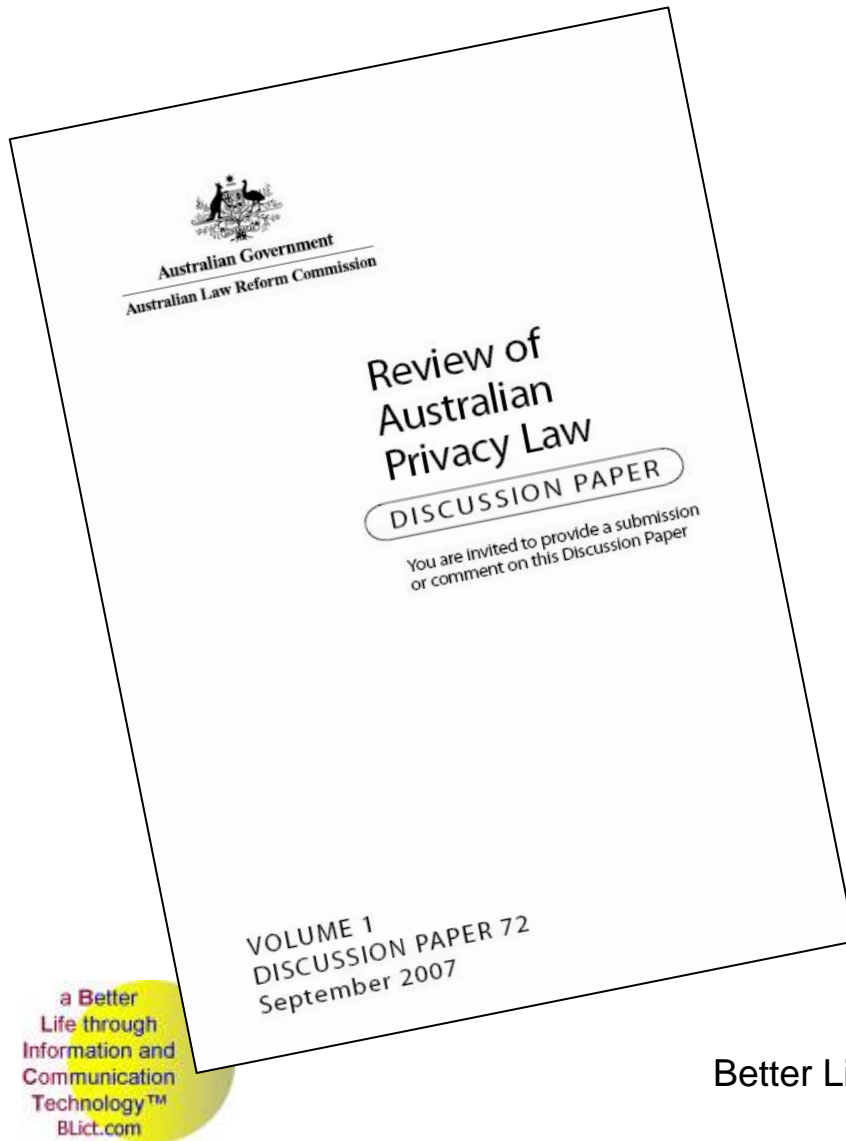
What does a PIA in Healthcare protect?

- 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

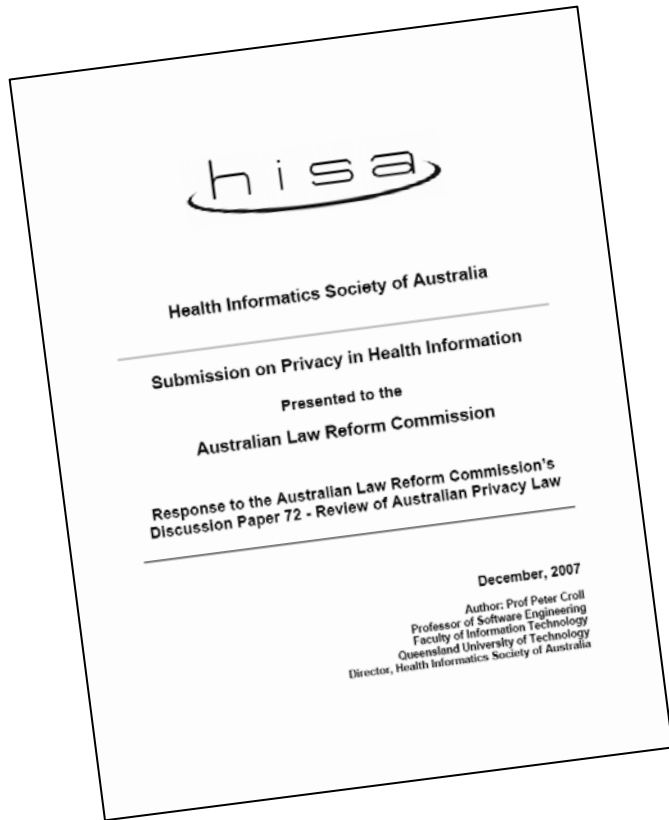
- ALRC propose that the Privacy Commissioner provides guidance about the meaning of ‘reasonable steps’.

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**

HIPS
HISA Privacy in Health

<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