

Undertaking a Privacy Impact Assessment

A discussion paper by:

Dr Peter R Croll

Chair of HIPS, HISA's Privacy in Health Forum

Director, Health Informatics Society of Australia (HISA Ltd.)

Director, International Association of Privacy Professionals (iappANZ)

Owner, Better Life ICT (www.bliect.com)

Overview:

In Australia, the Federal government's Office of the Privacy Commissioner (OPC) specifies guidelines for undertaking a Privacy Impact Assessment (PIA). These guidelines spell out the necessary steps to help an organisation determine if they are sufficiently compliant with current privacy legislation and help an organisation determine if they are following their vision and values.

Privacy is often cited as a key determining factor regarding the acceptance of electronic health records. Certainly, the current trust that exists between a clinician and a client can be damaged by a breach of confidentiality or privacy. The growing international evidence of security breaches and media loss with health data is beginning to fuel patient's reservations with electronic data storage. Furthermore, today's patients are seeking more control over who should be able to see their private and sensitive health data. As a result, a number of proposed health projects are advocating an 'opt-in' approach to address these concerns, for example, NEHTA's Individual Electronic Health Record (IEHR) where *"the option to choose which providers may access individual health information (on an opt-in basis) is seen as the key underlying factor to the success of the IEHR"* [NEHTA 2008].

When it comes to breaches, it is difficult to know the true situation. In the USA you will find legislation making breach notification a compulsory requirement and sites dedicated to collating such reports (e.g. www.phiprivacy.net, www.infosecurityanalysis.com). Whereas in Australia, the OPC has only recently published breach notification guidelines and these are subject to interpretation as to whether a breach might result in "real risk of serious harm" [OPC 2008]. Many privacy breaches are unauthorised 'internal' access by staff and not a result of someone external to the organisation hacking in. Both the ATO and Centrelink in Australia have, through their own internal audits, uncovered such widespread inappropriate internal practices resulting in over 100 staff being either dismissed or resigning, e.g. [ABC 2006].

In recognition of the need to incorporate the advances in technology the federal Privacy Laws, *Privacy Act, 1988 (Cth)* are currently under review. The Australian Law Reform Commission on the proposed Privacy Law changes has now been tabled in Parliament [ALRC 2008]. In August 2008, Senator John Faulkner stated that legislation for the first stages of the Privacy law reform will be 12-18 months. He said that Health will be considered as part of the first stage *"as these issues interact directly with the recommendations on the UPPs (the proposed Unified Privacy Principals) as well as having been identified as priority issues by stakeholders and agencies."* Furthermore, he stated that:

"Dealing with them at an early stage is also consistent with COAG's current agenda on health and consumer credit reform."

Much of the Health related aspects in the Privacy law review depend on the creation of new "Privacy (Health Information) Regulations" by the Privacy Commissioner. These proposals were made prior to the recent economic downturn and it's still too early to know if the global financial crisis will result in any delay to these plans.

Professionals in health IT will need to be familiar with the proposed changes but be aware that conformance to the current laws is still needed for the foreseeable future.

Privacy Impact Assessments (PIA):

A PIA is a tool that can help determine if an organisation or agents are following their vision and values, can reduce the risk of not meeting their contractual and legal obligations and improve their position when, for example, tendering for new contracts. The Australian guidelines describe the PIA process as story being told about a project that will identify privacy impacts and lead onto management recommendations. The guidelines state:

"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]

The emphasis is on identifying when an organisation or government agency is collecting information that is unnecessary for the given project or whether the project will lack appropriate accountability or oversight processes. The aim is to identify, analyse and manage privacy impacts and seek out solutions that drive good privacy practice and underpin good public policy while still achieving the project's goals.

The key stages of the Australian PIA and the complexity of Health related information:

The starting point of a PIA is to broadly describe the project and then map out the 'information flows' of any personal information across an organisation. It should be noted that this is not health information specific. A PIA can, and should, be applied to any project that involves any personal information. In health there are some further concerns resulting from the highly sensitive nature of clinical information. In fact just having your registration details located at a particular healthcare provider might constitute sensitive information, e.g. mental and sexual health practices. Therefore any mapping should consider all personal information before looking at the sensitivity risks.

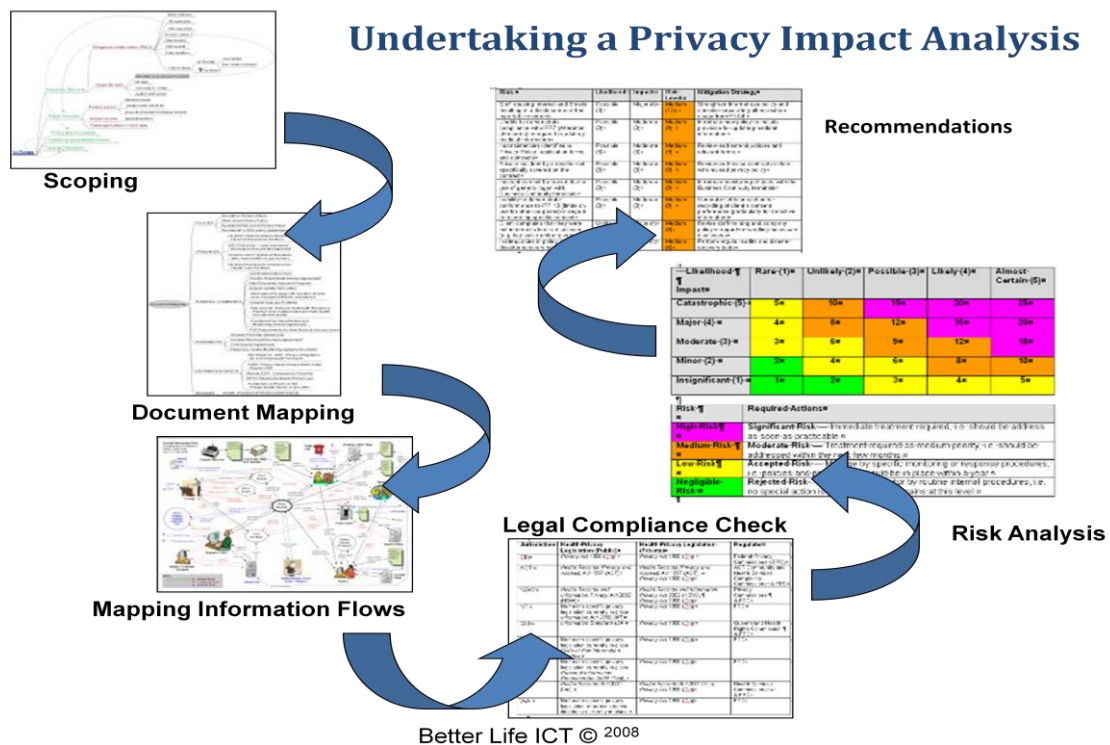
The Australian PIA guidelines provide a check list to determine compliance with each of the Privacy Principals, i.e. either the 11 Information Privacy Principals (IPPs) and/or the 10 National Privacy Principals (NPPs). This is a bit more complex with Health data since the Australian Privacy laws can differ depending on whether we are considering private or public healthcare providers and then which State they reside in. Further complexities occur with the use of this data when it crosses

borders and jurisdictions and if it will have a secondary use for medical and public health research. This topic is too complex to be adequately addressed in this discussion paper, for further details please refer to [Liu 2008, Magnusson 2004, ALRC 2007 and Croll 2006-8].

By using the checklist supplied in the PIA guidelines and creating an information flow mapping it is possible to determine the main privacy risk impacts and draw up recommendations for management. In practice this can be a non-trivial task, especially when dealing with complex organisations that have evolved their privacy principals over time and are driven by different motives to that of the community and the individuals they hold information on.

An independent analysis is the best way to determine the actual working practices within an organisation. It is also critical to get an external insight on the 'perceived risks' and a measure on how best to handle them as these can have a direct negative effect on the attitude and behaviour of your customers and clients.

The following diagram indicates the stages involved in a full analysis:



Outcome:

The Australian PIA guidelines state a number of key benefits can arise from undertaking a PIA. In brief these include:

- avoiding costly or embarrassing privacy mistakes;
- compliance with privacy laws;
- reflecting community values;
- avoiding function creep relating to privacy;
- future proof against known upcoming privacy law changes;
- ensuring stakeholders and the community are better informed;
- demonstrating that protecting personal information is important to the organisation concerned and that this has been critically evaluated.

Dr Croll's direct experience at undertaking PIA's with international organisations has led to the development of a set of software tools that streamline the process specifically for health related applications.

Contact his team at anytime for a free professional assessment of your needs:

Email: enquiry@healthprivacy.com.au or peter@blict.com

Phone: **0458 625 428** (045 TO BLICT) at any time.

References:

[ABC 2006] "Centrelink staff sacked for privacy breaches", news report ABC online (<http://www.abc.net.au/news/newsitems/200608/s1721505.htm>), Wed, Aug 23, 2006.

[ALRC 2008] "Review of the Australian Privacy Law", ALRC report 108, Australian Law Reform Commission (<http://www.austlii.edu.au/au/other/alrc/publications/reports/108/>), May 2008.

[Croll 2006a] PR Croll, Are undue Privacy concerns putting our Health Research at high risk? Privacy Law Bulletin, LexisNexis Butterworths, vol. 2, no.10, April 2006, pp139-140.

[Croll 2006b] PR Croll & J Croll, Privacy Compliance – Managing the Risks when Integrating Health Data, Health Informatics Conference Sydney, Aug. HIC 2006.

[Croll 2008a] PR Croll, Special Issue: Health Information Privacy and Security, electronic Journal of Health Informatics www.eJHI.net, Vol 3, No 1 (2008).

[Croll 2008b] PR Croll, Privacy Impact Assessments – the Organisation versus the Individual's viewpoints, Health Informatics Conference HIC'08, Melbourne 2008.

[Liu 2008] V. Liu, L. May, W. Caelli, PR. Croll, Strengthening Legal Compliance for Privacy in Electronic Health Information Systems: A Review and Analysis, electronic Journal of Health Informatics, 2008; 3(1): e3.

[Magnusson 2004] Roger Magnusson, 'The changing legal and conceptual shape of health care privacy' (2004) 32 Journal of Law, Medicine & Ethics 680-691.

[NEHTA 2008] Privacy Blueprint for the Individual Electronic Health Record - Report on Feedback, Nation E-Health Transition Authority (www.nehta.gov.au), Nov 2008.

[OPC 2008] Guide to handling personal information security breaches, Office of the Privacy Commissioner (http://www.privacy.gov.au/publications/breach_guide.html), Aug 2008

[PIA 2006] Privacy Impact Assessment, Australian Gov., Office Privacy Commissioner (www.privacy.gov.au), Aug 2006.