

# Privacy Impact Assessments – the Organisational versus the Individual's viewpoints

Croll, P

*Better Life ICT, Brisbane*

## Abstract

In Australia the Federal government's Office of the Privacy Commissioner 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. This paper is based on the author's experience of undertaking PIAs and considers if they are suited to the complex needs found within healthcare service organisations. It will be demonstrated that they suit an organisational viewpoint as is the case with many risk assessments sponsored by management. It will show that the individual's view point is crucial and this can too easily be overlooked to the detriment effect of the project concerned. Discussion regarding further research is included about extending the standard questions beyond the privacy principles to include best working practice of international standards together with a more people-centric view to minimise the real risks resulting from inadequate organisational policies and procedures.

## Introduction:

The need for confidentiality with a patient's personal data can be traced back over 2000 years to the 'Hippocratic Oath'. Translated from the original Greek the excerpt on confidentiality reads: "Whatever, in connection with my professional service, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret." [Harvard 1910]. Physicians encapsulate these values by ensuring that discussion about an individual's conditions be confined within a practice or department for the primary purpose of helping the patient concerned. Any secondary use that could advance medical knowledge would not normally identify the individual concerned unless they had consented.

The more recent advancement of digital technology and e-health is providing a revolution in both medical know-how and healthcare provision. But with this advance the traditional boundaries are being breached. The concept of confining information in written form to a physical location, such as a surgery, is gradually disappearing. The remote and high speed access that today's digital technology brings presents new challenges and not only with healthcare providers but for governments, the ICT industries, lawyers and individuals alike. The individuals as patients have a right to privacy over any personal and sensitive health data. They traditionally would talk to a doctor in confidence and assume that the associated healthcare organisation would be able to adequately protect their privacy. The knowledge required to keep a contemporary computer system secure is extensive and often beyond that of the healthcare practitioner especially with personal computers that were not specifically designed with security in mind. A number of guidelines and standards are issued to assist in security and privacy. This paper considers the efficacy of the Privacy Impact Assessment [PIA 2006] in its application to healthcare service organisations. To appreciate the complexities and subtleties of the subject, IT Privacy is first introduced, then the international perspective is reviewed before the PIA process is analysed. This paper evaluates the most serious shortcomings from a contemporary Health Informatics viewpoint and proposes the need for further study to facilitate a more people-centric view.

To appreciate the difference between privacy and security consider an exhibition that is displaying valuable antiques. The display cabinets can be made of reinforced glass and well secured. The contents are intentionally visible for all to see but kept locked to prevent anyone from stealing them. Now with an IT system such stealing might involve using a memory stick or even an iPod to remove data. This could also be achieved remotely via the internet or other network connections. A range of security measures can be employed to prevent unauthorised copying of information, e.g., firewalls, smartcards or one of a number of password protected access control mechanisms [Liu et al 2007]. A privacy violation might not involve copying and stealing data but simply viewing it as in the case of the exhibition display cabinets. To view private information either on a screen or because your account access rights permit it may well be improper. This is more likely to occur internally within an organisation due to the IT security measure put in place but need not be the case if the system is configured to allow remote viewing. One of the main problems facing organisations is determining what constitutes an unauthorised person viewing a record and how to handle this in a pragmatic manner? Because of the way contemporary systems are configured some people have wide ranging access rights. In Australia we have seen this problem emerge with the Tax Office and Centrelink [ABC 2006]. From a medical view point, personal data should only be viewable on a 'need-to-know' basis. That is, the individuals concerned should be part of a case file, or they have given consent permission to look at their information, or their life is in danger, or access has legal authority. Consent is a complex and often emotive issue. It is not always clear-cut that permission may have been granted for general access within a healthcare organisation and, furthermore, each organisation and even divisions within the same health authority, develop and use their own consent forms. The legal standing of these forms again is unclear and one of the reasons why the Health Informatics Society of Australia (HISA) has recommended changes in their submission ([www.hisa.org.au/hips](http://www.hisa.org.au/hips)) to the Australian Privacy Law Reform Commission in response to their discussion paper [ALRC 2007].

## **Health Privacy - International Perspective:**

The International Medical Informatics Association's (IMIA) working party 4 (Security) is progressing towards standardising some of the best practice approaches for minimising risks with privacy and security. We have a long way to go before any international unification in this area. For example, some whole regions have little or not data protection at all such as the six Middle Eastern GCC countries that have nothing in place to protect their health records. Countries that lead in Privacy regulations have a range of extensive legislative requirements, for example the ECC countries, Canada, NZ and the US, yet their approach can be distinctly different. Prof. James Whitman maintains that: "American privacy laws is a body caught in the orbit of liberty values, while European law is caught in the orbit of dignity" [Whitman 2004]. Although these laws appear to approach each other they are pulled in different directions and result in "legal orders that do meaningfully differ". To appreciate this in practice it is interesting to see the emergence of the recent Californian legislation 'AB1298' [Jones 2007]. This Assembly Bill ensures an organisation is legally bound to notify the individual resulting from any health privacy disclosure. That can include an individual's health insurance ID number and follows along the lines of credit card number disclosures. Note how this differs from the recent case in Perth where the WA Health Minister was claiming that the personal information obtained from a rubbish skip and then subsequently revealed by the Sunday Times newspaper amounted to "stealing the computers and hacking into their contents" [S.Times 2008]. The implication is that the Sunday Times acted illegally and hence in an undignified way to the individuals concerned. The blame was on the organisation that revealed the information. No legal requirement was on the organisation holding the information to protect the liberty of the individuals concerned by informing them of this breach.

With all these differing legislative regulations and guidelines across countries and with different perspectives on how to protect sensitive information, are there any common grounds? In fact, many of the leading countries do adopt a similar approach although the outcomes may differ to suit the local legislation. Guidelines on reducing the risk of privacy violations through the application of a Privacy Impact Assessments are available in several countries as shown in the following table:

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

### **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:

“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 Australian guide follows the other countries in stating a number of key benefits that 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 this has been critically evaluated.

### **The key stages of the Australian PIA and how they relate to Health ICT:**

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 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 which State they reside in. Further complexities occur with the use of this data across 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 paper and has been well address before [Liu 2008, Magnusson 2004, ALRC 2007, Croll 2006].

From the checklist and information flow mapping it is possible to determine the main privacy risk impacts and draw up recommendations for management. Of course this is a very simplistic view. In practice you are normally 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. So what is it that the PIA actually protects? Is this adequate for contemporary healthcare providers and the shift towards patient-centric views that are now increasingly being advocated?

### **What does a PIA in Healthcare protect?:**

The key question is: 'does a PIA protect the privacy of the individual or protect the organisation concerned?' From experience of undertaking PIAs with public and private organisations, it very much depends on the values of the organisation. If they are looking for a check on their legal compliance to satisfy their board of directors and lawyers then it may focus on the areas of non-compliance. The broader benefits of satisfying the expectations of external contractors and reassuring the community at large, requires more emphasis on the view point of the individual. For example, consider question 2 of IPP 1 on the PIA checklist: 'Will the information collected be "necessary for" or "directly related to" that purpose?' An organisation looking to protect themselves will justify the reasons for collecting information even if from the individual's viewpoint it is only loosely related. Now consider question 2 of IPP 2: 'Will "reasonable steps" be taken to inform the individual of the purpose of the collection?' Again, 'reasonable steps' allows for interpretation. Taken from an individual's perspective they might expect to be told about the purpose of collecting the information when initially asked and also see this in print. From an organisational view providing a web reference where this can be found in the small print might be considered reasonable for them. In fact 'reasonable steps' appear in many questions in addition to 'reasonable technical security' and 'reasonable physical security'. This introduces a cost / benefit analysis associated with any risk management decision making process. The questions are not framed as 'would the majority of individuals concerned consider this to be "reasonable steps"?' There is some emphasis on ensuring the organisation is putting in place procedure to help determine if the individual would have thought that to be reasonable. For example IPP 10 check list question 2 'Will processes be put in place to make individuals aware of the usual disclosures and to assist the record-keeper determine whether the individual was "reasonably likely to have been aware" of such disclosures?' But again the mechanism for determining this rests with the organisation's interpretation. They are responsible for determining what would constitute an appropriate quality process for finding out about what is considered 'reasonably likely' with individuals. Hence, the ALRC are proposing (proposal 25-3) [ALRC 2007] that the Privacy Commissioner provides guidance about the meaning of the term 'reasonable steps'.

It is necessary to implement a robust IT security system that will ensure the information is privacy protected adequately from outsiders. What constitutes a robust system is again left to interpretation. The Australian Privacy Law 1988 (Cth) only expects 'reasonable steps' to be made which is why the ALRC are recommending that the Privacy Commissioner determines which privacy and security standards for relevant technologies are mandated by legislative instrument [ALRC 2007]. There are many international standards that can be applied, e.g. [AS17799 2006] plus many new Health IT related standards are under development by the 'Health Informatics' ISO Technical Committee 215 ([www.isotc.iso.org](http://www.isotc.iso.org)).

### **Evaluation and Conclusions:**

In practice, the risk of not embracing the individual's concerns can be catastrophic. In Australia the \$1 Billion Health and Social Security Smart card was scrapped after a rough ride through Senate over Privacy concerns. Other literature indicates that Privacy concerns of individuals can both seriously delay and undermine the confidence of large health IT project roll-outs [Lui et al 2007]. Yet for evidence that this message is not getting through then consider a recent tender for a national EHR system issued by the Ministry of Health in Saudi Arabia which only mentions security and not privacy in their requirements. As it stands this does not prevent the hospitals providing all their data to health insurance companies and without the individual's knowledge or consent or providing them with any option to check the accuracy of that information. How much valuable information will be withheld by concerned individuals if this lack of protection is common practice?

Hence, putting the individual first is the only way that many of the benefits from a PIA identified above will be fully realised. The risk of ignoring people's concerns can be a real show stopper for emerging projects, especially in health. These may be real or perceived risks [Croll & Morarji 2006c] but either way they need to be addressed. In Australia, it will be some time before the new generic Privacy Act is in place and possibly much longer before the proposed health guidelines and other related standards are recommended by the Privacy Commissioner. Health Informatics is in a rapid growth phase and cannot wait for this legislation. The PIA is a valuable and essential tool to determine the privacy and associated risks with new projects. It needs to be appropriately managed to get the best result, that is, one where both the organisational concerns and the individual concerns are adequately addressed. The current guidelines are weighted towards new projects and the expectation that 'reasonable steps' will be taken by the organisations concerned. Changing these questions and introducing new consultation steps to reflect the opinion of the end users is essential to ensure a people-centric view is adopted.

## References:

- [ABC 2006] "Centrelink staff sacked for privacy breaches", news report ABC online, Wed, Aug 23, 2006.
- [ALRC 2007] "Review of the Australian Privacy Law", Discussion paper 72, Australian Law Reform Commission ([www.alrc.gov.au](http://www.alrc.gov.au)), Sept 2007.
- [AS17799 2006] AS17799:2006 – Information Technology Security Techniques – Code of practice for information security management, Standards Australia.
- [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, pp 139-140.
- [Croll 2006b] PR Croll & J Croll, Privacy Compliance – Managing the Risks when Integrating Health Data, Health Informatics Conference Sydney, Aug. HIC 2006.
- [Croll 2006c] Croll, PR. & Morarji, H. (2006) Perceived Risk: Human Factors Affecting ICT of Critical Infrastructure. Proc. The Social Implications of Inf. Security Measures on Citizens and Business, pp. 213-222
- [Harvard 1910] "Harvard Classics, Volume 38" Copyright 1910 by P.F. Collier and Son.
- [Jones 2007] Safeguarding personal information, LEGISLATIVE COUNSEL'S DIGEST AB 1298, Bill introduced by Assembly Member Jones, State Legislation California, 2007.
- [Liu 2008] V. Liu, L. May, W. Caelli, P. Croll, Strengthening Legal Compliance for Privacy in Electronic Health Information Systems: A Review and Analysis, electronic Journal of Health Informatics, 2008; 3(1): e3.
- [Lui 2007] Vicky Liu, L May, W Caelli, P Croll, A Sustainable Approach to Security and Privacy in Health Information Systems, 18th Aus Conf. on Information Systems (ACIS'07), Dec 2007, pp 225- 265.
- [Magnusson 2004] Roger Magnusson, 'The changing legal and conceptual shape of health care privacy' (2004) 32 Journal of Law, Medicine & Ethics 680-691.
- [PIA 2006] Privacy Impact Assessment, Australian Government, Office of the Privacy Commissioner ([www.privacy.gov.au](http://www.privacy.gov.au)), Aug 2006.
- [S. Times 2008] Royal Perth Hospital dump computers, patient details, Exclusive: Paul Lampathakis, Sunday Times, April 06, 2008
- [Whitman 2004] J Whitman, 'The Two Western Cultures of Privacy: Dignity v Liberty' (2004) 113 Yale Law Journal 1151, 1221.