University of Wollongong
Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

2011

Consumers, ALRC privacy principles and the 2010 Healthcare Identifiers Act

Jennifer A. Heath
University of Wollongong, jheath@uow.edu.au

Follow this and additional works at: https://ro.uow.edu.au/infopapers

 Part of the Physical Sciences and Mathematics Commons

Recommended Citation

Heath, Jennifer A.: Consumers, ALRC privacy principles and the 2010 Healthcare Identifiers Act 2011, 46.1-46.8.
https://ro.uow.edu.au/infopapers/3650

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

Consumers, ALRC privacy principles and the 2010 Healthcare Identifiers Act

Abstract

Aspects of the 2010 Healthcare Identifiers Act (HIA) are compared to the Australian Law Reform Commission (ALRC) Unified Privacy Principles. The opportunity for improved healthcare delivery through the enabling healthcare identifiers is acknowledged and discussion moves beyond such justifications to consideration of broader implications for Australian society. Law Academic Roger Magnusson's three broad, sequential conceptual shifts in health privacy provide a framework for the discussion. Lost opportunities for Australian consumers are also highlighted.

Keywords

era2015

Disciplines

Physical Sciences and Mathematics

Publication Details

Heath, J. (2011). Consumers, ALRC privacy principles and the 2010 Healthcare Identifiers Act. Telecommunications Journal of Australia, 61 (3), 46.1-46.8.

This journal article is available at Research Online: https://ro.uow.edu.au/infopapers/3650

CONSUMERS, ALRC PRIVACY PRINCIPLES AND THE 2010 HEALTHCARE IDENTIFIERS ACT

Jennifer Heath
University of Wollongong

Aspects of the 2010 Healthcare Identifiers Act (HIA) are compared to the Australian Law Reform Commission (ALRC) Unified Privacy Principles. The opportunity for improved healthcare delivery through the enabling healthcare identifiers is acknowledged and discussion moves beyond such justifications to consideration of broader implications for Australian society. Law Academic Roger Magnusson's three broad, sequential conceptual shifts in health privacy provide a framework for the discussion. Lost opportunities for Australian consumers are also highlighted.

INTRODUCTION

The introduction of electronic health records (EHR) has proven to be a challenge in Australia, as it has elsewhere in the world (Kalra 2006; Baird et al 2011; Gunter and Terry 2005; Hayrinen et al 2008; Ludwick et al 2010). Healthcare professionals strongly argue the case for EHR in terms of the benefits to both individual healthcare consumers and society as a whole. (National Electronic Health Records Taskforce 2000) An important step towards the introduction of the Australian EHR was undertaken in 2010 with the passing of the Healthcare Identifiers Act (HIA) through the Australian Parliament.

In parallel to the above developments in the health care sector the Australian Law Reform Commission (ALRC) has wrestled with the concept of privacy in the Information Age. Following extensive consultation with community members, policy and law makers the ALRC proposed a set of eleven Unified Privacy Principles (UPPs) for Australia. (ALRC 2008) The main objective was to unify and enhance the provision of the Commonwealth sector Information Privacy Principles (IPPs) and the private sector National Privacy Principles (NPPs).

The UPPs moved through consultation to become the final thirteen exposure draft Australian Privacy Principles (APPs). Health related provisions that were previously covered by IPPs and NPPs are, however, not covered by the APPs. The *Healthcare identifiers and privacy: Discussion paper on proposals for legislative support* (2009) referred to the UPPs and included them as an appendix. Table 1 provides a timeline to illustrate the parallel journey these two important national endeavours have taken over the last few years.

The release of the Exposure Australian Privacy Principles came 11 months **after** the release of the healthcare identifiers and privacy discussion paper. The Healthcare Identifiers Act was finalised in the month following release of the exposure APPs. The Australian Government is yet to release law reform proposals to deal with specific privacy protections for information relating to health. (Companion Guide to APPs 2010, 4)

As the APPs have not yet been finalised, and given that the UPPs did not aim to exclude health care provisions and they were used in the healthcare identifiers discussion paper, they are used in this paper to facilitate discussion.

Published	Document
May 2008	Australian Law Reform Commission Model Unified Privacy Principles.
July 2009	Healthcare identifiers and privacy: Discussion paper on proposals for legislative support.
June 2010	Exposure Australian Privacy Principles + Companion Guide to Australian Privacy Principles.
July 2010	Healthcare Identifiers Act 2010. Draft released for comment: in mid Dec 2009, Submissions closed: 7 Jan 2010.
Due July 2011	Senate Committee report on Exposure Australian Privacy Principles.

Table 1 - Influential documents in two parallel activities with national importance: ALRC Privacy and health sector identifiers.

In contrast to the Australian approach the US Government reserved support for a unique, national health identifier until Congress had enacted comprehensive legislation to protect consumer privacy. (Ng 2000)

This paper highlights several tension points regarding privacy in these Australian national endeavours. It moves the discussion beyond the EHR objectives to consider Magnusson's "*mother of all function creeps"* and broader societal impacts.

MAGNUSSON'S 3 CONCEPTUAL SHIFTS IN HEALTH PRIVACY

Roger Magnusson argues that the challenges to health information privacy are best understood by considering three very broad, sequential conceptual shifts from a relationship between a single clinician and a patient, to more complex scenarios with multiple clinicians (Magnusson 2004). The essential components of the health information privacy transitions perceived by Magnusson are summarised below.

CONCEPT 1: PATIENT-CENTRED HEALTH RECORDS

Clinical care is delivered by a sole practitioner who receives or generates sensitive information during the care of a patient/consumer. Information is stored on hardcopy health records. Protection of confidentiality within the bilateral doctor/patient relationship is paramount. The hardcopy nature of the health record aids in restricting access to the consumer's information. The clinician consults with the patient in the 'gatekeeper' role, seeking consent where necessary to release records for secondary purposes, meaning those purposes that do not pertain to the direct delivery of healthcare to an individual. (Safran et al. 2006)

Within this paradigm, the law focuses on offering consumers protection by imposing penalties on the doctor for unauthorised disclosure of personal information.

CONCEPT 2: MULTI-FUNCTION HEALTH DATA HOLDINGS

Clinical care is typically delivered in a "corporate" environment including hospitals, medical centres and community-based practice groups. Patient information is recorded in a centralised, shared record which can be accessed by a range of clinicians and administrators. The need for specialised and efficient care results in many team members widely accessing the individual's health record. In institutional contexts the treating physician does not broker access to patient records. There will rarely be a single 'gatekeeper' allowing access.

Within this paradigm, the focus of the law shifts from protecting confidentiality in a relationship to protecting the actual medical information.

On the shift from bilateral to multilateral confidentiality Magnusson states:

> 'The growth of computers and the revolution in information technology has made this transition inevitable. Privacy legislation goes beyond confidentiality to regulate other elements of the "information processing cycle"; namely the collection of personal information, its accuracy, security and storage; the right of the subject to access it, as well as use and disclosure' (Magnusson 2004, 683)

CONCEPT 3: TRANS-ORGANISATIONAL HEALTH DATA FLOWS

Patient health records are stored in electronic health records in a manner to facilitate national linkage and potentially more surveillance. Management of privacy extends beyond one organisation's health care environment. In Australia this includes the national health insurance scheme, Medicare, General Practitioners and Super-Clinics, prescriptions details held in the Pharmaceutical Benefits System, private health insurance organisations, public and private hospitals and allied health agencies.

The argument for electronic health records, which characterise Magnusson's third conceptual shift, is usually pitched in terms of improved health care outcomes for individuals. The benefit to the government is the way health information networks enable the monitoring and measurement of the national health system performance.

On the matter of secondary uses of medical data Magnusson is very clear. Under the initial patient-centred model the use of a patient's health information for secondary purposes can be considered extraordinary. His prediction for the future direction of secondary uses is foreboding for privacy advocates:

> 'The mother of all "function creeps", but only likely to become increasingly apparent over the next decade or so is the gradual absorption of patients' health records within a broader public health infrastructure whose goals explicitly include the protection and promotion of population health'. (Magnusson 2004, 686)

In this final trans-organisational concept Magnusson anticipates strong pressure for a surveillance architecture permitting linkages between health systems, environmental, demographic and socio-economic surveillance data – thus truly achieving the Orwellian future feared by privacy advocates. The broader, more recent research of M.G. and Katina Michael (Michael and Michael 2010) reflects on the need to carefully consider the adoption of new technologies and perhaps " ... reject its rampant application and diffusion without studied consideration as to the potential effects and consequences." The notions of Uberveillance posited by M.G. and Katina Michael resonate with the future envisioned by Magnusson.

CURRENT AUSTRALIAN POSITION

The HIA is moving Australian society towards Magnusson's third conceptual shift of Trans-Organisational Health Data Flows. Writing in 2004, Magnusson anticipated that it would take

almost a decade to see evidence of the conceptual shifts. To date discussions and justifications for creation of healthcare identifiers and EHR have largely focussed on the potential, positive aspects associated with improved health care. Adopting a broader view Magnusson draws our attention to uses beyond direct healthcare, including performance monitoring by governments. The notion of monitoring Australian health system performance is currently under debate in the *Medical Journal of Australia* (Braithwaite and Mannion 2011; Jorm and Frommer 2011). Individual and Provider Identifiers are fundamental building blocks of the information systems that provide the vast volumes of data needed for corporate and trans-organisational and national performance monitoring.

The next section of this paper compares and contrasts the Identifier Principle of the ALRC UPPs and the 2010 Healthcare Identifiers Act. This enables a multi-dimensional perspective to allow reflection on both the immediate EHR drivers and broader societal impact.

IDENTIFIERS - ALRC PRIVACY PRINCIPLES

In developing the proposed UPPs, the ALRC considered many aspects of privacy in the Australian context including: the background to privacy regulation; achieving national consistency; regulating privacy; impacts of developing technology on privacy and associated matters. ALRC Recommendation 30.3, clarifies the term 'Identifier':

> 'The 'Identifiers' principle should define 'identifier' inclusively to mean a number, symbol or biometric information that is collected for the purpose of automated biometric identification or verification that:
>
> (a) uniquely identifies or verifies the identity of an individual for the purpose of an agency's operations; or
>
> (b) is determined to be an identifier by the Privacy Commissioner'

On the issue of the Identifiers Principle the ALRC states

> 'It is not desirable for organisations to refer to individuals by an identifier that is assigned by an agency, nor is it desirable to facilitate data-matching between agencies and organisations through the use of an identifier'. (ALRC 2008, Vol2, 1029)

It is clear here that the ALRC is warning that organisations should not be allowed to adopt unique, individual identifiers that have been allocated by Government agencies. Allowing numerous organisations to adopt the same Government generated unique, individual identifier enables data from disparate organisations information systems to be readily linked. The level of individual surveillance and secondary data use that is possible with such architectures is for many members of society quite alarming – hence the ALRC strong position here.

The development of national identity numbers is not a notion endorsed in any way by the ALRC, published discussion specifically refers to preventing the creation of de facto national identifiers:

> 'The policy objectives underlying the recommended 'Identifiers' principle—preventing an identifier that is assigned by an agency from becoming a de facto national identity number, and restricting the use of an identifier to facilitate data matching programs—are also relevant to the handling of identifiers by agencies'. (ALRC 2008, 1034)

The Australian Privacy Commissioner provided a concise description of the importance of identifiers in a submission to the ALRC,

> 'The privacy risks of sharing unique identifiers are not always immediate. The risks accumulate as more organisations or agencies adopt the number for their own purposes, and as greater amounts of otherwise unrelated personal information become associated with that number. Accordingly, individuals may not always be

> conscious of the inherent risks of consenting to incrementally greater uses of their unique identifier'. (ALRC 2008, Vol2, 1047)

Moving on from the UPPs the Companion Guide to the Australian Privacy Principles (2010) provides very clear guidance on the use of identifiers issued by government agencies via *Australian Privacy Principle 9 – adoption, use or disclosure of government related identifier:*

> 'This principle is aimed at ensuring that organisations (not agencies) do not refer to individuals within their own systems according to identifiers (for example, Medicare numbers) issued by government agencies. Further, it prevents the facilitation of unlawful data-matching by organisations through use and disclosure of such identifiers.
>
> The key goal of this principle is to restrict general use of identifiers issued by government agencies and prevent such identifiers from becoming de facto national identity numbers'. (Companion Guide APPs 2010, 11)

The substantial consultation undertaken by the ALRC in the development of the Model UPPs and subsequent progress to Exposure Australian Privacy Principles indicates a real engagement with the issue of privacy in the Information Age. There is a recognition that adoption of information and communication technologies is not always in the best interests of individuals as they inevitably leave electronic footprints through their day-to-day activities. The notion of undesirable citizen surveillance is acknowledged by the ALRC and prevention of such is a clear objective throughout its three-volume report (ALRC 2008) and Exposure Australian Privacy Principle 9.

IDENTIFIERS - 2010 HEALTHCARE IDENTIFIERS ACT

The *Healthcare identifiers and privacy: Discussion paper on proposals for legislative support* was issued by the Australian Health Ministers' Advisory Council in July 2009. This paper described legislative proposals to support the creation and implementation of Australian national healthcare identifiers and associated arrangements for privacy of health information. Included in this proposal is the creation of an Individual Healthcare Identifier (IHI) for every Australian.

The Discussion Paper puts forward the case for establishment of the national healthcare identifiers with the associated Health Identifier Service expected to be operational by mid 2010. As noted in the Executive Summary to the Discussion Paper*:*

"Discussions between governments about a national privacy framework across all jurisdictions and its implementation may not be completed by that time". (Discussion Paper 2009, 3) This is a lost opportunity for consumers as a stable, well established national privacy framework would have been advantageous for consumers both now and in the future as the identifiers are more widely adopted.

The Discussion Paper stated that *"assignment of IHIs will be authorised by legislation and individual consent will not be sought".* (Discussion Paper 2009, 25) The arguments for this are sound from an information systems point of view, that is from the outset the health data management goals would be best served by a complete, valid and comprehensive set of individual identifiers. Assigning health care identifiers on a voluntary basis is rejected in the Discussion Paper as it *"...would create numerous implementation problems and complexities, placing increased burden on healthcare providers and consumers, and resulting in poor uptake".* (Discussion Paper 2009, 11) Authors of the Discussion Paper go on to state that *"Limited or inconsistent uptake will mean that many of the efficiency gains for health care providers and important quality and safety benefits for patients will not be realised."* (Discussion Paper 2009, 11)

This approach can be seen as very 'heavy-handed' and somewhat paternalistic and an 'opt-out' option for Australian consumers who did not wish to participate in the de facto national identifiers could also have been supported from a privacy-protective perspective. Arguments against the failed Australia Card are pertinent here but will not be revisited in this paper.

The Discussion Paper also explains that healthcare providers will be given approval to adopt the new Individual Healthcare Identifiers in their health information systems. This suggestion is in **direct conflict** with the ALRC policy objective, UPP 10 and APP 9 that prevents the adoption of such identifiers due to concern regarding data linkage and the future potential for surveillance. This is also in **direct conflict** with the risks raised by the Australian Privacy Commissioner, as presented above, where the issues with shared identifier use are not initially obvious but become more apparent over time with broader adoption by a growing number of organisations.

The Discussion Paper also acknowledges that this aspect of the Healthcare Identifier proposal is **at odds** with the Commonwealth Privacy Act 1988:

> 'Specific authority will be given to private sector healthcare provider organisations to adopt, use or disclose and IHI or HPI-I for health information management and communication purposes. This is to overcome a restriction in the present Commonwealth Privacy Act 1988'. (Discussion Paper 2009, 3).

The draft Exposure Healthcare Identifiers Bill was available for scrutiny and comment across the Christmas-New Year period from mid-December 2009 to 7 Jan 2010. The brief consultation across the traditional holiday period was not ideal for consumer engagement. The 2010 Healthcare Identifiers Act was enacted in July 2010 with all Australians allocated a 16 digit unique identifier.

Within the HIA, *Division 3 Section 25 Adoption by healthcare,* authorises healthcare providers to use the national identifier within their own information systems:

> 25 Adoption by healthcare provider
>
> A healthcare provider is authorised to adopt the healthcare identifier of a healthcare recipient (including a healthcare identifier disclosed to the healthcare provider for any purpose under section 24) as the healthcare provider's own identifier of the healthcare recipient.

Using this de facto national identifier as a possible primary key or foreign key within healthcare provider's disparate information systems could at a later date readily facilitate data linkage and surveillance. The impact of this on future Australian society is alarming yet this legislation has passed fairly quietly through Federal Parliament.

There is a note in the legislation attached to this section that states that this approval only relates to the identifier not the associated consumer personal health information. The associated health information is to be dealt with by 'other' legislation including the *Privacy Act 1988*. When using information technology it is the identifier that is needed for linkage and it is somewhat inadequate to refer back to the *Privacy Act 1988* seeking protection for the remainder of the held personal information. Australian researchers have recently noted the complexity in navigating privacy legislation (O'Keefe and Connolly 2010) and this splitting of the individual healthcare identifier and the associated medical information between two (or more) Acts may not assist.

As Magnusson foreshadowed in Concept 3, the gradual absorption of individual's health records within a broader public health infrastructure is evident in the HIA. Specifically, *Section 24 Use and disclosure for other purposes* authorises release of health identifiers for a range of secondary purposes including but not limited to: management, funding, monitoring or evaluation of healthcare; provision of indemnity cover for a healthcare provider; conduct of research that has been approved by a Human Research Ethics Committee and to lessen or prevent serious threats to public health. Clearly the healthcare identifiers alone would be insufficient to facilitate such secondary uses and the associated personal and medical data is also required.

Within *Section 24* the HIA is strengthened by the inclusion of four excluded secondary uses:

> Certain purposes excluded

This section does not authorise the use or disclosure of the healthcare identifier of a healthcare recipient for the purpose of communicating or managing health information as part of:

(a) underwriting a contract of insurance that covers the healthcare recipient; or

(b) determining whether to enter into a contract of insurance that covers the healthcare recipient (whether alone or as a member of a class); or

(c) determining whether a contract of insurance covers the healthcare recipient in relation to a particular event; or

(d) employing the healthcare recipient.

The exclusion of these secondary purposes reflects Australian consumers concerns regarding secondary use of medical data by insurance organisations and employers as gathered by a pilot consumer survey in 2009. (Heath 2010)

CONCLUSIONS

By looking beyond the healthcare drivers that led to the 2010 Healthcare Identifiers Act, it is possible to recognise that there are broader societal impacts that, as the Privacy Commissioner and Magnusson have warned, are not always immediately apparent. Ideally the Australian Privacy Principles (APP) would have been finalised and supported by legislation prior to tackling the complex issue of creation of Australian Healthcare Identifiers.

Looking to the future we can expect increased interest in secondary uses of Australian consumers medical data as the adoption of the IHI facilitates linkage of disparate datasets. Secondary uses include: commercial activities such as those offered by data brokers; medical research; clinical audit and healthcare administration. Research is currently underway to explore Australian consumer's expectations regarding secondary use of their medical data (Heath 2010). The outcomes of this research should assist by providing consumers voices in upcoming Government initiatives concerning eHealth and privacy.

REFERENCES

Australian Health Ministers' Advisory Committee. 2009. Healthcare identifiers and privacy: Discussion paper on proposals for legislative support: Australian Health Ministers' Advisory Council.

Australian Law Reform Commission. 2008. For Your Information: Australian Privacy Law and Practice. Report No. 108. 3 vols. 2008.

Australian Privacy Principles Companion Guide. 2010. Cabinet Secretary, Australian Government.

Baird, A., North, F; Raghu, T. S. 2011. 'Personal Health Records (PHR) and the future of the physician-patient relationship'. Paper read at ACM International Conference Proceeding Series, 8-11 February 2011, Seattle, Washington.

Braithwaite, J; Mannion, Russell. 2011. 'Government plans for public reporting of performance data in health care: the case against'. *Medical Journal of Australia* 195 (1): 41.

Gunter, Tracey D; Terry, Nicolas P. 2005. 'The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs and Questions'. *Journal of Medical Internet Research* 7 (1).

Hayrinen, Kristiina; Saranto, Kaija; Nykanen, Pirkko. 2008. 'Definition, structure, content, use and impacts of electronic health records: A review of the research literature'. *International Journal of Medical Informatics* 77: 291-304.

Heath, Jennifer. 2010. 'Emerging Consumers Views of Secondary Uses of Medical Data'. Paper read at 2010 International Symposium on Technology and Society, at Wollongong, New South Wales.

Jorm, Christine; Frommer, Michael. 2011. 'Government plans for public reporting of performance data in health care: the case for'. *Medical Journal of Australia* 195 (1).

Kalra, D. 2006. 'Electronic Health Record Standards'. *IMIA Yearbook of Medical Informatics 2006*: 136-144.

Ludwick, Dave; Manca, Donna; Doucette, John. 2010. 'Primary care physicians' experiences with electronic medical records'. *Canadian Family Physician* 56 (January 2010): 40-47.

Magnusson, R. S. 2004. 'The changing legal and conceptual shape of health care privacy'. *Journal of Law, Medicine and Ethics* 32 (4): 680-691.

Michael, M.G; Michael, Katina. 2010. 'Toward a State of Uberveillance'. *IEEE Technology and Society Magazine* 29 (2) :9-16.

National Electronic Health Records Taskforce. 2000. A Health Information Network for Australia: Report to Health Ministers by the National Electronic Health Records Taskforce.

Ng, Betty M. 2000. 'Universal Health Identifier: Invasion of Privacy or Medical Advancement?' *Rutgers Computer and Technology Law Journal* 26(2) (March 2000): 331-356.

O'Keefe, Christine M; Connolly, Chris J. 2010. 'Privacy and the use of health data for research'. *Medical Journal of Australia* 193(9) (November 2010): 537:541.

Safran, C; Bloomrosen, M; Hammond, W.E; Labkoff, S; Markel-Fox, S; Tang, P; Detmer, D. 2006. Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper. Maryland, USA.

Cite this article as: Heath, Jennifer. 2011. 'Consumers, ALRC Privacy Principles and the 2010 Healthcare Identifiers Act'. *Telecommunications Journal of Australia* 61 (3): 46.1-46.8. Available from http://tja.org.au.