Australian Privacy Foundation

enquiries@privacy.org.au

http://www.privacy.org.au/

14 February 2013

Joanna Kelly
Doll Martin Associates
Level 18 323 Castlereagh St
Sydney NSW 2000

Email: jkelly@dollmartin.com.au

Dear Ms Kelly

APF feedback - Review of the Healthcare Identifiers Act (2010) and Health Identifier Service.

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. I write as Chair of the Health Sub Committee of the APF. I refer to the Review of the Healthcare Identifier Act (2010) and Health Identifier Service background information paper, December 2012. The APF welcomes this opportunity to offer information that will influence the review.

The response that follows is organised in a grid that parallels components identified in the review document. In many places I refer to relevant, previuosly overlooked, APF submissions. I have also added a copy of the IAPPANZ presentation delivered last year to support the response. The APF Board is composed of voluntary members and reference to the submissions rather than repetition seemed a logical way to respond to the review. I have also added a copy of the relevant APF policies for your information.

Please do not hesitate to contact me if you require further clarification of the response.

Yours sincerely

Dr. Juanita Fernando
Chair, Health Sub Committee
Australian Privacy Foundation

Contact Details for the APF and its Board Members are at:http://www.privacy.org.au/About/Contacts.html

Dr Fernando is in Medicine, Nursing & Health Sciences, Monash University
Phone 03 9905 8537 or 0408 131 535 Email to:juanita.fernando@monash.edu

Dr Fernando is a Fellow and former councillor of the Australasian College of Health Informatics. http://www.achi.org.au/

REVIEW OF THE HEALTHCARE IDENTIFIER ACT (2010) AND HEALTH IDENTIFIER SERVICE

Introduction

Section 35(1) of the Healthcare Identifiers (HI) Act (2010) requires that an independent review is undertaken of the HI legislation and the HI Service after 2 years of operation. The aim of the review is to ensure that the Act provides the regulatory support to enable the HI Service to operate efficiently and effectively and the extent to which it supports the sharing of clinical information in practice.

The review will consider:

☐ The HI Act 2010; Regulations made under the Act

☐ Amendments to the HI Act proposed in the Personally Controlled Electronic Health Record (PCEHR) (Consequential Amendments) Act 2012

☐ The implementation, operation, performance and governance of:

- The HI Service
- The HI Service Operator (SO).

The review will consider any legislative, operational or administrative barriers that may be impacting the Act achieving its objectives and will make recommendations on changes that may be made to improve performance against the objectives of the HI Act.

The first phase of the Review will involve meeting with key stakeholders to discuss any issues, either with the Health Identifier legislation or with the operation of the Health Identifier Service, that impact current or future implementation of Health Identifiers to support clinical practice and the broader eHealth agenda.

Scope of the Review

*Please note there are known issues with downloading APF submissions with the Chrome browser

Review component	Review considerations	APF response
Assignment of identifiers	☐ Effectiveness of assignment of identifiers ☐ Effectiveness of record keeping by the Service Operator in relation to assignment of identifiers	1. The IHI is complex for use and creates additional work in complex settings. This results in error re the misidentification of patients with the result that incorrect records are updated. Consequently health records privacy breaches occur and the record attached to an IHI is not reliable for patient care; according to many patients' these errors can and do occur. 2. Patients have expressed concern the IHI has been used in various health locations to populate individual records in bulk. Patients have advised this was done without their consent. 3. Are visitors to Australia automatically assigned an IHI without consent? Are they presented with healthcare options that do not involve the use of an IHI? The APF has received mixed responses to this question. 4. The Service Operator has not ensured the effectiveness of record keeping in relation to assignment of the identifiers, see 1 above. 5. See also*: 5.1. RE: APF SUBMISSION, 1. HI SERVICE IMPLEMENTATION APPROACH, 2. HI SERVICE COMMUNICATION PLANS, 3. HEALTHCARE IDENTIFIER REGULATIONS http://privacy.org.au/Papers/NEHTA_HI_Comm_Impl_100625.pdf 5.2. RE: APF submission; Inquiry into Healthcare Identifiers Bill 2010 and Healthcare Identifiers (Consequential Amendments) Bill 2010 http://privacy.org.au/Papers/HI-Senate-100304.pdf 5.3. Re: Patient access to HI-related patient data http://privacy.org.au/Papers/Hlth-PatientAccess-100212.pdf for further information 5.4. APF feedback about the Personally Controlled Electronic Health Record (PCEHR) system: Legislation Issues Paper. http://privacy.org.au/Papers/PCEHR-LegIssues-110803.pdf 5.5 Policy Position: eHealth Data and Health Identifiers, 28 August 2009 http://privacy.org.au/Papers/eHealth-Policy-090828.pdf

Review component	Review considerations	APF response
Use and disclosure of identifying information	Effectiveness of provisions in relation to: ☐ Use and disclosure of identifying information by providers ☐ Disclosure of identifying information by data sources ☐ Disclosure of identifying information by the national registration authority ☐ Extent of/effectiveness of penalties for unauthorised use or disclosure	1. See 5, above. 2. Also see "How the Privacy Act and PCEHR Act inter-relate in respect of health privacy: A story" iappANZ Privacy Summit, Sydney, November 2012.
Disclosure of identifiers by Service Operator	Effectiveness of provisions in relation the Service Operator's obligations to: ☐ Disclose Individual Healthcare Identifiers (IHI) to a provider for authorised purposes ☐ Disclose the Healthcare Provider Identifier-Individual (HPI-I) to the registration authority to register the provider	1. Dual role of the service operator is problematic. Governance issues have not been managed appropriately and there is no detail in the public domain about the Service Operator's responsibilities 2. See APF submission; Inquiry into Healthcare Identifiers Bill 2010 and Healthcare Identifiers (Consequential Amendments) Bill 2010 http://privacy.org.au/Papers/HI-Senate-100304.pdf 3. APF feedback about the exposure draft PCEHR Bill 2011 (PCEHR Draft Bill) and exposure draft PCEHR (Consequential Amendments) Bill 2011 http://privacy.org.au/Papers/DoHA-PCEHRBills-111027.pdf 4. Inquiry into the PCEHR Bills Supplementary Submission re Governance http://privacy.org.au/Papers/Sen-PCEHR-Bill-Supp-120214.pdf
Disclosure of identifiers by healthcare providers	☐ Effectiveness of provisions in relation to the obligations of providers to disclose IHIs to the healthcare recipient or entity for purposes prescribed under the Act	1. See all comments and submissions above 2. See also, APF policy documents: 2.1.eHealth Data and Health Identifiers, Policy Statement (28 August 2009) http://privacy.org.au/Papers/eHealth-Policy-090828.pdf 2.2. eHealth Care Data Breach, Policy Statement (28 August 2009) http://privacy.org.au/Papers/eHealth-DataBreach-090828.pdf 3. What is a healthcare provider- this remains undefined e.g. are allopathy, comp med, support services (such as Meals on Wheels) healthcare providers?

Review component	Review considerations	APF response
Unauthorised use and disclosure of identifiers	☐ Effectiveness of penalties imposed for unauthorised use or disclosure of identifiers	1. See "How the Privacy Act and PCEHR Act inter-relate in respect of health privacy: A story" iappANZ Privacy Summit, Sydney, November 2012. 2. Also, see APF submission - eHealth record system OAIC Enforcement Guidelines. http://privacy.org.au/Papers/OAIC-PCEHREnf-120924.pdf 3. What is a healthcare organisation/provider- this remains undefined e.g. allopathy, comp med, support services (such as Meals on Wheels)?
Interaction with the Privacy Act 1988	☐ Breaches of privacy under the Privacy Act 1988 ☐ Findings of any Audits or investigations of the Service Operator undertaken by the Privacy Commissioner ☐ Complaints regarding the HI Service handled by the Privacy Commissioner ☐ Issues highlighted by the Privacy Commissioner and enforcement activities undertaken in relation to the HI service	1. See: "How the Privacy Act and PCEHR Act inter-relate in respect of health privacy: A story" iappANZ Privacy Summit, Sydney, November 2012. 2. See also: 2.1. APF submission - eHealth record system OAIC Enforcement Guidelines. http://privacy.org.au/Papers/OAIC-PCEHREnf-120924.pdf 2.2 APF feedback about the Personally Controlled Electronic Health Record (PCEHR) system: Legislation Issues Paper. http://privacy.org.au/Papers/PCEHR-LegIssues-110803.pdf 2.3 Policy Position: eHealth Data and Health Identifiers, 28 August 2009 http://privacy.org.au/Papers/eHealth-Policy-090828.pdf 2.4 RE: APF submission; Inquiry into Healthcare Identifiers Bill 2010 and Healthcare Identifiers (Consequential Amendments) Bill 2010 http://privacy.org.au/Papers/HI-Senate-100304.pdf (Section 1)
Oversight role of the Ministerial Council	☐ Directions given by the Minister for Health to the Service Operator ☐ Compliance by the Service Operator with directions issued ☐ Compliance by the Service Operator in relation to preparation of an Annual Report on the HI Service	1. The dual role of the service operator is problematic. Governance issues have not been managed appropriately and there is no detail in the public domain about the Service Operator's responsibilities, see relevant points made above. 2. See RE: APF submission; Inquiry into Healthcare Identifiers Bill 2010 and Healthcare Identifiers (Consequential Amendments) Bill 2010 http://privacy.org.au/Papers/HI-Senate-100304.pdf 3. APF feedback about the exposure draft PCEHR Bill 2011 (PCEHR Draft Bill) and exposure draft PCEHR (Consequential Amendments) Bill 2011 http://privacy.org.au/Papers/DoHA-PCEHRBills-111027.pdf

Review component	Review considerations	APF response
Performance of the HI Service Operator (DHS)	Consideration of the performance of the HI Service Operator in relation to: ☐ Maintenance of HI databases and infrastructure ☐ Recordkeeping ☐ Management of change requests ☐ Provision of the healthcare provider directory ☐ Support provided to healthcare organisations in implementing the service ☐ Contractual arrangements supporting operation of the HI Service, including Service Level Agreements (SLA)	1. What is a healthcare organisation- this remains undefined e.g. allopathy, complimentary medicine, support services (such as Meals on Wheels)? 2. Recordkeeping inaccuracies 2.1 APF submission – draft Mandatory data breach notification in the eHealth record system guide. http://privacy.org.au/Papers/OAIC-PCEHR-BreachNotificn-120929.pdf 2.2 Re: Inquiry into the PCEHR Bills Supplementary Submission re Governance http://privacy.org.au/Papers/Sen-PCEHR-Bill-Supp-120214.pdf 2.3 "How the Privacy Act and PCEHR Act inter-relate in respect of health privacy: A story" iappANZ Privacy Summit, Sydney, November 2012. 3. Required reports are very limited to no support given to some healthcare organisations, such as those offering complimentary medicine
Performance of NEHTA	Consideration of the performance of NEHTA in relation to: ☐ Validating the service is fit for purpose ☐ Support for the widespread adoption of the HI service through ongoing development of HI implementation collateral ☐ Distribution channels for the HI service (HI Service Channel Enhancement Project) ☐ Collaboration with HI Service to improve service delivery	1. Various codes are lacking, i.e. Dx, Mx etc. This lack of diagnostic choices leads to misunderstanding and medico legal consequences for clinicians and patient care error 2. Service is not able to support error in records re speedy response or notification to health services that an error has occurred- process too bureaucratic and patients health endangered as a result e.g. 2.1 APF submission – draft Mandatory data breach notification in the eHealth record system guide. http://privacy.org.au/Papers/OAIC-PCEHR-BreachNotificn-120929.pdf 2.2 Re: Inquiry into the PCEHR Bills Supplementary Submission re Governance http://privacy.org.au/Papers/Sen-PCEHR-Bill-Supp-120214.pdf

Review component	Review considerations	APF response
Barriers to achievement of objectives of the Act	Consideration of: ☐ Any legislative, administrative or operational restrictions to use of the HI Service ☐ Amendments to the HI Act proposed in the PCEHR (Consequential Amendments) Act 2012 ☐ Support of the HI Service for clinical practice in relation to: o Sharing healthcare information o Identification of other healthcare providers o Identification of consumers	1. The Act adds an layer of complexity to medical record keeping for healthcare providers 2. Each health organisation uses different practice software designed to differing standards that are not always able to interoperate for sharing healthcare information where this is appropriate. 3. The APF requires clarification of how much information from PCEHR that a clinician may download to their own records (i.e. screen dumps, scans of printed material) 4. Patients and clinicians do not trust the PCEHR, see 4.1 The Emperor's new clothes: PCEHR system security http://privacy.org.au/Papers/AusCERT-PCEHR-120518.pdf 4.2 Discharge summaries get diagnosis wrong January 31, 2013 : http://www.theage.com.au/national/discharge-summaries-get-diagnosis-wrong-20130130-2dl80.html 4.3 Experts: mHealth poses privacy challenge http://www.healthcareitnews.com/news/experts-mhealth-poses-privacy-challenge
Recommendations	Recommendations in relation to: ☐ Clarification of the legislation ☐ Removal of legislative restrictions ☐ Changes to overcome any administrative restrictions	1. The community is required to create an "Australia.gov.au" account, linking the generic AU government ID and the PCEHR patient login. This is a privacy invasive practice that enables all government information held about an individual to be stored, used and disseminated without consent. Future integration with other government agencies is planned, if not executed, in some instances – the IHI will be used for purposes other than healthcare. Many in the community are unaware of the extent of this access because health agencies promoting the service euphemize the real life meaning of their consent. 2. See 2.1 “How the Privacy Act and PCEHR Act inter-relate in respect of health privacy: A story” iappANZ Privacy Summit, Sydney, November 2012. 2.2 The Emperor's new clothes: PCEHR system security http://privacy.org.au/Papers/AusCERT-PCEHR-120518.pdf

Review component	APF response
Missing from the review	1. Publically available report as to the technical aspects of the HI – are these working? (response time, up time, etc) 2. An overview of the types of error and breaches that have occurred thus far that is beyond APF experience- i.e. available in the public domains. 3. Publically available information as to the level of usage of the system in terms of actuality – downloads would be a separate figure. 4. Information as to a further review in 12 months or so - this review seems too early. 5. Responses to matters previously raised in APF submissions 6. The legislation underpinning the PCEHR (http://www.comlaw.gov.au/Details/F2012L01703) evidently does not a) define an authorised user b) explicitly say that only authorised users are permitted to access a person's PCEHR. It would at first look, appear that there is nothing, legally, stopping anyone in the government from being given access to the PCEHR and looking at any data. 7. Does the audit log show when the system operator (in this case it would seem to be DoHA and APIS) accesses a citizen's eHealth record? And that includes the help desk and system admin staff. 8. Default access controls For the purposes of paragraph 15(b) and (c) and subsection 109(6) of the Act, the System Operator must establish and maintain default access controls that: (a) permit all registered healthcare provider organisations involved in the care of a registered consumer to access the consumer's PCEHR; (b) include an access list of the registered healthcare provider organisations that are permitted to access the consumer's PCEHR because the organisation is involved in the care of the registered consumer; The interesting thing is that the rules only apply to registered healthcare provider organisations and the consumer. If you are not in either of these groups, the rules do not apply to you. The rules do not explicitly state that only these groups should be allowed to access a PCEHR. So, technically it seems that anybody who can get access to the PCEHR system, provided they are not part of a registered healthcare provider organisation, can legally access anybody's PCEHR. 9. To many people in the community, the mandatory requirement "To register for an eHealth record you need to create an Australia.gov.au account, or log" seems unnecessarily privacy intrusive. No public explanation is given for this. Many in the community see the registration process for a PCEHR as a backdoor recreation of the "Australia Card". What is the purpose of this process from the consumers' point of view? 10. The Parliamentary Inquiry into "Cyber Security for Senior Citizens" is due to report in April. Its recommendations need to be considered as part of this review. 11. The hacking of IT records is a serious ongoing issue. However, there is an increasing incidence of computer theft or wrongful access to the expanding use of complex mobile phones, IPads etc. throughout the health system.(Study shows 94% of US healthcare organisations leaked data. Computer Fraud & Security:

	Volume 2013, Issue 1, January 2013, Pages 20 http://www.sciencedirect.com/science/article/pii/S1361372313700113; http://dx.doi.org/10.1016/S1361-3723(13)70011-3) 12. Discussion with industry about the development of data repositories/warehouses and the consequent inter-operability operation is just commencing. This is a very challenging and broad issue, a significant part of which will relate to privacy and security. This area is not widely understood and needs independent inquiry and ongoing oversight. 13.A major issue is quality implementation without which we are unlikely to have a useful system. Without appropriate Governance and Operational Management armed with a quality Business Case, Meaningful use implementation is unlikely to occur 14. The OAIC role is confined to historical legalistic action, which can be fine, but the complexity of a national system requires access to immediate investigation and action relating to many millions of individuals with daily needs by a multiplicity of service providers. This is a serious unmet community demand for your review.

Australian Privacy Foundation

Policy Position

Protections Against eHealth Data Breaches

28 August 2009

http://www.privacy.org.au/Papers/eHealth-DataBreach-090828.pdf

Personal health data is by its nature highly sensitive, so unauthorised access and disclosure is of even greater concern than it is with other categories of data. Irrespective of what laws and norms might apply to data breaches generally, it is vital that clear and effective protections exist for personal health care data. The APF has accordingly adopted the following policy on the matter.

A **data breach** occurs when personal health care data is exposed to an unauthorised person, and there is a reasonable likelihood of actual or perceived harm to an interest of the person to whom the data relates.

1. **An organisation that handles personal health care data must**:

   (a) take such steps to prevent, detect and enable the investigation of data breaches as are commensurate with the circumstances

   (b) conduct staff training with regard to security, privacy and e-health

   (c) subject health care data systems to a programme of audits of security measures

   (d) when health care data systems are in the process of being created, and when such systems are being materially changed, conduct a Privacy Impact Assessment (PIA), in order to ensure that appropriate data protections are designed into the systems, and to demonstrate publicly that this is the case

2. **Where gounds exist for suspecting that a data breach may have occurred, the organisation responsible must**:

   (a) investigate

   (b) if a data breach is found to have occurred, take the further steps detailed below

   (c) document the outcomes

   (d) publish information about the outcomes, at an appropriate level of detail

3. **Where a data breach has occurred, the organisation responsible must**:

   (a) promptly advise affected individuals (and/or their next of kin or carers)

   (b) provide an explanation and apology to affected individuals

   (c) where material harm has occurred, provide appropriate restitution

   (d) publish an appropriate notice and explanation in a manner that facilitates discovery and access by people seeking the information

   (e) advise the Office of the Federal Privacy Commissioner

4. **Where a serious data breach has occurred, the Office of the Federal Privacy Commissioner must**:

   (a) review the outcomes of any investigation undertaken by the responsible organisation

   (b) where any doubt exists about the quality, conduct its own independent investigation

   (c) publish the results of the review and/or investigation

   (d) add the details of the data breach to a publicly available register, including any decision made as the result of the investigation, in order to ensure that information is available to support informed public debate about protections for personal health care data

5. **Where a data breach occurs that results in material harm**, the affected individuals must have recourse to remedies, both under the Privacy Act and through a statutory cause of action

Australian Privacy Foundation

Policy Position
eHealth Data and Health Identifiers

28 August 2009

http://www.privacy.org.au/Papers/eHealth-Policy-090828.pdf

This document builds on the APF's submissions over the last two decades, and particularly during the last three years, in order to consolidate APF's policy position. It presents a concise statement of general Principles and specific Criteria to support the assessment of proposals for eHealth initiatives and eHealth regulatory measures.

The first page contains headlines only, and the subsequent pages provide further explanation.

General Principles

1 **Health care must be universally accessible.**

2 **The health care sector is by its nature dispersed.**

3 **Personal health care data is inherently sensitive.**

4 **The primary purpose of personal health care data is personal health care.**

5 **Other purposes of personal health care data are secondary, or tertiary.**

6 **Patients must be recognised as the key stakeholder.**

7 **Health information systems are vital to personal health care.**

8 **Health carers make limited and focussed use of patient data.**

9 **Data consolidation is inherently risky.**

10 **Privacy impact assessment is essential.**

Specific Criteria

1 **The health care sector must remain a federation of islands.**

2 **Consolidated health records must be the exception not the norm.**

3 **Identifiers must be at the level of individual applications.**

4 **Pseudo-identifiers must be widely-used.**

5 **Anonymity and persistent pseudonyms must be actively supported.**

6 **All accesses must be subject to controls.**

7 **All accesses of a sensitive nature must be monitored.**

8 **Personal data access must be based primarily on personal consent.**

9 **Additional authorised accesses must be subject to pre- and post-controls.**

10 **Emergency access must be subject to post-controls.**

11 **Personal data quality and security must be assured.**

12 **Personal access and correction rights must be clear, and facilitated.**

General Principles

1 **Health care must be universally accessible**. Access to health care must not be conditional on access to health care data or on demonstration of the person's status (such as residency rights or level of insurance)

2 **The health care sector is by its nature dispersed**. Health care is provided by thousands of organisations and individual professionals, each with a considerable degree of self-responsibility. The sector is far too large, and far too complex to be centrally planned. Instead it must be managed as a large, complex and highly de-coupled system of autonomous entities, each of which is subject to regulation by law, Standards and Codes

3 **Personal health care data is inherently sensitive**. Many individuals have serious concerns about the handling of at least some categories of health care data about themselves. Their willingness to divulge important information is important to their health care, but is dependent on them having confidence about how that information will be managed

4 **The primary purpose of personal health care data is personal health care**. The protection of the individual person is the primary function of personal health care data and systems that process it. The key users of that data are health care professionals

5 **Other purposes of personal health care data are secondary, or tertiary**. Public health is important, but is a secondary purpose. Administration, insurance, accounting, research, etc. are neither primary nor secondary but tertiary uses. The tail of health and public health administration and research must not be permitted to wag the dog of personal health care

6 **Patients must be recognised as the key stakeholder**. Government agencies and corporations must directly involve people, at least through representatives of and advocates for their interests, in the analysis, design, construction, integration, testing and implementation of health information systems

7 **Health information systems are vital to personal health care**. People want systems to deliver quality of service, but also to be trustworthy, transparent and respectful of their needs and values. In the absence of trust, the quality of data collection will be greatly reduced

8 **Health carers make limited and focussed use of patient data**. Health care professionals do not need or want access to their patients' complete health records, but rather access to small quantities of relevant information of assured quality. This requires effective but controlled inter-operability among health care data systems, and effective but controlled communications among health care professionals. Calls for a general-purpose national health record are for the benefit of tertiary users (administration, insurance, accounting, research, etc.), not for the benefit of personal health care

9 **Data consolidation is inherently risky**. Physically and even virtually centralised records create serious and unjustified risks. Services can be undermined by single points of failure; health care data isn't universally understandable but depends on context; consolidation produces a 'honey pot' that attracts break-ins and unauthorised secondary uses and creates the additional risk of identity theft; and diseconomies of scale and scope exceed economies

10 **Privacy impact assessment is essential**. Proposals relating to personal health care data and health care information systems must be subject to PIA processes, including prior publication of information, consultation with affected people and their representatives and advocates, and publication of the outcomes of the study. Designs for systems and associated business processes must be based on the results of the PIA, and implementations must be rejected if they fail to embody the required features

Specific Criteria

1 **The health care sector must remain a federation of islands**. The health care sector must be conceived as islands that inter-communicate, not as elements of a whole. Health care information systems must be conceived as independent services and supporting databases that inter-operate, not as part of a virtually centralised database managed by the State. Coordinating bodies must negotiate and facilitate inter-operability, not impose central schemes

2 **Consolidated health records must be the exception not the norm**. A small proportion of the population may benefit from linkage of data from multiple sources, primarily patients with chronic and/or complex conditions. Those patients must be the subject of consent-based, specific-purpose data consolidation. This activity must not apply to people generally

3 **Identifiers must be at the level of individual applications**. Each of the large number of dispersed health care information systems must use its own identifier for people. A system-wide or national identifier might serve the needs of tertiary users of personal data, but does little for the primary purpose of personal care, and it creates unnecessary risks for individuals

4 **Pseudo-identifiers must be widely-used**. Particularly when personal data moves between organisations, the maximum practicable use must be made of one-time-use and other forms of pseudo-identifiers, in order to keep people's identities separate from the data itself, and minimise the risk of personal health care data escaping and being abused

5 **Anonymity and persistent pseudonyms must be actively supported**. Anonymity is vital in particular circumstances such as ensuring that people are treated for sexually transmitted diseases. Persistent pseudonyms are vital in particular circumstances such as for protected witnesses, victims of domestic violence, and celebrities and notorieties who have reason to be concerned about such threats as stalking, kidnapping and extortion

6 **All accesses must be subject to controls**. Access to personal data must be subject to controls commensurate with the circumstances, including the sensitivity of the data and the potential for access and abuse of access. This requires identification of the category of person and in many cases of the individual who accesses the data, and authentication of the category or individual identity. However, the barriers to access and the strength of authentication must balance the important value of personal privacy and effective and efficient access by health care professionals

7 **All accesses of a sensitive nature must be monitored**. Non-routine accesses and accesses to particularly sensitive data must be detected, recorded, and subject to analysis, reporting, sanctions and enforcement

8 **Personal data access must be based primarily on personal consent**. The primary basis for access to personal data is approval by the person concerned. Consent may be express or implied, and may be written, verbal or non-verbal, depending on the circumstances. All accesses based on consent must be detected, recorded and subject to analysis, reporting, investigation, sanctions and enforcement

9 **Additional authorised accesses must be subject to pre- and post-controls**. All accesses that are not based on personal consent must be the subject of explicit legal authority that has been subject to prior public justification. All such accesses must be detected, recorded and subject to analysis, reporting. investigation, sanctions and enforcement

10 **Emergency access must be subject to post-controls**. Health care professionals (but only health care professionals) must have the practical capacity to access data in apparent violation of the personal consent principle, but must only do so where they reasonably believe that it is necessary to prevent harm to some person. All such accesses must be detected, recorded, reported and subject to analysis, investigation, sanctions and enforcement

11 **Personal data quality and security must be assured**. Data must be of a quality appropriate to its uses, and retained only as long as it remains relevant. Personal data in storage, in transit, and in use, must be subject to security controls commensurate with its sensitivity, and with the circumstances

12 **Personal access and correction rights must be clear, and facilitated**. Each person must have access to data about themselves, and access must be facilitated by any organisation that holds data that can be associated with them. Where appropriate, the access may be intermediated, in order to avoid misunderstandings and misinterpretation of the data. Where data is not of appropriate quality, the person must be able to achieve corrections to it

How the Privacy Act and PCEHR Act inter-relate in respect of health privacy: A story

Dr Juanita Fernando
Chair, Health Sub Committee
Australian Privacy Foundation

Health Informatics Researcher
Medicine, Nursing and Health Sciences
Monash University

Which law?*

- Australian health privacy legislation should inform standards and guidelines to regulate patient information-handling.
- Federal regulations contradict many state & territory legislative frameworks
- The introduction of the PCEHR system adds a new layer of complexity to the regulations.
- The regulatory environment is both confusing and contradictory.

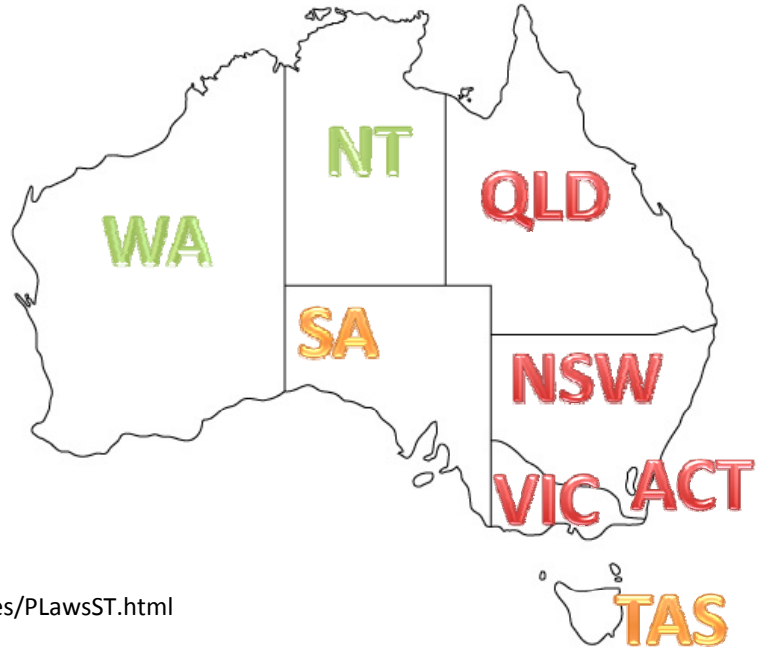
*Jan Whitaker, APF Board

Overview

1. Australian legal frameworks (excluding privacy principles)
2. ALRC review of privacy laws
3. eHealth and the PCEHR
4. Practice at the intersection: the clinician, the patient
5. A way forward

The Australian Privacy Act

- Health care offered by a mixture of public/private clinicians in public care settings
- Federal Privacy Act (extended in 2000 to incorporate private sector health practices)



http://www.privacy.org.au/Resources/PLawsST.html

Example: Victorian Health Records Act (VHRA)

Designed to bolster and compliment the Federal Act : contradictions

Privacy Act	VHRA
Contemporaneous	Retrospective
Exempts employee records	Does not exempt the records
Co-regulatory	Not co-regulatory
Private sector amendments	
NHMRC guidelines (S95)	

Authorities: practical, realistic, discretionary

Feasibility?

Secondary uses of PCEHR data

- Refers to use outside the delivery of direct patient care so long as this is related to medical treatment and can reasonably be expected by the patient.

- How does one determine what uses are and are not **reasonably expected**?

- **We will return to this point later**

Australian Law Reform Commission (ALRC) review

This 28-month inquiry of Australian health privacy law: *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108).

Key privacy findings influencing health care (8 of 10):
1. Simplification and streamlining of laws
2. Uniform privacy principles and national consistency
3. Regulating cross-border data flows & accountability
4. Rationalisation of exemptions and exceptions
5. Improved complaint handling and stronger penalties
6. Mandated data breach notification
7. Cause of action for a serious invasion of privacy
8. Health privacy – new regulation

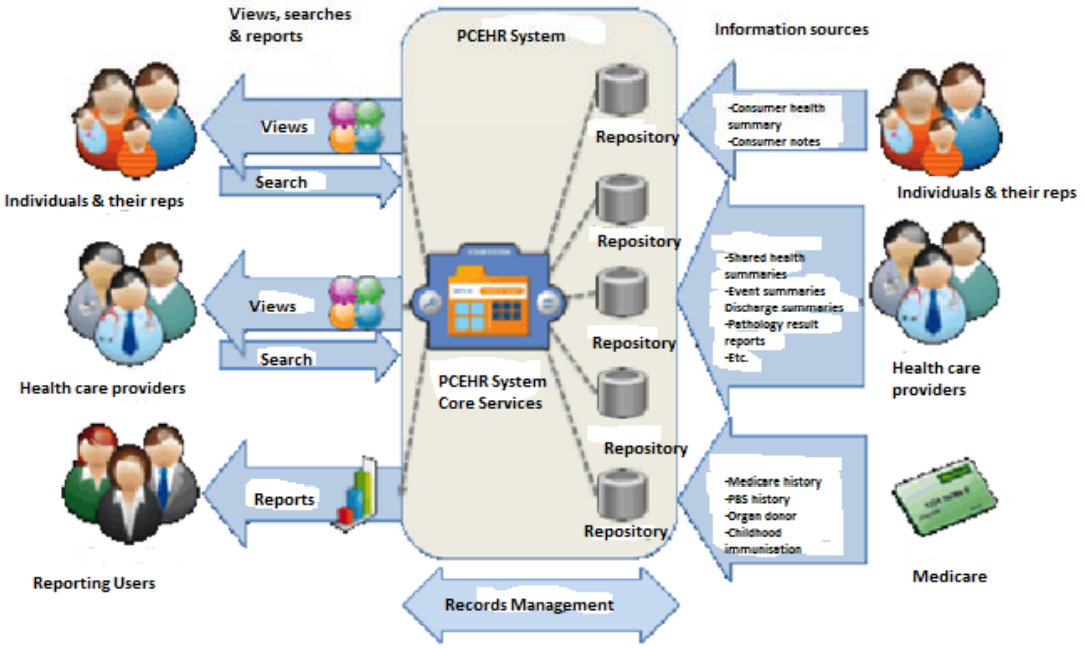
Privacy surpasses all other considerations: cost, convenience

eHealth

- eHealth : the intersection of digital technologies and health and wellbeing at the “doing end”
- New and emerging technologies as health enablers
- Unified national eHealth systems world-wide

The Personally Controlled E-Health Record system overview

According to health authorities the national PCEHR , has been designed as a secure, electronic record of patient medical history that is ... “stored and shared in a network of connected systems” (http://www.nehta.gov.au/ehealth-implementation/what-is-a-pcher)



The PCEHR system implementation

- Live mid 2012
- Overlaps existing apps
- Foundation: Individual Health Identifier (IHI) number
- Privacy legislation amended for IHI number , secondary use

Patient hopes : PCEHR system

- Governance at its heart
- Transparent
- Direct patient control
- Informed consent

Reality & the PCEHR

- Amnesty from responsibility for breaches
- Human factors ignored by technical audit
- Breach scope limited

Grievances & the PCEHR

- Complaints handling
  - Process
  - Criteria
  - Lack of certainty

The PCEHR Intersection

Supporting legislation and guidelines –

- overlap existing systems
- regulates collection, use and disclosure of system information.
- does not regulate data security or data accuracy
- Is complex & contradictory

Privacy and security challenges

- Security possible without privacy but no privacy without security
- Lack of serious enforcement exemplars
- Rhetoric – privacy is critical

Summary of the status quo

PCEHR/Privacy Legislation	ALRC findings
Uncertain/ no consistency (PPs)	Certainty/ consistency
Weakened health privacy legislation	New health privacy legislation
Complaints: bureaucratic, confusing	Improved complaint handling
Technical breach penalties	Penalties for all breaches
Data breach notification optional	Data breach notification mandatory
Optional cause of action for serious privacy breaches, discretionary	Cause of action for serious privacy invasions
Exemptions & exceptions	Accountable (rationalise exceptions etc.)

... reasonable, practical, to the best of one's ability, individual judgement, discretionary
... significant breaches
... The Information Commissioner may choose not to act on proven breaches ...

Approaches to status quo

- Legal: interpretation of thresholds
- Information commission : no body of guidance
- IT consultant : effective auditing regime?
- Operational manager : confusing (resources)

“Reasonable” in the real world

- Wireless and emerging technologies
- IT networks and servers
- Clinician uncertainty and trust
- Support of clinician eHealth expertise

Safety errors in context of “reasonable”

1. User interface
2. Never-ending system demands
3. Unfavourable work flow
4. Combined technology
5. Time demands
6. Other software issues

Clinicians

View of confusing, overlapping, health privacy

"…It would be nice if there was a standard thing and everything [patient privacy controls were] … right across the board and it was literally

something, a Gantt chart, you followed

through…"

-leads to lack of trust, workarounds

Clinical views

I'm doing 5 things at once and I'm the only person there"

a "*trade-off between what would be great security and what becomes inconvenient*" in care settings

"... People tend to leave it open on the ward and don't close it after they've finished

... It's very obtrusive, although the time might be relatively small ... Its time you can't spare

"literally red with rage"

"… minimal administration support and staff don't do the bulk of their work in that area."

"… in the end, the system works on trust"

Patients

"damage done when trust and confidence is lost between a patient and providers of health care …– … that alone, if no other harm is done or identified, is already harm enough … [to a patient]".

Patient views

" I don't understand computers … "

"I was very upset. This is the equivalent of finding all the medical records dumped for anyone to find them … "

"I've never used a computer before … my children are showing me how …"

" … because I cannot spell, and I do not understand the spellcheck function sorry [sic] …"

*" … supporting clinical information for an entire cancer are team was available in clear text …[*cached by a search engine)"

"I don't trust it… [the Internet]"

"We were never given a password or website to access so there is no reason for this information to be online - it is not like we could log on and check it ourselves."

" I don't have one …"

" I'm not computer savvy…"

" I don't use computers …"

" I didn't know …"

Accountability

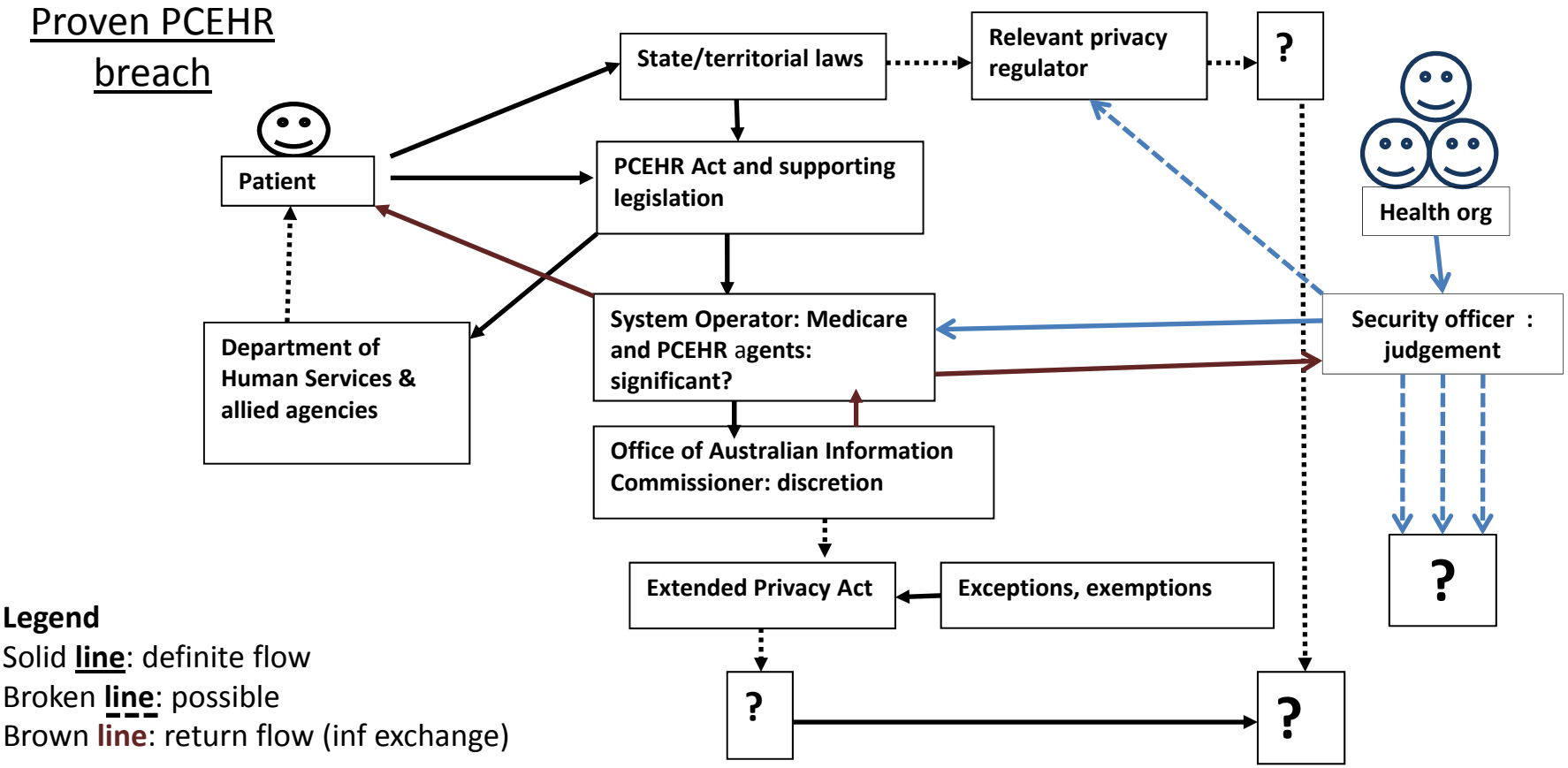
"Truth" in a person's eHealth record

- Validity of interpretation
- Transparency-data mining
- Responsibility for downstream use

The moral of the privacy story

- Australians care about their privacy
- Clinicians and patients care about outcomes
- Privacy legislation inconsistent
- Lack of robust exemplars, models
- OAIC draft guidelines and legislation don’t seem to support these concepts.

How things work in real life



How are patients and clinicians expected to function in this setting?

Ways forward

- Deconstruct legislative guidelines
- Develop new legislative models and guides (ALRC)
- Use current and emerging evidence
    1. Jennifer Heath, PhD, “A privacy framework for secondary use of medical data”
    2. Privacy experts and other professionals

Thank you

- Questions

My contact email:

juanita.fernando@monash.edu