Australian Privacy Foundation

enquiries@privacy.org.au

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

12 February 2013

Natasha Roberts
Policy adviser
Office of the Australian Information Commissioner
GPO Box 2999
CANBERRA ACT 2601

Email: Natasha Roberts <Natasha.Roberts@oaic.gov.au>

Dear Ms Roberts

APF feedback on a series of draft factsheets developed for consumers on privacy and eHealth

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 your request for our feedback on a series of factsheets developed by your office for consumers on privacy and eHealth. We welcome this opportunity to offer information that will influence factsheet content.

The response that follows is organised in a series of points that applies to all the factsheets unless otherwise specified. I have also added a copy of the IAPPANZ presentation delivered last year to support the response, along with copies of the relevant APF policies for your information.

1. The "factsheets" do not distinguish between eHealthcare records and the Personally Controlled Electronic Healthcare Record (PCEHR). Do the "factsheets" provide information about the PCEHR or eHealthcare records including the PCEHR – these are not the same thing?

The nomenclature needs to be accurate so that consumers can understand and contextualise information embedded in the "factsheets".

2. The "factsheets" suggest consumers can control access to their eHealthcare record by editing access controls in an online consumer portal. Firstly, does the consumer portal exist at present? Secondly, there is no mention of practitioner screenshots and print-outs of the eHealthcare records stored or circulated in **any** eHealthcare systems.

Individuals require advice about how they may control unauthorized print outs and screen shots of the eHealthcare record. They also require an Internet link to the consumer portal.

3. The factsheets suggest consumers can access their own e Healthcare record. The APF understands such access will be mediated by health authorities, such as the Deportment of Human Services. However the "factsheets" refer to an online consumer portal version of an individual's health record. Is an individual able to audit information and access their own eHealthcare record without a third party mediating such?

Individuals require direct and unmediated access to their own eHealthcare record.

4. The message I receive reading through the "factsheets" is that once I have consented to and populated a PCEHR with my doctor, who must also be registered, that I will lose all control over any health or medical information stored in the eHealthrecord.

5. Several pertinent matters are not addressed in the "factsheets". The list that follows is drawn from the PCEHR Act 2012 and the eHealth website at http://www.ehealth.gov.au

PCEHR is never deleted, even on cancellation
PCEHR is held for up to 130 years
PCEHR can be revealed for law enforcement purposes
PCEHR can be revealed for medical insurance and other purposes
Healthcare providers sign an agreement giving the Department of Health and Ageing the right to copy, adapt and communicate your PCEHR to others
These rights can never be revoked even on termination of the agreement
These rights are then conferred by the Department to all other participants in the agreement
General practitioners who do not sign the participation agreement will become ineligible for incentive payments up to $50,000 per annum per practice
The information held in your PCEHR may lawfully be obtained by means other than accessing your PCEHR
Even after "cancellation", your PCEHR may be accessed by healthcare providers and for "other purposes authorised by law"

The APF believes this information requires addition to all the "factsheets". ……

6. The document assumes that all individuals are computer-savvy and will be able to follow advice provided in the "factsheets". This is not the case. I have attached a copy of the presentation "How the Privacy Act and PCEHR Act inter-relate in respect of health privacy: A story", iappANZ Privacy Summit, Sydney, November 2012, to our feedback for your information. I have also refer you to the APF submission - "eHealth record system OAIC Enforcement Guidelines", http://privacy.org.au/Papers/OAIC-PCEHREnf-120924.pdf, for further information on this matter.

The "factsheets" assume knowledge of computer technology that many in the community do not posses.

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/

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

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

APF Policy Statement on Information Security

23 December 2012 : http://www.privacy.org.au/Papers/PS-Secy.html

Organisations hold a great deal of personal data. All of it is at least to some degree sensitive, and some of it highly so. Inappropriate handling of personal data represents a threat variously to the safety, wellbeing and peace of mind of the people it relates to. Primary privacy concerns are in the areas of unauthorised use and disclosure of data, with other issues including loss of data and threats to data integrity. Personal data needs the same level of care as financial information.

The privacy interest shares a great deal of common ground with organisations' own needs for protection of data of financial and competitive value, with commercial confidentiality, and with government and national sovereignty desires for the protection of sensitive data.

Information and Information Technology Security are well-established fields of professional endeavour, supported by a substantial array of products and services and a busy industry.

Organisations have moral and legal obligations to apply the available knowledge and to thereby ensure privacy protection. This applies to:

- all government agencies at federal, State and Territory, and local levels
- large and medium-sized business enterprises and not-for-profit organisations
- small business enterprises and not-for-profit organisations that handle personal data
- service-providers, including to small organisations and consumers, where the services provided involve personal data that is under the control of the service-provider's customer (particularly personal health records and credit-card data, but also, for example, records of goods and services purchased, social media, dating services and business-contact lists)

The following, specific obligations exist, must be recognised by organisations throughout the public and private sectors, and must be enforced by regulatory agencies.

Security Governance

All organisations have obligations to:

- conduct Information Security Risk Assessment (SRA), which identifies and evaluates threats, vulnerabilities and potential harm, including a focus on risks to the privacy of individuals whose data the organisation handles
- establish an Information Security Risk Management Plan (SRMP), which specifies the information security safeguards that are to be established and maintained, including safeguards against risks to the privacy of individuals whose data the organisation handles
- establish and maintain business processes to ensure the implementation, maintenance, review and audit of those information security safeguards

Resources to guide and support these activities include:

- ISO/IEC 27005:2008 'Information technology – Security techniques – Information security risk management'
- NIST (2012) 'Guide for Conducting Risk Assessments' US National Institute for Standards and Technology, SP 800-30 Rev. 1 Sept. 2012, pp. 23-36

Security Safeguards

All organisations have obligations to establish and maintain a sufficiently comprehensive set of information security safeguards in the following areas, commensurate with the sensitivity of the data:

- Physical Access Controls, such as locks, and authorisation processes for entry to premises
- Logical Access Controls, such as user account management, privilege assignment, and user authentication
- Data Protection in Transit, such as channel encryption and authentication of devices
- Data Protection in Storage, such as access logs, backup and recovery procedures, and encryption
- Perimeter Security, such as firewalls, malware detection, and intrusion detection
- Internal Security, such as vulnerability testing, patch management, software whitelisting, malware detection, and automated detection of security incidents
- Software Security, such as pre-release testing, change control and configuration management
- Organisational Measures, such as staff training, staff supervision, separation of duties, security incident management, log monitoring and audits
- Legal Measures, such as terms of use for employees, and terms of contract for suppliers
- Data Breach Notification Processes
- Formal Audit of data protection measures

Resources to guide and support the design and implementation of effective safeguards include:

- Andress J. (2011) 'The Basics of Information Security' Syngress, www.syngress.com, 208 pp.
- Clarke R. (2013) 'Information Security for Small and Medium-Sized Organisations' Xamax Consultancy Pty Ltd, 2013
- PCI-DSS (2010) 'Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures' Version 2.0, PCI Security Standards Council, October 2010
- ISM (2012) 'Information Security Manual – Controls' Defence Signals Directorate, 2012
- ISO/IEC 27001:2006 'Information technology — Security techniques – Information security management systems – Requirements', Annex A, pp. 13-29
- Goodrich M. & Tamassia R. (2011) 'Introduction to Computer Security' Addison-Wesley, 2011, 576 pp.

Sanctions

All organisations, and individuals within organisations, must be subject to sanctions where they fail to fulfil their information security obligations.

Sanctions must exist, and must be applied, at all of the following levels:

- civil liability by organisations
- civil liability by directors
- staff disciplinary action, up to and including dismissal in serious cases
- criminal liability for serious and repeated cases

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.

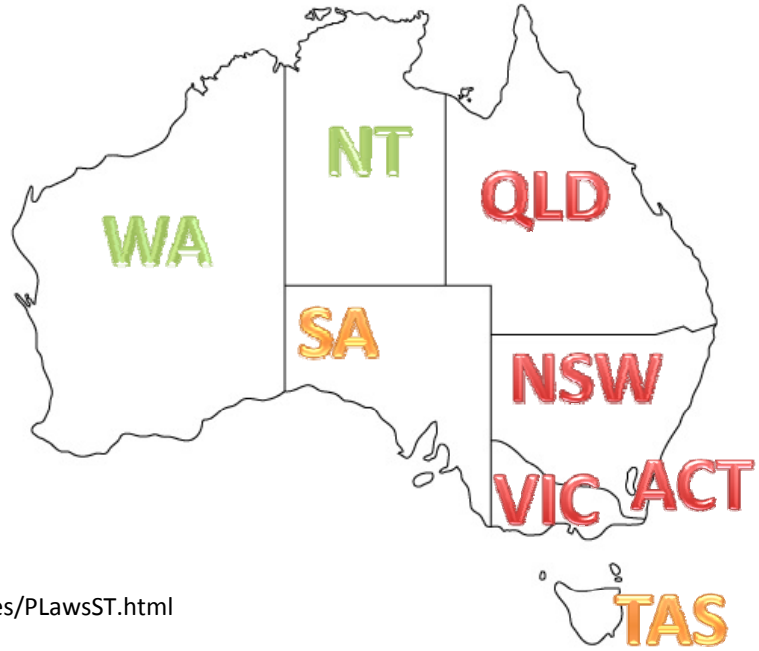
*Jan Whitaker, APF Board

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

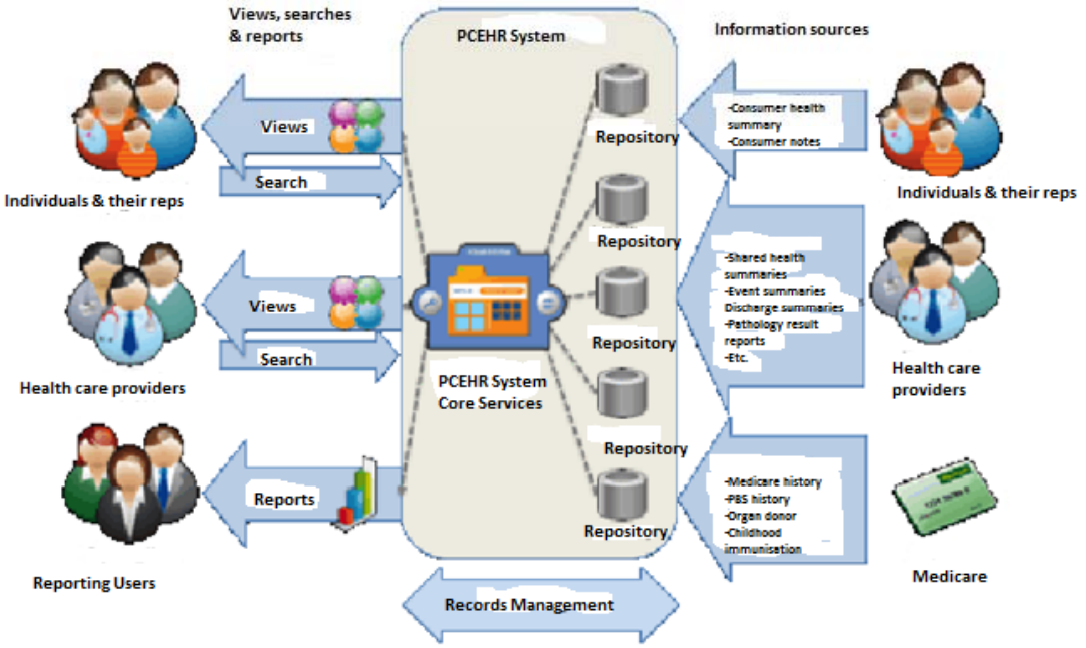
Privacy surpasses all other considerations: cost, convenience

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

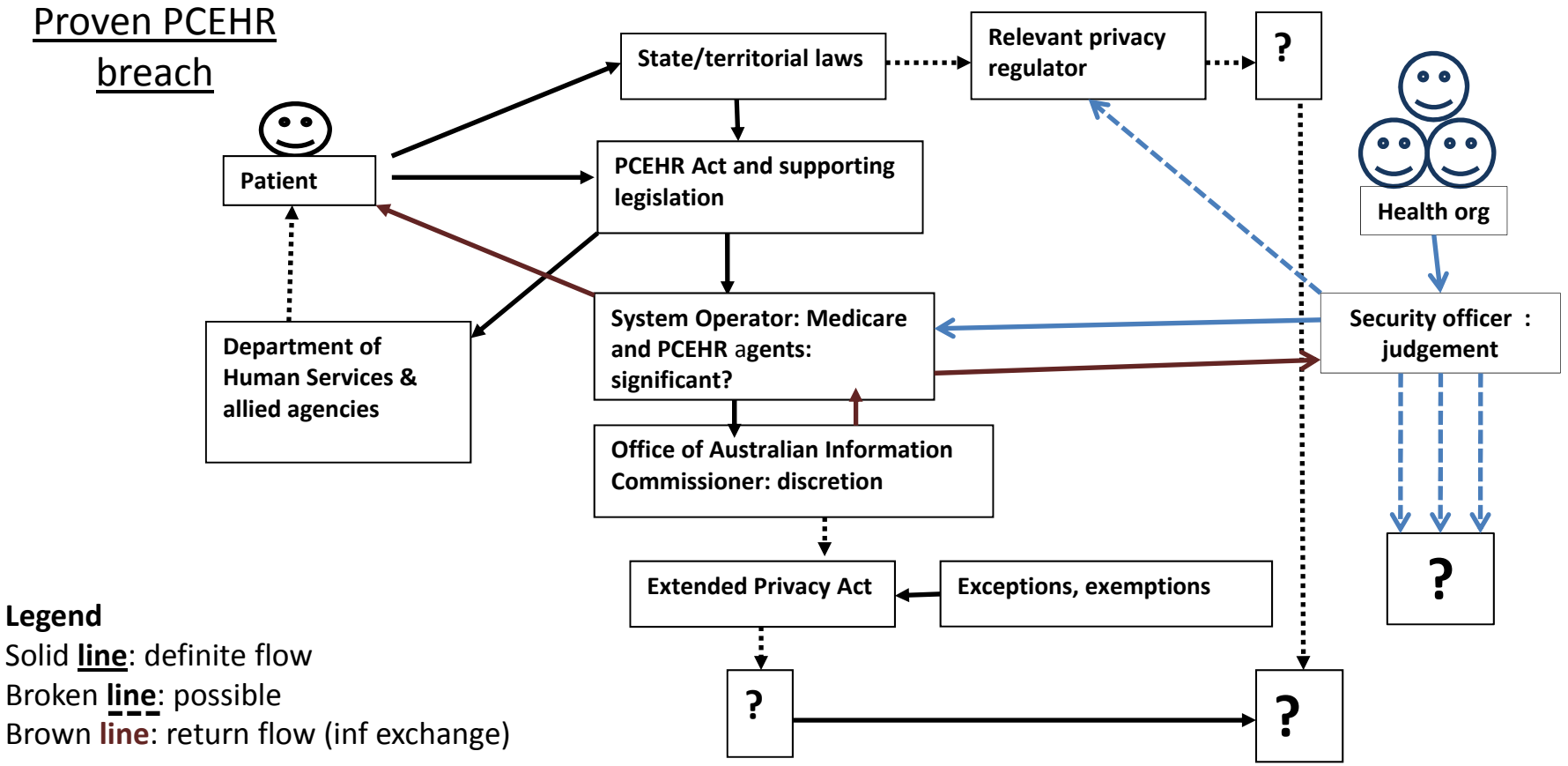
"Truth" in a person's eHealth record

- 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