MONASH University

Medicine, Nursing and Health Sciences

The Emperor's new clothes: PCEHR system security

Dr. Juanita Fernando
Bachelor of Medicine Bachelor of Surgery (MBBS)

Mobile Health Research Group

Chair, Health Sub Committee, Australian Privacy Foundation

AusCERT 2012
Security on the Move
14th-18th May 2012;
Royal Pines Resort Gold Coast, Queensland Australia.

Australian Privacy Foundation

Important matters outside the scope of this presentation

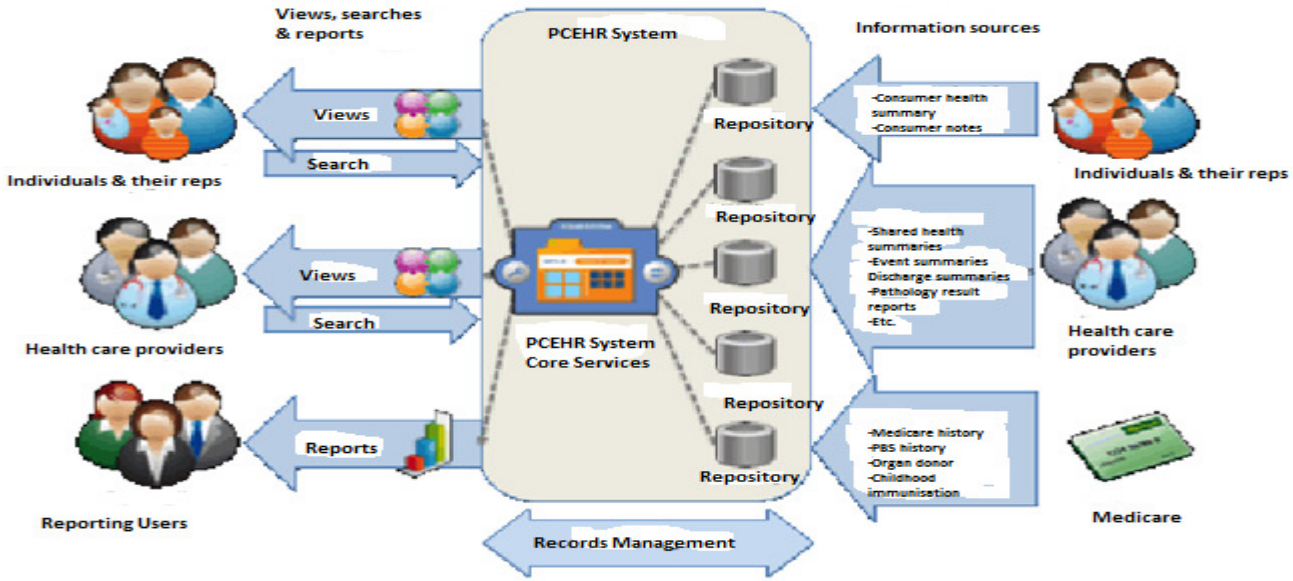
Exclusions
Privacy as a specific concern
The “opt-in” or “opt-out” discussion
NEHTA’s corporate status
Emergencies
Informed consent, consumer education
Governance- retrofitted and incomplete
Absolution of government jurisdictions and their agents
Schedule of actual deliverable and benchmarks
Document viewing service
IP - copyright or moral rights
Support for e-health enabled patient care

What is the PCEHR system?

1. PCEHR= the Personally Controlled Electronic Health Record national system
2. Ostensibly a secure, electronic record of patient medical history
3. Stored and shared in a network of connected systems

(http://www.nehta.gov.au/ehealth-implementation/what-is-a-pcehr)

Diagrammatic overview



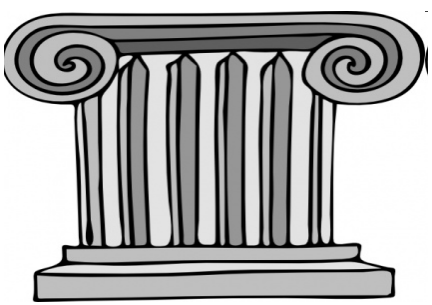
PCEHR Concept of Operations, Sept 2011: http://www.nehta.gov.au/

The PCEHR & The Emperor's New Clothes (Hans Christian Andersen)

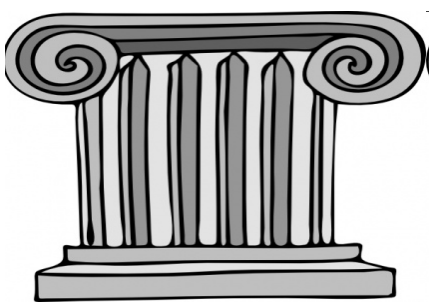
http://technicalinfodotnet.blogspot.com.au/2012/03/virtual-execution-and-emperors-new.html

Security & patient care

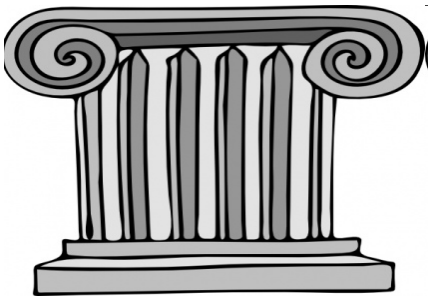
1. Familiar 3 pillars of data-CIA
2. Same as required for good consultation techniques



CONFIDENTIALITY



INTEGRITY



AVAILABILITY

PCEHR system realities

Just because one pillar is secure, it doesn't mean the others are.

Why?

1. Human factors
2. Practice organisations
3. Standards and specs
4. The security terrain is always moving

Human factors (1 of 2): Clinicians

"queues" so "*sometimes we don't bother to update the medical record*"

Paper useful "*when the IT system is down"*

"a pain in the arse"

*"shut the bastard down [*security system*] for it's …erm … ethics"*

"*literally red with rage"*

"interrupt the diagnostic process"

"they will ring me and I will tell them the password"

"*In the end the [*health information] *system works on trust, whatever bits and pieces you've got in the place."*

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

Many clinicians- *"simply given up"*

Human factors (2 of 2): Patients

" I don't understand computers … "

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

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

" I don't have one …"

" I'm not computer savvy…"

" I didn't know …"

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

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

"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 use computers …"

System reality #1

-Clinicians are busy and time-poor, security is not their work priority

-Many patients do not know how to secure e-health information

- The PCEHR system assumes an equal level of e-health security competence and understanding is shared by all Australians, when reality clearly demonstrates otherwise

Practice organizations

Current problems
PBS and MBS information co-located in database (Hansard, Inquiry into Personally Controlled e-Health Records Bill 2011)
Prescription data stored on pharmacy computers fail ANAO audit (Brettingham-Moore, C. ,Medical Observer, June 4 2010)
QLD health unsustainable : Tony O'Connell (Courier Mail. Nov 1 2011)
Access control – passwords, clear text (patient reports & Fernando, J; MJA 196:7)
2 year amnesty period : accidental breaches - penalties, jail terms (MSIA submission, Inquiry into PCEHR Bill and Consequential Amendments Bill 2011)
Pause primary care desktops at Lead sites; software incompatibilities; specs not fit for purpose. (The Aus 24 Jan; Parnell, S.)
No liability for government agents (Hansard, Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011, Personally Controlled Electronic Health Records Bill 2011)

" I have no idea how it happened …" [e-health security breach]

System reality #2

- When government instruments fail security tests either no action is taken or security rules are weakened.
- Current security trials for the PCEHR have occurred during an amnesty. No end user can learn from this experience or has access to the evidence.
- From July 2012 national PCEHR implementations may see clinicians facing medico-legal consequences in real life, including jail.
- So many factors, often low level or only partially relevant, will combine to threaten a national PCEHR system.

Standards and specs 1/2

Medibank database leveraged for IHI numbers (NEHTA: Draft Concept of Operations, March 2011)	Data-IA
NEHTA's SAF – use of existing patient numbers as IHI unreliable (NEHTA (2009). *HI service and security access framework version 1.0.)*	Data-IA
Urgent review of vendor portal, many unresolved issues (MSIA submission, Inquiry into PCEHR Bill and Consequential Amendments Bill 2011)	Data-CIA
Bolt – on, parasitic software : buffer overflows (Dr McCauley & Dr Patricia Williams in Dearne, K.The Australian, February 05, 2012)	Data-CIA
Centrally managed data-base linked to indexed system of federated data-bases (PCEHR Concept of Operations, Sept 2011: http://www.nehta.gov.au/)	Data-CIA

Standards and specs 2/2

Technical & policy audits only (Hansard, Personally Controlled Electronic Health Records (Consequential Amendments) Bill 2011, Personally Controlled Electronic Health Records Bill 2011)	Data-CIA
Failure to take advice (Ongoing submissions and evidence to Senate Inquiries)	Data-CIA
Immature clinical terminology (More, D. Australian HIT blog: http://hl7-watch.blogspot.com/)	Data-IA
First 6 of 10 digits of the unique PCEHR website system logon to Australian Health Practitioner Regulation Agency common to all registered clinicians (O'Brien, M, Medical Observer, 27 April 2012)	Data-CIA
Internet-based training for clinicians and consumer: released May 10 2012 (E-Health Learning goes live, www.ehealth.gov.au & follow learning links, email to subscribers of PCEHR.Engagement@nehta.gov.au)	Data-CIA
People with limited or no access to or use of computers	Data-CIA

Yet the system is inexorably moving on to meet a July 1 deadline.

System reality #3

- The PCEHR system standards and specs are a moral-minefield of security threat.
- Expert advice doesn’t seem to be heeded or incorporated into risk mitigation strategies.
- Stop rushing to arbitrary deadlines, get it right first.

The security terrain is always moving

Security: minefield of medico-legal and patient safety concerns
No fixed gateway perimeter to protect
Cloud computing - Google, Microsoft and other Cloud Services down for hours
Smart Phones – designed for point to point communication not a replacement computer system
Tablets – designed for point to point communication not a replacement computer system
Software for smart phones and tablets – personal and professional use combined (clinicians and many other Australians)
Unintended risks we cannot yet foresee

System reality #4

- Many systems that will be used in a PCEHR context are simply not up to the job now!
- What is secure today will not be secure tomorrow.
- We cannot future-proof security but we can address the risks we know of now.

The security-aware tailor’s task

The fabric of the PCEHR system – be like the child in the story of the Emperor's New Clothes

- The fundamental tenets of system security are the same as those required for error-free patient care. It isn’t too late yet.

- Point out problems and fixes :
    1. Human factors
    2. Practice organisations
    3. Standards and specifications
    4. The fluid security terrain

- Help tailor a system security fabric that will work for all Australians.

Thank you

Questions?

Monash University

Australia

Malaysia

South Africa

Italy

India

Australian Privacy Foundation

Dedicated to protecting privacy rights